設定CA憑證

SnapCenter Software 5.0

NetApp
July 18, 2024

目錄

設定CA憑證

產生CA認證CSR檔案

您可以產生「憑證簽署要求」（CSR）、然後匯入可以使用產生的CSR從「憑證授權單位」（CA）取得的憑證。憑證將會有與其相關的私密金鑰。

CSR是編碼文字區塊、提供給授權憑證廠商以取得簽署的CA憑證。

CA 憑證 RSA 金鑰長度至少應為 3072 位元。

如需產生 CSR 的資訊、請參閱 "如何產生CA憑證CSR檔案"。

如果您擁有網域（*.domain.company.com）或系統（machine1.domain.company.com）的CA憑證、您可以跳過產生CA憑證CSR檔案的步驟。您可以使用SnapCenter 效益管理程式來部署現有的CA憑證。

對於叢集組態、叢集名稱（虛擬叢集FQDN）和各自的主機名稱應在CA憑證中提及。您可以在取得憑證之前填寫「Subject Alternative Name（SAN）（主體替代名稱（SAN））」欄位、以更新憑證。若為萬用字元憑證（*.domain.company.com）、憑證將會隱含包含網域的所有主機名稱。

匯入CA憑證

您必須SnapCenter 使用Microsoft管理主控台（MMC）、將CA憑證匯入到S倚賴 者支援的伺服器和Windows主機外掛程式。

步驟

1. 移至Microsoft管理主控台（MMC）、然後按一下*檔案*>*新增/移除Snapin *。
2. 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。
3. 在「憑證」嵌入式管理單元視窗中、選取「電腦帳戶」選項、然後按一下「完成」。
4. 按一下*主控台根目錄*>*憑證–本機電腦*>*信任的根憑證授權單位*>*憑證*。
5. 在「Trusted Root Certification Authorities」（受信任的根憑證授權單位）資料夾上按一下滑鼠右鍵、然後選取「* All Tasks」（所有工作）>「 Import」（匯入）以啟動匯入精靈。
6. 完成精靈、如下所示：

在此精靈視窗中...	請執行下列動作...
匯入私密金鑰	選取選項* Yes*、匯入私密金鑰、然後按一下* Next*。
匯入檔案格式	不做任何變更；按一下*下一步*。

在此精靈視窗中...	請執行下列動作...
安全性	指定匯出憑證所使用的新密碼、然後按一下*「下一步*」。
完成「憑證匯入精靈」	檢閱摘要、然後按一下「完成」開始匯入。

匯入憑證應與私密金鑰搭售（支援的格式為：。**pfx**、。p12和*。p7b）。

7. 對「Personal」資料夾重複步驟5。

取得CA憑證指紋

憑證指紋是用來識別憑證的十六進位字串。指紋是使用指紋演算法、從憑證內容中計算出來。

步驟

1. 在GUI上執行下列步驟：
   a. 按兩下憑證。
   b. 在「憑證」對話方塊中、按一下「詳細資料」索引標籤。
   c. 捲動欄位清單、然後按一下* Thumbprint*。
   d. 複製方塊中的十六進位字元。
   e. 移除十六進位數字之間的空格。

      例如、如果指紋為：「A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 d 42 77 A3 2a 7b」、則移除空格後、將會是：「a909502dd82ae41433e6f83886b00d4277a32a7b」。

2. 從PowerShell執行下列作業：
   a. 執行下列命令、列出已安裝憑證的指紋、並依主體名稱識別最近安裝的憑證。

      *Get-ChildItem*路徑認證：*\LocalComputer\My*

   b. 複製指紋。

使用Windows主機外掛程式服務設定CA憑證

您應該使用Windows主機外掛程式服務來設定CA憑證、以啟動安裝的數位憑證。

請在SnapCenter 已部署CA憑證的所有插件主機上執行下列步驟。

步驟

1. 執行下列命令、以SMCore預設連接埠8145移除現有的憑證繫結：

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

例如：

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

. 執行下列命令、將新安裝的憑證與Windows主機外掛程式服務連結：

```
> $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SnapCenter Linux主機上設定「CA憑證」以使用「支援整套自訂外掛程式」服務

您應該管理自訂外掛程式Keystore的密碼及其憑證、設定CA憑證、設定根或中繼憑證至自訂外掛程式信任存放區、以及設定CA簽署金鑰配對至自訂外掛程式信任存放區、並使用SnapCenter 「依賴自訂外掛程式」服務啟動已安裝的數位憑證。

自訂外掛程式會使用位於_/opt /NetApp/snapcenter/sccc/etc_的「keystore .jks」檔案做為其信任存放區和金鑰存放區。

管理自訂外掛程式Keystore的密碼、以及使用中的CA簽署金鑰配對別名

步驟

1. 您可以從自訂外掛程式代理程式內容檔擷取自訂外掛程式Keystore預設密碼。

   這是對應至金鑰「keystore _pass」的值。

2. 變更Keystore密碼：

