# 管理憑證

## E-Series storage systems

NetApp
January 20, 2026

# 目錄

# 管理憑證

## 瞭解如何在 **SANtricity Storage Plugin for vCenter** 中管理憑證

vCenter儲存外掛程式中的「憑證管理」可讓您建立憑證簽署要求（CSR）、匯入憑證、以及管理現有的憑證。

### 什麼是憑證？

憑證是數位檔案、可識別網站和伺服器等線上實體、以便在網際網路上進行安全通訊。它們確保Web通訊只能在指定的伺服器和用戶端之間以加密形式進行傳輸、無論是私下傳輸或是未經變更。使用Storage Plugin for vCenter、您可以管理主機管理系統上瀏覽器的憑證、以及探索到的儲存陣列中的控制器。

憑證可以由信任的授權單位簽署、也可以自行簽署。「簽署」只是指有人驗證擁有者的身分、並判斷其裝置是否值得信任。

儲存陣列會在每個控制器上隨附自動產生的自我簽署憑證。您可以繼續使用自我簽署的憑證、或是取得CA簽署的憑證、以便在控制器與主機系統之間建立更安全的連線。

> 雖然CA簽署的憑證可提供更好的安全保護（例如預防攔截式攻擊）、但如果您的網路規模較大、也需要支付昂貴的費用。相較之下、自我簽署的憑證較不安全、但完全免費。因此、自我簽署的憑證最常用於內部測試環境、而非正式作業環境。

### 簽署的憑證

已簽署的憑證會由信任的協力廠商組織之憑證授權單位（CA）驗證。簽署的憑證包括實體擁有者（通常是伺服器或網站）、憑證發行日期和到期日期、實體的有效網域、以及由字母和數字組成的數位簽章等詳細資料。

當您開啟瀏覽器並輸入網址時、系統會在背景執行憑證檢查程序、以判斷您是否要連線至內含有效CA簽署憑證的網站。一般而言、以簽署憑證保護的站台會在位址中包含掛鎖圖示和https指定名稱。如果您嘗試連線至不含CA簽署憑證的網站、瀏覽器會顯示網站不安全的警告。

CA會在應用程式處理期間採取步驟來驗證您的身分。他們可能會傳送電子郵件給您的註冊企業、驗證您的公司地址、並執行HTTP或DNS驗證。應用程式程序完成後、CA會傳送數位檔案給您、以便載入主機管理系統。通常、這些檔案包括信任鏈、如下所示：

- 根-階層頂端是根憑證、其中包含用於簽署其他憑證的私密金鑰。根可識別特定的CA組織。如果您的所有網路裝置都使用相同的CA、則只需要一個根憑證。
- 中級：從根目錄下分出的是中繼憑證。CA會發出一或多個中繼憑證、做為受保護根憑證與伺服器憑證之間的中間人。
- 伺服器：在鏈結底部是伺服器憑證、可識別您的特定實體、例如網站或其他裝置。儲存陣列中的每個控制器都需要個別的伺服器憑證。

### 自我簽署的憑證

儲存陣列中的每個控制器都包含預先安裝的自我簽署憑證。自我簽署的憑證與CA簽署的憑證類似、只是由實體擁有者（而非第三方）驗證。如同CA簽署的憑證、自我簽署的憑證也包含自己的私密金鑰、同時確保資料經過加密、並透過伺服器與用戶端之間的HTTPS連線傳送。

自我簽署的憑證不受瀏覽器「信任」。每次您嘗試連線至僅包含自我簽署憑證的網站時、瀏覽器都會顯示警告訊息。您必須按一下警告訊息中的連結、以便繼續前往網站；如此一來、您基本上就會接受自我簽署的憑證。

### 管理證書

當您開啟外掛程式時、瀏覽器會檢查數位憑證、以驗證管理主機是否為信任來源。如果瀏覽器找不到CA簽署的憑證、則會開啟警告訊息。您可以從這裡繼續前往網站、接受該工作階段的自我簽署憑證。您也可以從CA取得已簽署的數位憑證、因此不會再看到警告訊息。

### 信任的憑證

在外掛程式工作階段期間、當您嘗試存取沒有CA簽署憑證的控制器時、可能會看到其他安全性訊息。在此情況下、您可以永久信任自我簽署的憑證、也可以匯入控制器的CA簽署憑證、讓外掛程式能夠驗證這些控制器傳入的用戶端要求。

# 在 SANtricity Storage Plugin for vCenter 中使用 CA 簽署的憑證

您可以取得並匯入CA簽署的憑證、以安全地存取裝載Storage Plugin for vCenter的管理系統。

使用CA簽署的憑證是三個步驟的程序：

- 步驟1：完成CSR檔案。
- 步驟2：提交CSR檔案。
- [步驟3：匯入管理憑證]。

## 步驟1：完成CSR檔案

您必須先產生憑證簽署要求（CSR）檔案、以識別您的組織和執行外掛程式的主機系統。或者、您也可以使用諸如OpenSSL的工具來產生CSR檔案、然後跳至 步驟2：提交CSR檔案。

