



为Windows主机配置CA证书

SnapCenter Software 6.0

NetApp
July 23, 2024

目录

为Windows主机配置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
使用 SnapCenter 站点配置 CA 证书	3
为 SnapCenter 启用 CA 证书	3

为Windows主机配置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 : \LOCALMACHINE\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"
```

使用 SnapCenter 站点配置 CA 证书

您应在 Windows 主机上使用 SnapCenter 站点配置 CA 证书。

• 步骤 *

1. 在安装了 SnapCenter 的 Windows 服务器上打开 IIS 管理器。
2. 在左侧导航窗格中，单击 * 连接 *。
3. 展开服务器和 * 站点 * 的名称。
4. 选择要安装 SSL 证书的 SnapCenter 网站。
5. 导航到 * 操作 * > * 编辑站点 *，单击 * 绑定 *。
6. 在绑定页面中，选择 * 绑定 https *。
7. 单击 * 编辑 *。
8. 从 SSL 证书下拉列表中，选择最近导入的 SSL 证书。
9. 单击 * 确定 *。



已为 SnapCenter 计划程序站点(默认端口：8154、HTTPS)配置自签名证书。此端口正在 SnapCenter 服务器主机中进行通信、不强制配置 CA 证书。但是、如果您的环境要求您使用 CA 证书、请使用 SnapCenter 计划程序站点重复步骤 5 到 9。



如果最近部署的 CA 证书未在下拉菜单中列出，请检查此 CA 证书是否与专用密钥关联。



确保使用以下路径添加证书： * 控制台根 > 证书-本地计算机 > 可信根证书颁发机构 > 证书 *。

为 SnapCenter 启用 CA 证书

您应配置 CA 证书并为 SnapCenter 服务器启用 CA 证书验证。





开始之前

- 您可以使用 `Set-SmCertificateSettings` cmdlet 启用或禁用 CA 证书。
- 您可以使用 `Get-SmCertificateSettings` cmdlet 显示 SnapCenter 服务器的证书状态。

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. 在设置页面中，导航到 * 设置 * > * 全局设置 * > * CA 证书设置 *。
 2. 选择 * 启用证书验证 *。
 3. 单击 * 应用 *。
- 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。

-  表示未启用或未分配给插件主机的 CA 证书。
-  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。

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。