



配置基于证书的身份验证

SnapCenter Software 5.0

NetApp
July 18, 2024

目录

配置基于证书的身份验证	1
从SnapCenter服务器导出证书颁发机构(CA)证书	1
将证书颁发机构(Certificate Authority、CA)证书导入到Windows插件主机	1
将CA证书导入到UNIX主机插件、并将根证书或中间证书配置到SPL信任存储库	2
启用基于证书的身份验证	3

配置基于证书的身份验证

从SnapCenter服务器导出证书颁发机构(CA)证书

您应使用Microsoft管理控制台(MMC)将CA证书从SnapCenter服务器导出到插件主机。

开始之前

您应已配置双向SSL。

• 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*>*个人*>*证书*。
5. 右键单击用于SnapCenter服务器的已获得CA证书，然后选择*All Tasks*>*Export*以启动导出向导。
6. 在向导中执行以下操作。

对于此选项...	执行以下操作 ...
导出私钥	选择*否，不导出私钥*，然后单击*下一步*。
导出文件格式	单击 * 下一步 *。
文件名	单击*浏览*并指定保存证书的文件路径，然后单击*下一步*。
正在完成证书导出向导	查看摘要，然后单击 * 完成 * 开始导出。



SnapCenter HA配置和适用于VMware vSphere的SnapCenter插件不支持基于证书的身份验证。

将证书颁发机构(Certificate Authority、CA)证书导入到Windows插件主机

要使用导出的SnapCenter服务器CA证书、应使用Microsoft管理控制台(MMC)将相关证书导入到SnapCenter Windows插件主机。

• 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*>*个人*>*证书*。
5. 右键单击“个人”文件夹，然后选择*All Tasks*>*Import*以启动导入向导。
6. 在向导中执行以下操作。

对于此选项...	执行以下操作 ...
存储位置	单击 * 下一步 *。
要导入的文件	选择以.cer扩展名结尾的SnapCenter服务器证书。
证书存储	单击 * 下一步 *。
正在完成证书导出向导	查看摘要，然后单击 * 完成 * 开始导入。

将CA证书导入到UNIX主机插件、并将根证书或中间证书配置到SPL信任存储库

将CA证书导入到UNIX插件主机

您应将CA证书导入到UNIX插件主机中。

- 关于此任务 *
- 您可以管理SPL密钥库的密码以及正在使用的CA签名密钥对的别名。
- SPL密钥库的密码和专用密钥的所有关联别名密码应相同。
- 步骤 *
 1. 您可以从 SPL 属性文件检索 SPL 密钥库默认密码。它是与键对应的值 `SPL_KEYSTORE_PASS`。
 2. 更改密钥库密码：`$ keytool -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同一密码：`$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
 4. 对文件中的密钥`SPL_KEYSTORE_Pass`进行相同更新 `spl.properties``。
 5. 更改密码后重新启动服务。

配置根证书或中间证书以 SPL 信任存储

您应将根证书或中间证书配置为SPL信任存储库。您应先添加根 CA 证书，然后再添加中间 CA 证书。

- 步骤 *
 1. 导航到包含SPL密钥库的文件夹：`/var/opt/snapcenter/spl/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 <AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. 将根证书或中间证书配置为 SPL 信任存储后重新启动服务。

将 **CA** 签名密钥对配置为 **SPL** 信任存储

您应将CA签名密钥对配置为SPL信任存储库。

- 步骤 *

1. 导航到SPL密钥库所在的文件夹 `/var/opt/snapcenter/spl/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. 添加具有私钥和公共密钥的CA证书。 `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -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SPL密钥库密码是文件中SPL_KEYORE_PAASS密钥的值 `spl.properties`。

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
```

1. 如果CA证书中的别名较长且包含空格或特殊字符("*、"、")、请将别名更改为简单名称: `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks``
2. 从位于文件中的密钥库配置别名 `spl.properties`。根据密钥 `SPL_certificate_alias` 更新此值。
3. 将 CA 签名密钥对配置为 SPL 信任存储后重新启动服务。

启用基于证书的身份验证

要为SnapCenter服务器和Windows插件主机启用基于证书的身份验证、请运行以下PowerShell cmdlet。对于Linux插件主机、启用双向SSL后、将启用基于证书的身份验证。

- 启用基于客户端证书的身份验证:

```
Set-SmConfigSettings -Agent -configSettings @{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- 禁用基于客户端证书的身份验证:

```
Set-SmConfigSettings -Agent -configSettings  
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

版权信息

版权所有 © 2024 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。