步驟

1. 選擇*憑證管理*。
2. 從*管理*索引標籤、選取*完整的csr*。
3. 輸入下列資訊、然後按一下*下一步*：
   - 組織：貴公司或組織的完整法定名稱。包括尾碼、例如Inc.或Corp.
   - 組織單位（選用）：您組織處理憑證的部門。
   - 城市/地區：您的主機系統或企業所在的城市。
   - 州/地區（選用）：主機系統或企業所在的州或地區。
   - 國家**ISO**代碼：您所在國家/地區的兩位數ISO（國際標準化組織）代碼、例如US。
4. 輸入外掛程式執行所在主機系統的下列資訊：
   - 一般名稱：執行外掛程式之主機系統的IP位址或DNS名稱。請確定此位址正確無誤、而且必須完全符合您輸入的內容、才能在瀏覽器中存取外掛程式。請勿包含http：//或https：//。DNS名稱不能以萬用字元

開頭。

- 備用**IP**位址-如果一般名稱是IP位址、您可以選擇輸入主機系統的任何其他IP位址或別名。對於多個項目、請使用以逗號分隔的格式。
- 備用**DNS**名稱-如果通用名稱是DNS名稱、請輸入主機系統的任何其他DNS名稱。對於多個項目、請使用以逗號分隔的格式。如果沒有替代DNS名稱、但您在第一個欄位中輸入DNS名稱、請在此處複製該名稱。DNS名稱不能以萬用字元開頭。

5. 確認主機資訊正確無誤。如果不是、當您嘗試匯入CA時、從CA傳回的憑證將會失敗。
6. 單擊*完成*。

## 步驟**2**：提交**CSR**檔案

建立憑證簽署要求（CSR）檔案之後、您會將產生的CSR檔案傳送給CA、以接收裝載外掛程式之系統的已簽署管理憑證。

E系列系統要求簽署的憑證使用PEm格式（Base64 Ascii編碼）、其中包含下列檔案類型：.pem、.crt、.cer或.key。

步驟

1. 找到下載的CSR檔案。

   下載的資料夾位置取決於您的瀏覽器。

2. 將CSR檔案提交給CA（例如、Verisign或Digiting）、並以PEV格式要求簽署的憑證。

> 將CSR檔案提交給CA之後、請勿重新產生另一個CSR檔案。

每當您產生CSR時、系統都會建立私密與公開金鑰配對。公開金鑰是CSR的一部分、而私密金鑰則保留在系統的Keystore中。當您收到簽署的憑證並匯入時、系統會確保私密金鑰和公開金鑰都是原始配對。如果金鑰不符、簽署的憑證將無法運作、您必須向CA要求新的憑證。

## 步驟**3**：匯入管理憑證

從憑證授權單位（CA）收到簽署的憑證後、請將憑證匯入安裝外掛程式的主機系統。

開始之前

- 您必須擁有CA所簽署的憑證。這些檔案包括根憑證、一或多個中繼憑證和伺服器憑證。
- 如果CA提供鏈結的憑證檔案（例如.p7b檔案）、您必須將鏈結的檔案解壓縮至個別檔案：根憑證、一或多個中繼憑證及伺服器憑證。您可以使用Windows certmanager公用程式來解壓縮檔案（按一下滑鼠右鍵、然後選取功能表：All Tasks [Export（所有工作[匯出]）。建議使用Base 64編碼。匯出完成後、會針對鏈中的每個憑證檔案顯示一個CER.檔案。
- 您必須將憑證檔案複製到執行外掛程式的主機系統。

步驟

1. 選擇*憑證管理*。
2. 從*管理*索引標籤、選取*匯入*。

   隨即開啟一個對話方塊、用於匯入憑證檔案。

3. 按一下*瀏覽*以先選取根和中繼憑證檔案、然後選取伺服器憑證。如果您是從外部工具產生CSR、也必須匯入與CSR一起建立的私密金鑰檔案。

   檔案名稱會顯示在對話方塊中。

4. 按一下*匯入*。

結果

檔案會上傳並驗證。憑證資訊會顯示在「憑證管理」頁面上。

# 在 SANtricity Storage Plugin for vCenter 中重設管理憑證

對於託管Storage Plugin for vCenter的管理系統、您可以將管理憑證還原為原始的原廠自我簽署狀態。

關於這項工作

此工作會從執行vCenter儲存外掛程式的主機系統刪除目前的管理憑證。重設憑證後、主機系統會恢復使用自我簽署的憑證。

步驟

1. 選擇*憑證管理*。
2. 從*管理*索引標籤、選取*重設*。

   隨即開啟「確認重設管理憑證」對話方塊。

3. 在欄位中輸入重設、然後按一下*重設*。

   瀏覽器重新整理之後、瀏覽器可能會封鎖對目的地站台的存取、並回報該站台使用HTTP嚴格傳輸安全性。當您切換回自我簽署的憑證時、就會出現這種情況。若要清除封鎖目的地存取的條件、您必須從瀏覽器清除瀏覽資料。

