配置并启用双向SSL通信

SnapCenter Software 4.9

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/snapcenter-49/install/task_configure_two_way_ssl.html on September 26, 2025. Always check docs.netapp.com for the latest.

目录

配置并启用双向SSL通信 1
配置双向SSL通信 1
配置SnapCenter Windows插件以实现双向SSL通信 2
启用双向SSL通信 3
禁用双向SSL通信 4

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
```

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。