```
 keytool -storepasswd -keystore keystore.jks
```

. 將Keystore中私密金鑰項目的所有別名密碼變更為與Keystore相同的密碼：

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

在_agent.properties_檔案中更新keyKeystore _pass的相同更新。

3. 變更密碼後重新啟動服務。

自訂外掛程式Keystore的密碼、以及私密金鑰的所有相關別名密碼均應相同。

將根或中繼憑證設定為自訂外掛程式信任存放區

您應該設定根或中繼憑證、而不使用私密金鑰、以自訂外掛程式信任存放區。

步驟

1. 瀏覽至包含自訂外掛程式Keystore的資料夾：/opp/NetApp/snapcenter/scc/等
2. 找到「keystore .jks」檔案。
3. 在Keystore中列出新增的憑證：

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

4. 新增根或中繼憑證：

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. 將根或中繼憑證設定為自訂外掛程式信任存放區之後、請重新啟動服務。
```

您應該先新增根CA憑證、然後再新增中繼CA憑證。

將CA簽署金鑰配對設定為自訂外掛程式信任存放區

您應該將CA簽署金鑰配對設定為自訂外掛程式信任存放區。

步驟

1. 瀏覽至包含自訂外掛程式Keystore /opp/NetApp/snapcenter/scc/等的資料夾
2. 找到「keystore .jks」檔案。
3. 在Keystore中列出新增的憑證：

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

4. 新增具有私密金鑰和公開金鑰的CA憑證。

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

5. 在Keystore中列出新增的憑證。

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

6. 驗證密鑰庫是否包含與新CA憑證對應的別名、該CA憑證已新增至金鑰庫。
7. 將CA憑證的新增私密金鑰密碼變更為金鑰庫密碼。

   預設的自訂外掛程式Keystore密碼是agent.properties檔案中KeyKeyKeystore _pass的值。

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

   . 如果CA憑證中的別名很長且包含空格或特殊字元（「
   *」、「」、」）、請將別名變更為簡單名稱：

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

   . 在agent.properties檔案中設定CA憑證的別名。

   請根據SCC_IDATure_ALIAS金鑰更新此值。

8. 將CA簽署金鑰配對設定為自訂外掛程式信任存放區之後、請重新啟動服務。

針對**SnapCenter** 「不一樣的自訂外掛程式」設定憑證撤銷清單（**CRL**）

關於這項工作

- 「自訂外掛程式」會在預先設定的目錄中搜尋CRL檔案。SnapCenter
- 適用於「SetcCustom Plug-in」的CRL檔案預設目錄SnapCenter 為「opt /NetApp/snapcenter/scc / etc/crl」。

步驟

1. 您可以根據金鑰CRP_path修改及更新agent.properties檔案中的預設目錄。

   您可以在此目錄中放置多個CRL檔案。傳入的憑證會根據每個CRL進行驗證。

在**SnapCenter Windows**主機上設定「**CA**憑證」以使用「更新自訂外掛程式」服務

您應該管理自訂外掛程式Keystore的密碼及其憑證、設定CA憑證、設定根或中繼憑證至自訂外掛程式信任存放區、以及設定CA簽署金鑰配對至自訂外掛程式信任存放區、並使用SnapCenter 「依賴自訂外掛程式」服務啟動已安裝的數位憑證。

自訂外掛程式使用檔案_keyKeystore。jks_、位於_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_、兩者都是其信任存放區和金鑰存放區。

管理自訂外掛程式**Keystore**的密碼、以及使用中的**CA**簽署金鑰配對別名

步驟

1. 您可以從自訂外掛程式代理程式內容檔擷取自訂外掛程式Keystore預設密碼。

   它是對應於key_keystore _pass的值。

2. 變更Keystore密碼：

   keytool-storepasswd -keystore keystor.jks

   如果Windows命令提示字元無法辨識「keytool」命令、請將keytoolt命令替換為完整路徑。

   C：\Program Files\Java\<JDK_VERY>\BIN\keytool.exe"-storepasswd -keystore keyKeystore .jks

