



配置 **CA** 证书 SnapCenter software

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/snapcenter-61/protect-nsp/generate_CA_certificate_CSR_file.html on November 06, 2025. Always check docs.netapp.com for the latest.

目录

- 配置 CA 证书 1
 - 生成CA证书CSR文件 1
 - 导入 CA 证书 1
 - 获取 CA 证书指纹 2
 - 使用 Windows 主机插件服务配置 CA 证书 2
 - 为 Linux 主机上NetApp支持的插件服务配置 CA 证书 3
 - 管理插件密钥库的密码以及正在使用的 CA 签名密钥对的别名 3
 - 配置根证书或中间证书以插入信任库 4
 - 配置 CA 签名密钥对以插入信任库 4
 - 为插件配置证书吊销列表 (CRL) 5
 - 在 Windows 主机上为NetApp支持的插件服务配置 CA 证书 5
 - 管理插件密钥库的密码以及正在使用的 CA 签名密钥对的别名 5
 - 配置根证书或中间证书以插入信任库 6
 - 配置 CA 签名密钥对以插入信任库 6
 - 为SnapCenter插件配置证书吊销列表 (CRL) 7
 - 为插件启用 CA 证书 7

配置 CA 证书

生成CA证书CSR文件

您可以生成证书签名请求 (CSR) 并导入可使用生成的 CSR 从证书颁发机构 (CA) 获取的证书。该证书将有一个与之关联的私钥。

CSR 是一段编码文本，提供给授权证书供应商以获取签名的 CA 证书。



CA 证书 RSA 密钥长度必须至少为 3072 位。

有关生成 CSR 的信息，请参阅 ["如何生成CA证书CSR文件"](#)。



如果您拥有您的域 (*.domain.company.com) 或您的系统 (machine1.domain.company.com) 的 CA 证书，您可以跳过生成 CA 证书 CSR 文件。您可以使用SnapCenter部署现有的 CA 证书。

对于集群配置，CA 证书中应提及集群名称（虚拟集群 FQDN）和相应的主机名。在获取证书之前，可以通过填写主题备用名称 (SAN) 字段来更新证书。对于通配符证书 (*.domain.company.com)，该证书将隐式包含域的所有主机名。

导入 CA 证书

您必须使用 Microsoft 管理控制台 (MMC) 将 CA 证书导入SnapCenter服务器和 Windows 主机插件。

步骤

1. 转到 Microsoft 管理控制台 (MMC)，然后单击 文件 > 添加/删除管理单元。
2. 在“添加或删除管理单元”窗口中，选择“证书”，然后单击“添加”。
3. 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”。
4. 单击 控制台根 > 证书 - 本地计算机 > 受信任的根证书颁发机构 > 证书。
5. 右键单击文件夹“受信任的根证书颁发机构”，然后选择*所有任务*>*导入*以启动导入向导。
6. 完成向导，如下所示：

在此向导窗口中...	执行以下操作...
导入私钥	选择选项*是*，导入私钥，然后单击*下一步*。
导入文件格式	不做任何更改；单击“下一步”。
安全性	指定导出证书要使用的新密码，然后单击“下一步”。
完成证书导入向导	查看摘要，然后单击“完成”开始导入。



导入证书时需携带私钥（支持格式为：**.pfx**、**.p12**、***.p7b**）。

7. 对“个人”文件夹重复步骤 5。

获取 CA 证书指纹

证书指纹是用于标识证书的十六进制字符串。指纹是使用指纹算法根据证书内容计算出来的。

步骤

1. 在 GUI 上执行以下操作：

- a. 双击该证书。
- b. 在证书对话框中，单击“详细信息”选项卡。
- c. 滚动浏览字段列表并单击“指纹”。
- d. 从框中复制十六进制字符。
- e. 删除十六进制数之间的空格。

例如，如果指纹为：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，删除空格后，将为：“a909502dd82ae41433e6f83886b00d4277a32a7b”。

2. 从 PowerShell 执行以下操作：

- a. 运行以下命令列出已安装证书的指纹并通过主题名称识别最近安装的证书。

```
Get-ChildItem -Path 证书:\LocalMachine\My
```

