Configurare e abilitare la comunicazione SSL bidirezionale

SnapCenter Software 5.0

NetApp
July 18, 2024

Sommario

Configurare e abilitare la comunicazione SSL bidirezionale

Configurare la comunicazione SSL bidirezionale

È necessario configurare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra il server SnapCenter e i plug-in.

Prima di iniziare

- Il file CSR del certificato CA dovrebbe essere stato generato con la lunghezza minima supportata della chiave di 3072.
- Il certificato CA deve supportare l'autenticazione del server e l'autenticazione del client.
- È necessario disporre di un certificato CA con chiave privata e dettagli di identificazione personale.
- La configurazione SSL unidirezionale dovrebbe essere stata attivata.

  Per ulteriori informazioni, vedere "Sezione Configure CA certificate (Configura certificato CA)."

- È necessario attivare la comunicazione SSL bidirezionale su tutti gli host plug-in e sul server SnapCenter.

  L'ambiente con alcuni host o server non abilitati per la comunicazione SSL bidirezionale non è supportato.

Fasi

1. Per eseguire il binding della porta, attenersi alla seguente procedura sull'host del server SnapCenter per la porta 8146 del server Web IIS SnapCenter (impostazione predefinita) e ancora per la porta 8145 SMCore (impostazione predefinita) utilizzando i comandi PowerShell.

   a. Rimuovere il binding della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

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

      Ad esempio,

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

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

   b. Associare il certificato CA appena procurato al server SnapCenter e alla porta 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>
      ```

Ad esempio,

```
> $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. Per accedere all'autorizzazione al certificato CA, aggiungere l'utente predefinito del server Web IIS di SnapCenter "**IIS AppPool/SnapCenter**" nell'elenco delle autorizzazioni del certificato eseguendo la procedura seguente per accedere al certificato CA appena procurato.
   a. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi SnapIn**.
   b. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
   c. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
   d. Fare clic su **Directory principale console** > **certificati – computer locale** > **personale** > **certificati**.
   e. Selezionare il certificato SnapCenter.
   f. Per avviare l'aggiunta guidata autorizzazioni utente, fare clic con il pulsante destro del mouse sul certificato CA e selezionare **tutte le attività** > **Gestisci chiavi private**.
   g. Fare clic su **Aggiungi**, nella procedura guidata Seleziona utenti e gruppi modificare la posizione in Nome computer locale (in alto nella gerarchia)
   h. Aggiungere l'utente di IIS AppPool/SnapCenter, assegnare autorizzazioni di controllo complete.
3. Per l'autorizzazione IIS * del certificato CA, aggiungere la nuova voce delle chiavi di registro DWORD nel server SnapCenter dal seguente percorso:

   Nell'editor del Registro di sistema di Windows, passare al percorso indicato di seguito,

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

4. Creare una nuova voce della chiave del Registro di sistema DWORD nel contesto della configurazione DEL Registro DI sistema SCHANNEL.

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

Configurare il plug-in Windows di SnapCenter per la comunicazione SSL bidirezionale

È necessario configurare il plug-in Windows di SnapCenter per la comunicazione SSL bidirezionale utilizzando i comandi PowerShell.

Prima di iniziare

Assicurarsi che il thumbprint del certificato CA sia disponibile.

Fasi

1. Per collegare la porta, eseguire le seguenti operazioni sull'host plug-in di Windows per la porta SMCore 8145 (impostazione predefinita).

   a. Rimuovere il binding della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

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

      Ad esempio,

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

   b. Associare il certificato CA appena procurato alla porta 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>
      ```

      Ad esempio,

      ```
      > $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
      ```

Abilitare la comunicazione SSL bidirezionale

È possibile abilitare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra il server SnapCenter e i plug-in utilizzando i comandi PowerShell.

Prima di iniziare

Eseguire i comandi per tutti i plug-in e l'agente SMCore prima e poi per il server.

Fasi

1. Per attivare la comunicazione SSL bidirezionale, eseguire i seguenti comandi sul server SnapCenter per i plug-in, il server e per ciascuno degli agenti per i quali è richiesta la comunicazione SSL bidirezionale.

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

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

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

2. Eseguire l'operazione di riciclo del pool di applicazioni IIS SnapCenter utilizzando il seguente comando. `> Restart-WebAppPool -Name "SnapCenter"`
3. Per i plug-in di Windows, riavviare il servizio SMCore eseguendo il seguente comando PowerShell:

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

Disattiva la comunicazione SSL bidirezionale

È possibile disattivare la comunicazione SSL bidirezionale utilizzando i comandi PowerShell.

A proposito di questa attività

- Eseguire i comandi per tutti i plug-in e l'agente SMCore prima e poi per il server.
- Quando si disattiva la comunicazione SSL bidirezionale, il certificato CA e la relativa configurazione non vengono rimossi.
- Per aggiungere un nuovo host al server SnapCenter, è necessario disattivare il protocollo SSL bidirezionale per tutti gli host plug-in.
- NLB e F5 non sono supportati.

Fasi

1. Per disattivare la comunicazione SSL bidirezionale, eseguire i seguenti comandi sul server SnapCenter per tutti gli host plug-in e l'host 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. Eseguire l'operazione di riciclo del pool di applicazioni IIS SnapCenter utilizzando il seguente comando. `> Restart-WebAppPool -Name "SnapCenter"`

3. Per i plug-in di Windows, riavviare il servizio SMCore eseguendo il seguente comando PowerShell:

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