3. 將Keystore中私密金鑰項目的所有別名密碼變更為與Keystore相同的密碼：

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

   在_agent.properties_檔案中更新keyKeystore _pass的相同更新。

4. 變更密碼後重新啟動服務。

   自訂外掛程式Keystore的密碼、以及私密金鑰的所有相關別名密碼均應相同。

將根或中繼憑證設定為自訂外掛程式信任存放區

您應該設定根或中繼憑證、而不使用私密金鑰、以自訂外掛程式信任存放區。

步驟

1. 瀏覽至包含自訂外掛程式Keystore _C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_的資料夾
2. 找到「keystore .jks」檔案。
3. 在Keystore中列出新增的憑證：

   keytool-list -v -keystore keyKeystore .jks

4. 新增根或中繼憑證：

   keytool-import -cactacerts -alias myRootCA -file /root/USERTrustra_root.cer -keystore keyKeystore .jks

5. 將根或中繼憑證設定為自訂外掛程式信任存放區之後、請重新啟動服務。

您應該先新增根CA憑證、然後再新增中繼CA憑證。

將**CA**簽署金鑰配對設定為自訂外掛程式信任存放區

您應該將CA簽署金鑰配對設定為自訂外掛程式信任存放區。

步驟

1. 瀏覽至包含自訂外掛程式Keystore _C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_的資料夾

2. 找到檔案_keystore。jks_。
3. 在Keystore中列出新增的憑證：

   keytool-list -v -keystore keyKeystore .jks

4. 新增具有私密金鑰和公開金鑰的CA憑證。

   keytool-importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype.kcs12 -destkeystore keyKeystore .jks -deststoretype.jks

5. 在Keystore中列出新增的憑證。

   keytool-list -v -keystore keyKeystore .jks

6. 驗證密鑰庫是否包含與新CA憑證對應的別名、該CA憑證已新增至金鑰庫。
7. 將CA憑證的新增私密金鑰密碼變更為金鑰庫密碼。

   預設的自訂外掛程式Keystore密碼是agent.properties檔案中KeyKeyKeystore _pass的值。

   keytool-keypasswd -alias "alias name_in_CA_cert "-keystore keyKeystore .jks

8. 在_agent.properties_檔案中設定CA憑證的別名。

   請根據SCC_IDATure_ALIAS金鑰更新此值。

9. 將CA簽署金鑰配對設定為自訂外掛程式信任存放區之後、請重新啟動服務。

針對**SnapCenter** 「不一樣的自訂外掛程式」設定憑證撤銷清單（**CRL**）

關於這項工作

- 若要下載相關 CA 憑證的最新 CRL 檔案，請參閱 "如何更新SnapCenter 「驗證CA憑證」中的憑證撤銷清單檔案"。
- 「自訂外掛程式」會在預先設定的目錄中搜尋CRL檔案。SnapCenter
- 適用於「不適用自訂外掛程式」的CRL檔案預設目錄SnapCenter 為：*C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-In Creator\ etc\crl_*。

步驟

1. 您可以根據金鑰CRP_path修改及更新_agent.properties_檔案中的預設目錄。
2. 您可以在此目錄中放置多個CRL檔案。

   傳入的憑證會根據每個CRL進行驗證。

啟用外掛程式的**CA**憑證

您應該設定CA憑證、並在SnapCenter 伺服器和對應的外掛程式主機上部署CA憑證。您應該為外掛程式啟用CA憑證驗證。

開始之前

- 您可以使用run *Set-SmCertificateSettings* Cmdlet來啟用或停用CA憑證。
- 您可以使用_Get-SmCertificateSettings_來顯示外掛程式的憑證狀態。

您可以執行_Get-Help命令name_來取得可搭配Cmdlet使用之參數及其說明的相關資訊。或者、您也可以參閱 "《軟件指令程式參考指南》SnapCenter"。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下「託管主機」。
3. 選取單一或多個外掛程式主機。
4. 按一下*更多選項*。
5. 選取*啟用憑證驗證*。

完成後

「受管理的主機」標籤主機會顯示掛鎖、掛鎖的色彩則會指出SnapCenter 「支援服務器」與外掛主機之間的連線狀態。

- * * 表示 CA 憑證未啟用或未指派給外掛主機。
- * * 表示 CA 憑證已成功驗證。
- * * 表示 CA 憑證無法驗證。
- * * 表示無法擷取連線資訊。

當狀態為黃色或綠色時、資料保護作業會成功完成。