配置 CA 证书

SnapCenter Software 5.0

NetApp
July 18, 2024

目录

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。此证书将具有一个关联的专用密钥。

CSR 是一个编码文本块，提供给授权证书供应商以采购签名的 CA 证书。

CA证书RSA密钥长度应至少为3072位。

有关生成CSR的信息，请参见 "如何生成 CA 证书 CSR 文件"。

如果您拥有域（ * .domain.company.com ）或系统（ machine1.domain.company.com ）的 CA 证书，则可以跳过生成 CA 证书 CSR 文件。您可以使用 SnapCenter 部署现有 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 ）以及相应的主机名。在获取证书之前，可以通过填写使用者替代名称（ SAN ）字段来更新此证书。对于通配符证书（ * .domain.company.com ），此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 证书导入到 SnapCenter 服务器和 Windows 主机插件中。

步骤

1. 转到 Microsoft 管理控制台（ MMC ），然后单击 * 文件 * > * 添加 / 删除 Snapin * 。
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 * > * 可信根证书颁发机构 * > * 证书 * 。
5. 右键单击文件夹 " 可信根证书颁发机构 " ，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 * 是 * 选项，导入私钥，然后单击 * 下一步 * 。
导入文件格式	不进行任何更改；单击 * 下一步 * 。
安全性	指定要用于导出的证书的新密码，然后单击 * 下一步 * 。
正在完成证书导入向导	查看摘要，然后单击 * 完成 * 开始导入。

导入证书应与私钥捆绑在一起(支持的格式为：。**pfx**、。p12和*。p7b)。

7. 对 "Personal" 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得出的。

步骤

1. 在 GUI 上执行以下操作：
   a. 双击证书。
   b. 在证书对话框中，单击 * 详细信息 * 选项卡。
   c. 滚动字段列表，然后单击 * 缩略图 * 。
   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" ，则在删除空格后，指纹将为 "a909502dd82ae41433e6f83886b00d4277a32a7b" 。

2. 从 PowerShell 执行以下操作：
   a. 运行以下命令以列出已安装证书的指纹，并按主题名称标识最近安装的证书。

      *Get-*子 项 *-Path Cert* ： *\LOCALLMACHINE\My*

   b. 复制指纹。

使用 Windows 主机插件服务配置 CA 证书

您应使用 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 服务器以及已部署 CA 证书的所有插件主机上执行以下步骤。

步骤

1. 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
   ```

. 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"
```

在 Linux 主机上为 SnapCenter 自定义插件服务配置 CA 证书

您应管理自定义插件密钥库及其证书的密码，配置 CA 证书，为自定义插件信任存储配置根或中间证书，并将 CA 签名密钥对配置为使用 SnapCenter 自定义插件服务的自定义插件信任存储，以激活已安装的数字证书。

自定义插件使用文件 "keystore.jks" ，该文件位于 */opt/netapp/snapcenter/scc/ etc* ，同时用作其信任存储和密钥存储。

管理自定义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. 您可以从自定义插件代理属性文件中检索自定义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
. 将密钥库中私钥条目的所有别名的密码更改为密钥库使用的相同密码：
```

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

   为 *agent.properties* 文件中的 keystore_pass 密钥更新相同的。

3. 更改密码后重新启动服务。

自定义插件密钥库的密码和专用密钥的所有关联别名密码应相同。

将根证书或中间证书配置为自定义插件信任存储

您应将不带私钥的根证书或中间证书配置为自定义插件信任存储。

步骤

1. 导航到包含自定义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
```

. 将根证书或中间证书配置为自定义插件信任存储后重新启动服务。

您应先添加根 CA 证书，然后再添加中间 CA 证书。

将 CA 签名密钥对配置为自定义插件信任存储

您应将 CA 签名密钥对配置为自定义插件信任存储。

步骤

1. 导航到包含自定义插件密钥库 /opt/netapp/snapcenter/scc/ 等的文件夹
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. 添加同时具有私钥和公有密钥的 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已添加到密钥库中的新 CA 证书对应的别名。
7. 将为 CA 证书添加的私钥密码更改为密钥库密码。

   默认自定义插件密钥库密码是 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，并且包含空格或特殊字符（ "*" ， " ， "
），请将别名更改为简单名称：

