在 Windows 主機上設定並啟用雙向 SSL 通信

SnapCenter software

NetApp
November 06, 2025

目錄

在 Windows 主機上設定並啟用雙向 SSL 通信 1
在 Windows 主機上設定雙向 SSL 通信 1
配置SnapCenter Windows 插件以進行雙向 SSL 通信 2
在 Windows 主機上啟用雙向 SSL 通信 3
禁用雙向 SSL 通信 4

在 Windows 主機上設定並啟用雙向 SSL 通信

在 Windows 主機上設定雙向 SSL 通信

您應該配置雙向 SSL 通訊以保護 Windows 主機上的SnapCenter伺服器與插件之間的相互通訊。

開始之前

- 您應該已經產生了具有最小支援金鑰長度 3072 的 CA 憑證 CSR 檔案。
- CA憑證應支援伺服器認證和用戶端認證。
- 您應該擁有一份包含私鑰和指紋詳細資訊的 CA 憑證。
- 您應該已經啟用單向 SSL 設定。

  有關詳細信息，請參閱 "配置CA憑證部分。"

- 您必須在所有插件主機和SnapCenter伺服器上啟用雙向 SSL 通訊。

  不支援某些主機或伺服器未啟用雙向 SSL 通訊的環境。

步驟

1. 若要綁定端口，請使用 PowerShell 命令在SnapCenter Server 主機上對SnapCenter IIS Web 伺服器連接埠 8146（預設）執行下列步驟，並再次對 SMCore 連接埠 8145（預設）執行下列步驟。

   a. 使用下列 PowerShell 指令刪除現有的SnapCenter自簽章憑證連接埠綁定。

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

      例如，

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

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

   b. 將新購買的 CA 憑證與SnapCenter伺服器和 SMCore 連接埠綁定。

      ```
      > $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>
      ```

      例如，

      ```
      > $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. 若要存取 CA 憑證的權限，請透過執行下列步驟在憑證權限清單中新增 SnapCenter 的預設 IIS Web 伺服器使用者「**IIS AppPool\ SnapCenter**」來存取新購買的 CA 憑證。
   a. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
   b. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
   c. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
   d. 按一下 控制台根 > 憑證 - 本機 > 個人 > 憑證。
   e. 選擇SnapCenter證書。
   f. 若要啟動新增使用者\權限精靈，請以滑鼠右鍵按一下 CA 憑證並選擇 所有任務 > 管理私密金鑰。
   g. 按一下“新增”，在“選取使用者和群組”精靈中將位置變更為本機電腦名稱（層次結構中的最頂層）
   h. 新增 IIS AppPool\ SnapCenter用戶，授予完全控制權限。
3. 對於 **CA** 憑證 **IIS** 權限，從下列路徑在SnapCenter Server 中新增新的 DWORD 登錄項目項目：

   在 Windows 登錄編輯器中，遍歷下面提到的路徑，

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

4. 在 SCHANNEL 註冊表配置上下文中建立新的 DWORD 註冊表項條目。

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

配置**SnapCenter Windows** 插件以進行雙向 **SSL** 通信

您應該使用 PowerShell 命令設定SnapCenter Windows 插件以進行雙向 SSL 通訊。

開始之前

確保 CA 憑證指紋可用。

步驟

1. 若要綁定端口，請在 Windows 插件主機上對 SMCore 連接埠 8145（預設）執行下列操作。

a. 使用下列 PowerShell 指令刪除現有的SnapCenter自簽章憑證連接埠綁定。

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

例如，

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

b. 將新購買的CA憑證與SMCore連接埠綁定。

```
> $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>
```

例如，

```
> $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
```

在 Windows 主機上啟用雙向 SSL 通信

您可以啟用雙向 SSL 通信，以使用 PowerShell 命令保護 Windows 主機上的SnapCenter伺服器與插件之間的相互通訊。

開始之前

首先執行所有插件和 SMCore 代理的命令，然後執行伺服器的命令。

步驟

1. 若要啟用雙向 SSL 通信，請在SnapCenter伺服器上執行下列命令，用於插件、伺服器以及需要雙向 SSL 通訊的每個代理程式。

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

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

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

2. 使用下列命令執行 IIS SnapCenter應用程式集區回收作業。 `> Restart-WebAppPool -Name "SnapCenter"`
3. 對於 Windows 插件，透過執行下列 PowerShell 命令重新啟動 SMCore 服務：

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

禁用雙向 SSL 通信

您可以使用 PowerShell 指令停用雙向 SSL 通訊。

關於此任務

- 首先執行所有插件和 SMCore 代理的命令，然後執行伺服器的命令。
- 當您停用雙向 SSL 通訊時，CA 憑證及其配置不會被刪除。
- 若要為SnapCenter Server 新增主機，必須停用所有插件主機的雙向 SSL。
- 不支援 NLB 和 F5。

步驟

1. 若要停用雙向 SSL 通信，請在SnapCenter Server 上對所有插件主機和SnapCenter主機執行下列命令。

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

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

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

2. 使用下列命令執行 IIS SnapCenter應用程式集區回收作業。 `> Restart-WebAppPool -Name "SnapCenter"`
3. 對於 Windows 插件，透過執行下列 PowerShell 命令重新啟動 SMCore 服務：

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

版權資訊

商標資訊