



設定憑證型驗證

SnapCenter Software 4.9

NetApp
March 20, 2024

目錄

設定憑證型驗證	1
從 SnapCenter 伺服器匯出憑證授權單位 (CA) 憑證	1
將憑證授權單位 (CA) 憑證匯入 Windows 外掛主機	1
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	2
啟用憑證型驗證	3

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 <AliasNameForCertificateToBeImported> -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 "<OriginalAliasName>" -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]`
```

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。