使用憑證
SANtricity 11.8

NetApp
December 16, 2024

目錄

使用憑證

控制器使用CA簽署的憑證

您可以取得CA簽署的憑證、以便在控制器與瀏覽器之間進行安全通訊、以存取System Manager。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- 您必須知道每個控制器的IP位址或DNS名稱。

關於這項工作

使用CA簽署的憑證是三個步驟的程序。

步驟1：完成控制器的CSR

您必須先為儲存陣列中的每個控制器產生憑證簽署要求（CSR）檔案。

關於這項工作

本工作說明如何從System Manager產生CSR檔案。CSR會提供組織的相關資訊、以及控制器的IP位址或DNS名稱。在此工作期間、如果儲存陣列有一個控制器和兩個CSR檔案（如果有兩個控制器）、則會產生一個CSR檔案。

或者，您也可以使用 Openssl 等工具產生 CSR 檔案，並可跳至步驟2：提交CSR檔案。

步驟

1. 選取功能表：設定[憑證]。
2. 從Array Management（陣列管理）選項卡中選擇*完整的csr*。

   如果看到對話方塊提示您接受第二個控制器的自我簽署憑證、請按一下*「接受自我簽署的憑證*」繼續。

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：儲存陣列或企業所在的城市。
   - 州/地區（選用）：儲存陣列或業務所在的州或地區。
   - 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。

   某些欄位可能會預先填入適當的資訊、例如控制器的IP位址。除非您確定預先填入的值不正確、否則請勿變更。例如、如果您尚未完成CSR、則控制器IP位址會設為「'localhost.」 在此情況下、您必須將「'localhost'」變更為控制器的DNS名稱或IP位址。

4. 驗證或輸入儲存陣列中控制器A的下列資訊：

   - 控制器一般名稱-預設會顯示控制器A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System Manager。DNS名稱不能以萬用字元開頭。
   - * 控制器替代 IP 位址 * — 如果一般名稱是 IP 位址，您可以選擇性地輸入控制器 A 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。
   - * 控制器替代 DNS 名稱 * — 如果一般名稱是 DNS 名稱，請輸入控制器 A 的任何其他 DNS 名稱。若為多個項目，請使用逗號分隔格式。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。如果儲存陣列只有一個控制器、則可使用* Finish（完成）*按鈕。

     如果儲存陣列有兩個控制器、則可使用* Next*按鈕。

   > 當您初次建立CSR要求時、請勿按一下*跳過此步驟*連結。此連結是在錯誤恢復情況下提供的。在極少數情況下、CSR要求可能會在一個控制器上失敗、但在另一個控制器上失敗。此連結可讓您跳過在控制器A上建立CSR要求的步驟（如果已定義）、然後繼續下一步、在控制器B上重新建立CSR要求

5. 如果只有一個控制器、請按一下「完成」。如果有兩個控制器、請按「下一步」輸入控制器B的資訊（與上述相同）、然後按一下「完成」。

   對於單一控制器、一個CSR檔案會下載到您的本機系統。對於雙控制器、會下載兩個CSR檔案。下載的資料夾位置取決於您的瀏覽器。

6. 前往 步驟2：提交CSR檔案。

步驟2：提交CSR檔案

建立憑證簽署要求（CSR）檔案之後、請將檔案傳送至憑證授權單位（CA）。E系列系統要求簽署的憑證使用PEE格式（Base64 Ascii編碼）、其中包含下列檔案類型：PEE、.CRT、.cer或.key。

步驟

1. 找到下載的CSR檔案。
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，請勿重新產生其他 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。

3. 當 CA 傳回簽署的憑證時，請移至步驟 3 ：匯入控制器的簽署憑證。

步驟 3 ：匯入控制器的簽署憑證

從憑證授權單位（CA）收到簽署的憑證後、請匯入控制器的檔案。

開始之前

- CA傳回簽署的憑證檔案。這些檔案包括根憑證、一或多個中繼憑證及伺服器憑證。

- 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、以及識別控制器的伺服器憑證。您可以使用 Windows `certmgr` 公用程式來解壓縮檔案（按一下滑鼠右鍵，然後選取功能表：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。
- 您已將憑證檔案複製到存取System Manager的主機系統。