結果

系統會從伺服器恢復使用自我簽署的憑證。因此、系統會提示使用者手動接受其工作階段的自我簽署憑證。

# 在 SANtricity Storage Plugin for vCenter 中匯入陣列的憑證

如有必要、您可以匯入儲存陣列的憑證、以便與裝載Storage Plugin for vCenter的系統進行驗證。憑證可以由憑證授權單位（CA）簽署、也可以自行簽署。

開始之前

如果您要匯入信任的憑證、則必須使用System Manager匯入儲存陣列控制器的憑證。

步驟

1. 選擇*憑證管理*。
2. 選取*信任的*索引標籤。

   此頁面顯示針對儲存陣列所報告的所有憑證。

3. 選取功能表：匯入[憑證]以匯入CA憑證、或選取功能表：匯入[自我簽署的儲存陣列憑證]以匯入自我簽署的憑證。
4. 若要限制檢視、您可以使用*顯示…*篩選的憑證欄位、或按一下其中一個欄位標題來排序憑證列。
5. 在對話方塊中、選取憑證、然後按一下*匯入*。

   憑證已上傳並驗證。

# 在 SANtricity Storage Plugin for vCenter 中檢視憑證

您可以檢視憑證的摘要資訊、包括使用憑證的組織、發行憑證的授權單位、有效期間及指紋（唯一識別碼）。

步驟

1. 選擇*憑證管理*。
2. 選取下列其中一個索引標籤：
   - 管理：顯示託管外掛程式之系統的憑證。管理憑證可由憑證授權單位（CA）自行簽署或核准。它允許安全存取外掛程式。
   - * Trusted （受信任的）-顯示外掛程式可存取儲存陣列和其他遠端伺服器（例如LDAP伺服器）的憑證。這些憑證可以從憑證授權單位（CA）核發、也可以自行簽署。
3. 若要查看有關憑證的詳細資訊、請選取其列、選取列尾端的省略符號、然後按一下*檢視*或*匯出*。

# 匯出 SANtricity Storage Plugin for vCenter 中的憑證

您可以匯出憑證以檢視其完整詳細資料。

開始之前

若要開啟匯出的檔案、您必須擁有憑證檢視器應用程式。

步驟

1. 選擇*憑證管理*。
2. 選取下列其中一個索引標籤：
   - 管理：顯示託管外掛程式之系統的憑證。管理憑證可由憑證授權單位（CA）自行簽署或核准。它允許安全存取外掛程式。
   - * Trusted （受信任的）-顯示外掛程式可存取儲存陣列和其他遠端伺服器（例如LDAP伺服器）的憑證。這些憑證可以從憑證授權單位（CA）核發、也可以自行簽署。
3. 從頁面選取憑證、然後按一下列結尾的省略符號。
4. 按一下「匯出」、然後儲存憑證檔案。
5. 在憑證檢視器應用程式中開啟檔案。

# 在 SANtricity Storage Plugin for vCenter 中刪除信任的憑證

您可以刪除一或多個不再需要的憑證、例如過期的憑證。

開始之前

請先匯入新的憑證、再刪除舊的憑證。

請注意、刪除根或中繼憑證可能會影響多個儲存陣列、因為這些陣列可以共用相同的憑證檔案。

步驟

1. 選擇*憑證管理*。
2. 選取*信任的*索引標籤。
3. 在表格中選取一或多個憑證、然後按一下*刪除*。

   預先安裝的憑證無法使用刪除功能。

   「確認刪除信任的憑證」對話方塊隨即開啟。

4. 確認刪除、然後按一下*刪除*。

   該憑證會從表格中移除。

# 在 SANtricity Storage Plugin for vCenter 中解決不受信任的憑證

從「憑證」頁面、您可以從儲存陣列匯入自我簽署的憑證、或匯入由信任的第三方所核發的憑證授權單位（CA）憑證、藉此解決不受信任的憑證。

開始之前

如果您打算匯入CA簽署的憑證、請確定：

- 您已為儲存陣列中的每個控制器產生憑證簽署要求（.CSR檔案）、並將其傳送至CA。
- CA傳回信任的憑證檔案。
- 您可以在本機系統上使用憑證檔案。

關於這項工作

當儲存陣列嘗試建立外掛程式的安全連線、但連線無法確認為安全時、就會發生不受信任的憑證。如果符合下列任一項條件、您可能需要安裝其他信任的CA憑證：

- 您最近新增了儲存陣列。
- 一個或兩個憑證都已過期或撤銷。
- 一或兩個憑證都遺失根或中繼憑證。

步驟

1. 選擇*憑證管理*。
2. 選取*信任的*索引標籤。

   此頁面顯示針對儲存陣列所報告的所有憑證。

3. 選取功能表：匯入[憑證]以匯入CA憑證、或選取功能表：匯入[自我簽署的儲存陣列憑證]以匯入自我簽署的憑證。
4. 若要限制檢視、您可以使用*顯示…*篩選的憑證欄位、或按一下其中一個欄位標題來排序憑證列。
5. 在對話方塊中選取憑證、然後按一下*匯入*。

   憑證已上傳並驗證。