# 配置并启用双向SSL通信

SnapCenter Software 5.0

NetApp
April 04, 2024

# 目录

# 配置并启用双向SSL通信

## 配置双向SSL通信

您应配置双向SSL通信、以确保SnapCenter服务器与插件之间的相互通信安全。

- 开始之前 *
- 您应已生成支持的最小密钥长度为3072的CA证书CSR文件。
- CA证书应支持服务器身份验证和客户端身份验证。
- 您应拥有一个CA证书、其中应包含私钥和指纹详细信息。
- 您应已启用单向SSL配置。

  有关详细信息，请参见 "配置CA证书部分。"

- 您必须已在所有插件主机和SnapCenter服务器上启用双向SSL通信。

  不支持某些主机或服务器未启用双向SSL通信的环境。

- 步骤 *

  1. 要绑定此端口、请在SnapCenter服务器主机上对SnapCenter IIS Web服务器端口8146 (默认)执行以下步骤、并使用PowerShell命令对SMCore端口8145 (默认)再次执行以下步骤。

     a. 使用以下PowerShell命令删除现有SnapCenter自签名证书端口绑定。

     ```
     > 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. 将新获取的CA证书与SnapCenter服务器和SMCore端口绑定。

     ```
     > $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. 要访问CA证书的权限、请执行以下步骤以访问新购买的CA证书、从而将SnapCenter的默认IIS Web服务器用户"**IIS AppPoool\SnapCenter**"添加到证书权限列表中。
   a. 转到Microsoft管理控制台(MMC)，然后单击*File*>*Add/Remove snapin。
   b. 在添加或删除管理单元窗口中，选择 * 证书 * ，然后单击 * 添加 * 。
   c. 在证书管理单元窗口中，选择 * 计算机帐户 * 选项，然后单击 * 完成 * 。
   d. 单击*控制台根*>*证书–本地计算机*>*个人*>*证书*。
   e. 选择SnapCenter证书。
   f. 要启动添加用户\权限向导，请右键单击CA证书，然后选择*All Tasks*>*Manage private keys*。
   g. 单击*Add*，在Select Users and Groups (选择用户和组)向导中将位置更改为本地计算机名称(层次结构中最顶端)
   h. 添加IIS Appool\SnapCenter用户、授予完全控制权限。
3. 对于*CA证书IIS权限*，从以下路径在SnapCenter服务器中添加新的DWORD注册表项条目：

   在Windows注册表编辑器中，遍历以下路径：

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

4. 在Schchannel注册表配置环境下创建新的DWORD注册表项条目。

   ```
   SendTrustedIssuerList = 0
   ```

```
ClientAuthTrustMode = 2
```

## 配置**SnapCenter Windows**插件以实现双向**SSL**通信

您应使用PowerShell命令配置SnapCenter Windows插件以实现双向SSL通信。

- 开始之前 *

确保CA证书指纹可用。

- 步骤 *

1. 要绑定端口、请在Windows插件主机上对SMCore端口8145 (默认)执行以下操作。

   a. 使用以下PowerShell命令删除现有SnapCenter自签名证书端口绑定。

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

   例如：

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

   b. 将新获得的CA证书与SMCore端口绑定。

   ```
   > $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
```

# 启用双向SSL通信

## 您可以使用PowerShell命令启用双向SSL通信、以确保SnapCenter服务器与插件之间的相互通信安全。

- 开始之前 *

先对所有插件和SMCore代理执行命令、然后再对服务器执行命令。

- 步骤 *

1. 要启用双向SSL通信、请在SnapCenter服务器上为需要双向SSL通信的插件、服务器和每个代理运行以下命令。

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

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

```
-HostName localhost
```

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

1. 使用以下命令执行IIS SnapCenter应用程序池回收操作。 `> Restart-WebAppPool -Name "SnapCenter"`
2. 对于Windows插件、运行以下PowerShell命令重新启动SMCore服务：

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

## 禁用双向SSL通信

您可以使用PowerShell命令禁用双向SSL通信。

- 关于此任务 *
- 先对所有插件和SMCore代理执行命令、然后再对服务器执行命令。
- 禁用双向SSL通信时、不会删除CA证书及其配置。
- 要向SnapCenter服务器添加新主机、必须对所有插件主机禁用双向SSL。
- 不支持NLB和F5。
- 步骤 *

1. 要禁用双向SSL通信、请在SnapCenter服务器上对所有插件主机和SnapCenter主机运行以下命令。

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

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

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

1. 使用以下命令执行IIS SnapCenter应用程序池回收操作。 `> Restart-WebAppPool -Name "SnapCenter"`
2. 对于Windows插件、运行以下PowerShell命令重新启动SMCore服务：

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