Configurer et activer la communication SSL bidirectionnelle

SnapCenter Software 5.0

NetApp
July 18, 2024

Sommaire

Configurer et activer la communication SSL bidirectionnelle

Configurer la communication SSL bidirectionnelle

Vous devez configurer la communication SSL bidirectionnelle pour sécuriser la communication mutuelle entre le serveur SnapCenter et les plug-ins.

Avant de commencer

- Vous devez avoir généré le fichier CSR du certificat de l'autorité de certification avec la longueur minimale de clé prise en charge de 3072.
- Le certificat de l'autorité de certification doit prendre en charge l'authentification du serveur et l'authentification du client.
- Vous devez disposer d'un certificat d'autorité de certification avec une clé privée et des détails d'empreinte digitale.
- Vous devez avoir activé la configuration SSL unidirectionnelle.

  Pour plus de détails, voir "Configurer la section certificat CA."

- Vous devez avoir activé la communication SSL bidirectionnelle sur tous les hôtes de plug-in et sur le serveur SnapCenter.

  L'environnement avec certains hôtes ou serveur non activé pour la communication SSL bidirectionnelle n'est pas pris en charge.

Étapes

1. Pour lier le port, effectuez les étapes suivantes sur l'hôte du serveur SnapCenter pour le port 8146 (par défaut) du serveur Web IIS de SnapCenter et une fois de plus pour le port 8145 (par défaut) de SMCore à l'aide des commandes PowerShell.

   a. Supprimez la liaison de port de certificat autosignée SnapCenter existante à l'aide de la commande PowerShell suivante.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
   ```

   Par exemple :

   ```
   > netsh http delete sslcert ipport=0.0.0.0:8145

   > netsh http delete sslcert ipport=0.0.0.0:8146
   ```

   b. Liez le nouveau certificat CA fourni au serveur SnapCenter et au port SMCore.

   ```
   > $cert = "<CA_certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>
   ```

```
certhash=$cert appid="$guid" clientcertnegotiation=enable
verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

Par exemple :

```
> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

> netsh http show sslcert ipport=0.0.0.0:8145
```

2. Pour accéder à l'autorisation du certificat de l'autorité de certification, ajoutez l'utilisateur par défaut du serveur Web IIS de SnapCenter «**IIS AppPool\SnapCenter** » dans la liste d'autorisations de certificat en effectuant les étapes suivantes pour accéder au certificat de l'autorité de certification nouvellement acquise.
   a. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier** > **Ajouter/Supprimer Snapin**.
   b. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
   c. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
   d. Cliquez sur **Console Root** > **Certificates – local Computer** > **Personal** > **Certificates**.
   e. Sélectionnez le certificat SnapCenter.
   f. Pour démarrer l'assistant d'ajout d'utilisateur/d'autorisation, cliquez avec le bouton droit de la souris sur le certificat de l'autorité de certification et sélectionnez **toutes les tâches** > **gérer les clés privées**.
   g. Cliquez sur **Ajouter**, dans l'assistant Sélectionner les utilisateurs et les groupes, modifiez l'emplacement en nom d'ordinateur local (en haut de la hiérarchie)
   h. Ajoutez l'utilisateur IIS AppPool\SnapCenter et donnez des autorisations de contrôle total.
3. Pour l'autorisation IIS * de certificat CA, ajoutez la nouvelle entrée de clés de Registre DWORD dans le serveur SnapCenter à partir du chemin suivant :

   Dans l'éditeur du Registre Windows, parcourez jusqu'au chemin mentionné ci-dessous.

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv ders\SCHANNEL
   ```

4. Créez une nouvelle entrée de clé de Registre DWORD dans le contexte de la configuration du registre SCHANNEL.

   ```
   SendTrustedIssuerList = 0
   ```

```
ClientAuthTrustMode = 2
```

Configurez le plug-in Windows SnapCenter pour une communication SSL bidirectionnelle

Vous devez configurer le plug-in Windows SnapCenter pour une communication SSL bidirectionnelle à l'aide des commandes PowerShell.

Avant de commencer

Assurez-vous que l'empreinte du certificat CA est disponible.

Étapes

1. Pour lier le port, effectuez les actions suivantes sur l'hôte du plug-in Windows pour le port SMCore 8145 (par défaut).

   a. Supprimez la liaison de port de certificat autosignée SnapCenter existante à l'aide de la commande PowerShell suivante.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
      ```

      Par exemple :

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145
      ```

   b. Liez le nouveau certificat d'autorité de certification fourni au port SMCore.

      ```
      > $cert = "<CA_certificate thumbprint>"

      > $guid = [guid]::NewGuid().ToString("B")

      > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
      appid="$guid" clientcertnegotiation=enable
      verifyclientcertrevocation=disable

      > netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
      ```

      Par exemple :

      ```
      > $cert = "abc123abc123abc123abc123"

      > $guid = [guid]::NewGuid().ToString("B")

      > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
      clientcertnegotiation=enable verifyclientcertrevocation=disable

  > netsh http show sslcert ipport=0.0.0.0:8145
      ```

Activez la communication SSL bidirectionnelle

Vous pouvez activer la communication SSL bidirectionnelle pour sécuriser la communication mutuelle entre le serveur SnapCenter et les plug-ins à l'aide des commandes PowerShell.

Avant de commencer

Exécutez d'abord les commandes de tous les plug-ins et de l'agent SMCore, puis de serveur.

Étapes

1. Pour activer la communication SSL bidirectionnelle, exécutez les commandes suivantes sur le serveur SnapCenter pour les plug-ins, le serveur et pour chacun des agents pour lesquels la communication SSL bidirectionnelle est requise.

   ```
   > Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
   -HostName <Plugin_HostName>

   > Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
   -HostName localhost

   > Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
   ```

2. Exécutez l'opération de recyclage du pool d'applications SnapCenter IIS à l'aide de la commande suivante.
   ```
   > Restart-WebAppPool -Name "SnapCenter"
   ```
3. Pour les plug-ins Windows, redémarrez le service SMCore en exécutant la commande PowerShell suivante :

   ```
   > Restart-Service -Name SnapManagerCoreService
   ```

Désactiver la communication SSL bidirectionnelle

Vous pouvez désactiver la communication SSL bidirectionnelle à l'aide des commandes PowerShell.

À propos de cette tâche

- Exécutez d'abord les commandes de tous les plug-ins et de l'agent SMCore, puis de serveur.
- Lorsque vous désactivez la communication SSL bidirectionnelle, le certificat de l'autorité de certification et sa configuration ne sont pas supprimés.
- Pour ajouter un nouvel hôte au serveur SnapCenter, vous devez désactiver le protocole SSL bidirectionnel pour tous les hôtes de plug-in.
- NLB et F5 ne sont pas pris en charge.

Étapes

1. Pour désactiver la communication SSL bidirectionnelle, exécutez les commandes suivantes sur le serveur SnapCenter pour tous les hôtes de plug-in et l'hôte SnapCenter.

   ```
   > Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
   -HostName <Agent_HostName>
   ```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. Exécutez l'opération de recyclage du pool d'applications SnapCenter IIS à l'aide de la commande suivante.
   ```
   > Restart-WebAppPool -Name "SnapCenter"
   ```
3. Pour les plug-ins Windows, redémarrez le service SMCore en exécutant la commande PowerShell suivante :

   ```
   > Restart-Service -Name SnapManagerCoreService
   ```

Informations sur le copyright

Informations sur les marques commerciales