步驟

1. 選取功能表：設定[憑證]
2. 從Array Management（陣列管理）選項卡中選擇* Import（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*按鈕、先選取根和中繼憑證檔案、然後選取控制器的每個伺服器憑證。兩個控制器的根和中間檔案相同。每個控制器只有伺服器憑證是唯一的。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*。

   檔案會上傳並驗證。

結果

工作階段會自動終止。您必須重新登入、憑證才能生效。當您再次登入時、新的CA簽署憑證會用於您的工作階段。

重設管理憑證

您可以將控制器上的憑證從使用CA簽署的憑證還原為原廠設定的自我簽署憑證。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- CA簽署的憑證必須先匯入。

關於這項工作

重設功能會從每個控制器刪除目前由CA簽署的憑證檔案。然後控制器將恢復使用自我簽署的憑證。

步驟

1. 選取功能表：設定[憑證]。
2. 從Array Management（陣列管理）選項卡中選擇* Reset*（重置*）。

   隨即開啟「確認重設管理憑證」對話方塊。

3. 在欄位中輸入 `reset`，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

控制器會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。

檢視匯入的憑證資訊

在「憑證」頁面中、您可以檢視儲存陣列的憑證類型、發行授權單位及有效的憑證日期範圍。

開始之前

您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。

步驟

1. 選取功能表：設定[憑證]。
2. 選取其中一個索引標籤以檢視憑證的相關資訊。

索引標籤	說明
陣列管理	檢視針對每個控制器匯入的CA簽署憑證相關資訊、包括根檔案、中繼檔案和伺服器檔案。
值得信賴	檢視所有其他類型的控制器匯入憑證的相關資訊。使用* Show certificates that are …*（顯示…的憑證）下的篩選欄位、即可檢視使用者安裝或預先安裝的憑證。 • 使用者安裝：使用者上傳至儲存陣列的憑證、當控制器做為用戶端（而非伺服器）、LDAPS憑證及身分識別聯盟憑證時、可包含信任的憑證。 • 預先安裝：儲存陣列隨附的自我簽署憑證。
金鑰管理	檢視匯入外部金鑰管理伺服器之CA簽署憑證的相關資訊。

以用戶端身分匯入控制器的憑證

如果控制器因為無法驗證網路伺服器的信任鏈結而拒絕連線、您可以從信任的索引標籤匯入憑證、讓控制器（做為用戶端）接受來自該伺服器的通訊。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- 憑證檔案會安裝在您的本機系統上。

關於這項工作

如果您想要允許其他伺服器聯絡控制器（例如使用TLS的LDAP伺服器或syslog伺服器）、可能需要從信任的索引標籤匯入憑證。

步驟

1. 選取功能表：設定[憑證]。

2. 從信任的索引標籤中、選取*匯入*。

   隨即開啟一個對話方塊、用於匯入信任的憑證檔案。

3. 單擊*瀏覽*以選擇控制器的證書文件。

   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。

啟用憑證撤銷檢查

您可以啟用撤銷憑證的自動檢查、讓線上憑證狀態傳輸協定（OCSP）伺服器封鎖使用者建立不安全的連線。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- DNS伺服器是在兩個控制器上設定、可讓OCSP伺服器使用完整網域名稱。此工作可從「硬體」頁面取得。
- 如果您要指定自己的OCSP伺服器、必須知道該伺服器的URL。

關於這項工作

自動撤銷檢查有助於在CA未適當核發憑證或私密金鑰遭洩漏的情況下進行撤銷檢查。

在此工作期間、您可以設定OCSP伺服器、或使用憑證檔案中指定的伺服器。OCSP伺服器會判斷CA是否在排定的到期日之前撤銷任何憑證、然後在憑證撤銷時封鎖使用者存取站台。

步驟

1. 選取功能表：設定[憑證]。
2. 選取*信任的*索引標籤。

   