- b. 复制指纹。

使用 Windows 主机插件服务配置 CA 证书

您应该使用 Windows 主机插件服务配置 CA 证书以激活已安装的数字证书。

在 SnapCenter 服务器和所有已部署 CA 证书的插件主机上执行以下步骤。

步骤

1. 通过运行以下命令删除与 SMCore 默认端口 8145 的现有证书绑定：

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}>
```

例如：

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

- 通过运行以下命令将新安装的证书与 Windows 主机插件服务绑定：

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

为 Linux 主机上NetApp支持的插件服务配置 CA 证书

您应该管理插件密钥库及其证书和密码，配置 CA 证书，将根证书或中间证书配置到插件信任库，并使用SnapCenter插件服务将 CA 签名密钥对配置到插件信任库以激活已安装的数字证书。

插件使用位于 `/opt/NetApp/snapcenter/scc/etc` 的文件“keystore.jks”作为其信任库和密钥库。

管理插件密钥库的密码以及正在使用的 CA 签名密钥对的别名

步骤

1. 您可以从插件代理属性文件中检索插件密钥库默认密码。

它是与密钥“KEYSTORE_PASS”对应的值。

2. 更改密钥库密码：

```
keytool -storepasswd -keystore keystore.jks  
. 将密钥库中所有私钥条目别名的密码更改为与密钥库相同的密码：
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

对 `agent.properties` 文件中的密钥 KEYSTORE_PASS 进行相同的更新。

3. 修改密码后重启服务。



插件密钥库的密码和私钥的所有相关别名的密码应该相同。

配置根证书或中间证书以插入信任库

您应该配置没有私钥的根证书或中间证书来插入信任库。

步骤

1. 导航到包含插件密钥库的文件夹：`/opt/ NetApp/snapcenter/scc/etc`。
2. 找到文件“`keystore.jks`”。
3. 列出密钥库中添加的证书：

```
keytool -list -v -keystore keystore.jks
```

4. 添加根证书或中间证书：

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. 配置根证书或中间证书以插入信任库后重新启动服务。
```



您应该添加根 CA 证书，然后添加中间 CA 证书。

配置 CA 签名密钥对以插入信任库

您应该将 CA 签名的密钥对配置到插件信任库。

步骤

1. 导航到包含插件密钥库 `/opt/ NetApp/snapcenter/scc/etc` 的文件夹。
2. 找到文件“`keystore.jks`”。
3. 列出密钥库中添加的证书：

```
keytool -list -v -keystore keystore.jks
```

4. 添加具有私钥和公钥的 CA 证书。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 列出密钥库中添加的证书。

```
keytool -list -v -keystore keystore.jks
```

6. 验证密钥库是否包含与添加到密钥库的新 CA 证书相对应的别名。
7. 将添加的CA证书私钥密码更改为keystore密码。

默认插件密钥库密码是 `agent.properties` 文件中密钥 `KEYSTORE_PASS` 的值。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

• 如果CA证书中的别名较长，且包含空格或特殊字符（“*”，“，”，“）”，请将别名修改为简单名称：

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

• 在 `agent.properties` 文件中配置来自 CA 证书的别名。

根据键 `SCC_CERTIFICATE_ALIAS` 更新此值。

8. 配置 CA 签名密钥对以插入信任库后重新启动服务。

为插件配置证书吊销列表 (CRL)

关于此任务

- SnapCenter插件将在预配置的目录中搜索 CRL 文件。
- SnapCenter插件的 CRL 文件的默认目录是“`opt/ NetApp/snapcenter/scc/etc/crl`”。

步骤

1. 您可以根据键 `CRL_PATH` 修改和更新 `agent.properties` 文件中的默认目录。

您可以在此目录中放置多个 CRL 文件。将根据每个 CRL 验证传入的证书。

在 Windows 主机上为NetApp支持的插件服务配置 CA 证书

您应该管理插件密钥库及其证书和密码，配置 CA 证书，将根证书或中间证书配置到插件信任库，并使用SnapCenter插件服务将 CA 签名密钥对配置到插件信任库以激活已安装的数字证书。

插件使用位于 `C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc` 的文件 `keystore.jks` 作为其信任库和密钥库。

管理插件密钥库的密码以及正在使用的 CA 签名密钥对的别名

步骤

1. 您可以从插件代理属性文件中检索插件密钥库默认密码。

它是与密钥 `_KEYSTORE_PASS_` 对应的值。

2. 更改密钥库密码：

