設定憑證型驗證

SnapCenter Software 4.9

NetApp
March 20, 2024

目錄

設定憑證型驗證

從 SnapCenter 伺服器匯出憑證授權單位（ CA ）憑證

您應該使用 Microsoft 管理主控台（ MMC ）、將 CA 憑證從 SnapCenter 伺服器匯出至外掛主機。

開始之前

您應該已設定雙向 SSL 。

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 * > * 個人 * > * 憑證 * 。
5. 以滑鼠右鍵按一下用於 SnapCenter 伺服器的已取得 CA 憑證、然後選取 * 所有工作 * > * 匯出 * 以啟動匯出精靈。
6. 在精靈中執行下列動作。

針對此選項 ...	請執行下列動作...
匯出私密金鑰	選擇 * 否、不要匯出私密金鑰 * 、然後按一下 * 下一步 * 。
匯出檔案格式	單擊 * 下一步 * 。
檔案名稱	按一下 * 瀏覽 * 並指定儲存憑證的檔案路徑、然後按一下 * 下一步 * 。
完成憑證匯出精靈	檢閱摘要、然後按一下「完成」開始匯出。

SnapCenter HA 組態和 SnapCenter Plug-in for VMware vSphere 不支援憑證型驗證。

將憑證授權單位（ CA ）憑證匯入 Windows 外掛主機

若要使用匯出的 SnapCenter 伺服器 CA 憑證、您應該使用 Microsoft 管理主控台（ MMC ）、將相關的憑證匯入 SnapCenter Windows 外掛主機。

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 * > * 個人 * > * 憑證 * 。
5. 在資料夾「個人」上按一下滑鼠右鍵、然後選取 * 所有工作 * > * 匯入 * 以啟動匯入精靈。
6. 在精靈中執行下列動作。

針對此選項 ...	請執行下列動作...
零售店位置	單擊 * 下一步 * 。
要匯入的檔案	選取以 .cer 副檔名結尾的 SnapCenter 伺服器憑證。
憑證存放區	單擊 * 下一步 * 。
完成憑證匯出精靈	檢閱摘要、然後按一下「完成」開始匯入。

將 CA 憑證匯入 UNIX 主機外掛程式、並將根或中繼憑證設定為 SPL 信任存放區

將 CA 憑證匯入 UNIX 外掛主機

您應該將 CA 憑證匯入 UNIX 外掛主機。

關於此工作

- 您可以管理 SPL Keystore 的密碼、以及使用中的 CA 簽署金鑰配對別名。
- SPL 密鑰庫和私鑰的所有關聯別名密碼應相同。

步驟

1. 您可以從SPL內容檔擷取SPL Keystore預設密碼。它是對應於金鑰的值 `SPL_KEYSTORE_PASS`。
2. 變更Keystore密碼： `$ keytool -storepasswd -keystore keystore.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>" -keystore keystore.jks`
4. 請針對 SPL_Keystore 密碼進行相同的更新 `spl.properties`` 檔案：
5. 變更密碼後重新啟動服務。

將根或中繼憑證設定為SPL信任存放區

您應該將根或中繼憑證設定為 SPL 信任存放區。您應該先新增根CA憑證、然後再新增中繼CA憑證。

步驟

1. 瀏覽至包含 SPL Keystore 的資料夾： `/var/opt/snapcenter/spl/etc`。
2. 找到檔案 `keystore.jks`。
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 <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. 將根或中繼憑證設定為SPL信任存放區之後、請重新啟動服務。

將**CA**簽署金鑰配對設定為**SPL**信任存放區

您應該將 CA 簽署金鑰配對設定為 SPL 信任存放區。

步驟

1. 瀏覽至包含 SPL Keystore 的資料夾 `/var/opt/snapcenter/spl/etc`。
2. 找到檔案 `keystore.jks`。
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 <CertificatePathToImport> -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 SPL 金鑰庫密碼是金鑰 SPL_Keystore 密碼的值 `spl.properties` 檔案：

   `$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
8. 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 "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. 從中的 Keystore 設定別名 `spl.properties` 檔案： 請根據SPL_PRO證 書別名更新此值。
10. 將CA簽署金鑰配對設定為SPL信任存放區後、請重新啟動服務。

啟用憑證型驗證

若要為 SnapCenter Server 和 Windows 外掛程式主機啟用憑證型驗證、請執行下列 PowerShell Cmdlet 。 對於 Linux 外掛主機、當您啟用雙向 SSL 時、將會啟用憑證型驗證。

- 若要啟用用戶端憑證型驗證：

  `Set-SmConfigSettings -Agent –configSettings`

```
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- 若要停用用戶端憑證型驗證：

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