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
```
. 从 agent.properties 文件中的 CA 证书配置别名。

根据密钥 SCC_certificate_alias 更新此值。

8. 将 CA 签名密钥对配置为自定义插件信任存储后重新启动服务。

为 SnapCenter 自定义插件配置证书撤消列表（ Certificate Revocation List ， CRL ）

关于此任务

- SnapCenter 自定义插件将在预配置的目录中搜索 CRL 文件。
- SnapCenter 自定义插件的 CRL 文件的默认目录为 " opt/netapp/snapcenter/SCC/etc/CRL" 。

步骤

1. 您可以使用密钥 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。系统将根据每个 CRL 验证传入的证书。

在 Windows 主机上为 SnapCenter 自定义插件服务配置 CA 证书

您应管理自定义插件密钥库及其证书的密码，配置 CA 证书，为自定义插件信任存储配置根或中间证书，并将 CA 签名密钥对配置为使用 SnapCenter 自定义插件服务的自定义插件信任存储，以激活已安装的数字证书。

自定义插件使用文件 *keystore.jks* ，该文件位于 *C： \Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc* ，同时用作其信任存储和密钥存储。

管理自定义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. 您可以从自定义插件代理属性文件中检索自定义插件密钥库默认密码。

   该值与 key_keystore_pass_ 键对应。

2. 更改密钥库密码：

   keytool -storepasswd -keystore keystore.jks

如果在 Windows 命令提示符处无法识别 "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. 将密钥库中私钥条目的所有别名的密码更改为密钥库使用的相同密码：

   keytool -keypasswd -alias "alias_name_in_ct" -keystore keystore.jks

   为 *agent.properties* 文件中的 keystore_pass 密钥更新相同的。

4. 更改密码后重新启动服务。

   自定义插件密钥库的密码和专用密钥的所有关联别名密码应相同。

将根证书或中间证书配置为自定义插件信任存储

您应将不带私钥的根证书或中间证书配置为自定义插件信任存储。

步骤

1. 导航到包含自定义插件密钥库 *C： \Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\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. 添加根证书或中间证书：

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

5. 将根证书或中间证书配置为自定义插件信任存储后重新启动服务。

您应先添加根 CA 证书，然后再添加中间 CA 证书。

将 **CA** 签名密钥对配置为自定义插件信任存储

您应将 CA 签名密钥对配置为自定义插件信任存储。

步骤

1. 导航到包含自定义插件密钥库 *C： \Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\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. 添加同时具有私钥和公有密钥的 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已添加到密钥库中的新 CA 证书对应的别名。
7. 将为 CA 证书添加的私钥密码更改为密钥库密码。

   默认自定义插件密钥库密码是 agent.properties 文件中密钥 keystore_pass 的值。

   keytool -keypasswd -alias "alias_name_in_CA_ct" -keystore keystore.jks

8. 从 *agent.properties* 文件中的 CA 证书配置别名。

   根据密钥 SCC_certificate_alias 更新此值。

9. 将 CA 签名密钥对配置为自定义插件信任存储后重新启动服务。

为 **SnapCenter** 自定义插件配置证书撤消列表（ **Certificate Revocation List** ， **CRL** ）

关于此任务

- 要下载相关CA证书的最新CRL文件，请参见 "如何更新 SnapCenter CA 证书中的证书撤消列表文件"。
- SnapCenter 自定义插件将在预配置的目录中搜索 CRL 文件。
- SnapCenter 自定义插件的 CRL 文件的默认目录为： *C* ： *\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\ etc\CRL'* 。

步骤

1. 您可以使用密钥 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。

   系统将根据每个 CRL 验证传入的证书。

为插件启用 **CA** 证书

您应在 SnapCenter 服务器和相应插件主机中配置 CA 证书并部署 CA 证书。您应为插件启用 CA 证书验证。

开始之前

- 您可以使用 run *set-SmCertificateSettings* cmdlet 启用或禁用 CA 证书。
- 您可以使用 *Get-SmCertificateSettings* 显示插件的证书状态。

有关可与 cmdlet 结合使用的参数及其说明的信息，可通过运行 *get-help command_name* 来获取。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 * 受管主机 * 。
3. 选择一个或多个插件主机。
4. 单击 * 更多选项 * 。
5. 选择 * 启用证书验证 * 。

完成后

受管主机选项卡主机会显示一个挂锁，挂锁的颜色表示 SnapCenter 服务器与插件主机之间的连接状态。

- ** 表示CA证书未启用、也未分配给插件主机。
- ** 表示CA证书已成功验证。
- ** 表示无法验证CA证书。
- ** 表示无法检索到连接信息。

> 如果状态为黄色或绿色，则表示数据保护操作已成功完成。