```
keytool -storepasswd -keystore 密钥库.jks
```



如果 Windows 命令提示符无法识别“keytool”命令，请将 keytool 命令替换为其完整路径。

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe"-storepasswd -keystore keystore.jks
```

3. 将密钥库中所有私钥条目别名的密码更改为与密钥库相同的密码：

```
keytool -keypasswd -alias“别名在证书中”-keystore keystore.jks
```

对 *agent.properties* 文件中的密钥 KEYSTORE_PASS 进行相同的更新。

4. 修改密码后重启服务。



插件密钥库的密码和私钥的所有相关别名的密码应该相同。

配置根证书或中间证书以插入信任库

您应该配置没有私钥的根证书或中间证书来插入信任库。

步骤

1. 导航到包含插件密钥库的文件夹 *C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc*
2. 找到文件“keystore.jks”。
3. 列出密钥库中添加的证书：

```
keytool -list -v -keystore keystore.jks
```

4. 添加根证书或中间证书：

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. 配置根证书或中间证书以插入信任库后重新启动服务。



您应该添加根 CA 证书，然后添加中间 CA 证书。

配置 CA 签名密钥对以插入信任库

您应该将 CA 签名的密钥对配置到插件信任库。

步骤

1. 导航到包含插件密钥库的文件夹 *C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc*
2. 找到文件 *_keystore.jks_*。
3. 列出密钥库中添加的证书：

```
keytool -list -v -keystore keystore.jks
```

4. 添加具有私钥和公钥的 CA 证书。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```


5. 列出密钥库中添加的证书。

```
keytool -list -v -keystore keystore.jks
```

6. 验证密钥库是否包含与添加到密钥库的新 CA 证书相对应的别名。
7. 将添加的CA证书私钥密码更改为keystore密码。

默认插件密钥库密码是 agent.properties 文件中密钥 KEYSTORE_PASS 的值。

```
keytool -keypasswd -alias“别名在CA证书中的名称”-keystore keystore.jks
```

8. 在_agent.properties_文件中配置来自CA证书的别名。

根据键 SCC_CERTIFICATE_ALIAS 更新此值。

9. 配置 CA 签名密钥对以插入信任库后重新启动服务。

为SnapCenter插件配置证书吊销列表 (CRL)

关于此任务

- 要下载相关 CA 证书的最新 CRL 文件，请参阅 ["如何更新SnapCenter CA 证书中的证书吊销列表文件"](#)。
- SnapCenter插件将在预配置的目录中搜索 CRL 文件。
- SnapCenter插件的 CRL 文件的默认目录是 'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'。

步骤

1. 您可以根据键 CRL_PATH 修改和更新 agent.properties 文件中的默认目录。
2. 您可以在此目录中放置多个 CRL 文件。

将根据每个 CRL 验证传入的证书。

为插件启用 CA 证书

您应该配置 CA 证书并在SnapCenter服务器和相应的插件主机中部署 CA 证书。您应该为插件启用 CA 证书验证。

开始之前

- 您可以使用运行_Set-SmCertificateSettings_ cmdlet 来启用或禁用 CA 证书。
- 您可以使用_Get-SmCertificateSettings_显示插件的证书状态。

可以通过运行_Get-Help command_name_来获取有关可与 cmdlet 一起使用的参数及其描述的信息。或者，您也可以参考 ["SnapCenter软件 Cmdlet 参考指南"](#)。

步骤

1. 在左侧导航窗格中，单击“主机”。
2. 在“主机”页面中，单击“托管主机”。

3. 选择单个或多个插件主机。
4. 单击“更多选项”。
5. 选择*启用证书验证*。

完成后

托管主机选项卡主机显示一个挂锁，挂锁的颜色表示SnapCenter服务器和插件主机之间的连接状态。

- *  * 表示 CA 证书未启用或未分配给插件主机。
- *  * 表示 CA 证书验证成功。
- *  * 表示无法验证 CA 证书。
- *  * 表示无法检索连接信息。



当状态为黄色或绿色时，表示数据保护操作成功完成。

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。