   您也可以從*金鑰管理*索引標籤啟用撤銷檢查。

3. 按一下「不尋常工作」、然後從下拉式功能表中選取「啟用撤銷檢查」。
4. 選取*我要啟用撤銷檢查*、如此核取方塊中會出現核取符號、對話方塊中會出現其他欄位。
5. 在「* OCSP回應程式位址*」欄位中、您可以選擇性地輸入OCSP回應程式伺服器的URL。如果您未輸入位址、系統會使用憑證檔案中的OCSP伺服器URL。
6. 按一下*測試位址*、確定系統可以開啟連線至指定的URL。
7. 按一下「 * 儲存 * 」。

結果

如果儲存陣列嘗試連線至具有撤銷憑證的伺服器、則連線會遭拒、並記錄事件。

刪除信任的憑證

您可以刪除先前從信任索引標籤匯入的使用者安裝憑證。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- 如果您要以新版本更新信任的憑證、則必須先匯入更新的憑證、才能刪除舊的憑證。

> 如果您在匯入替代憑證之前刪除用於驗證控制器和其他伺服器（例如LDAP伺服器）的憑證、則可能會喪失系統存取權。

關於這項工作

此工作說明如何刪除使用者安裝的憑證。無法刪除預先安裝的自我簽署憑證。

步驟

1. 選取功能表：設定[憑證]。
2. 選取*信任的*索引標籤。

   下表顯示儲存陣列的信任憑證。
3. 從表格中選取您要移除的憑證。
4. 按一下功能表：「Uncommon Tasks（非常見工作）」[Delete

   隨即開啟「確認刪除信任的憑證」對話方塊。
5. 在欄位中輸入 `delete`，然後按一下 * 刪除 * 。

使用CA簽署的憑證來驗證金鑰管理伺服器

若要在金鑰管理伺服器與儲存陣列控制器之間進行安全通訊、您必須設定適當的憑證集。

開始之前

您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。

關於這項工作

在控制器和金鑰管理伺服器之間進行驗證是兩步驟的程序。

步驟1：完成並提交CSR、以便使用金鑰管理伺服器進行驗證

您必須先產生憑證簽署要求（CSR）檔案、然後使用CSR向金鑰管理伺服器信任的憑證授權單位（CA）要求簽署的用戶端憑證。您也可以使用下載的CSR檔案、從金鑰管理伺服器建立及下載用戶端憑證。用戶端憑證會驗證儲存陣列的控制器、因此金鑰管理伺服器可以信任其金鑰管理互通性傳輸協定（KMIP）要求。

步驟

1. 選取功能表：設定[憑證]。
2. 從「金鑰管理」索引標籤中、選取*完整的csr*。

3. 輸入下列資訊：
   - 一般名稱-識別此CSR的名稱、例如儲存陣列名稱、將顯示在憑證檔案中。
   - 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：貴組織所在的城市或地區。
   - 州/地區（選用）：貴組織所在的州或地區。
   - 國家/地區**ISO**代碼-兩位數ISO（國際標準化組織）代碼、例如貴組織所在的美國。
4. 按一下*下載*。

   CSR檔案會儲存至本機系統。

5. 從金鑰管理伺服器信任的CA要求已簽署的用戶端憑證。
6. 擁有用戶端憑證時，請前往[步驟2：匯入金鑰管理伺服器的憑證]。

步驟2：匯入金鑰管理伺服器的憑證

下一步是匯入憑證、以便在儲存陣列與金鑰管理伺服器之間進行驗證。憑證有兩種類型：用戶端憑證會驗證儲存陣列的控制器、而金鑰管理伺服器憑證則會驗證伺服器。您必須同時載入控制器的用戶端憑證檔案、以及金鑰管理伺服器的伺服器憑證檔案。

開始之前

- 您有簽署的用戶端憑證檔案（請參閱步驟1：完成並提交CSR、以便使用金鑰管理伺服器進行驗證），而且已將該檔案複製到您要存取 System Manager 的主機。用戶端憑證會驗證儲存陣列的控制器、因此金鑰管理伺服器可以信任其金鑰管理互通性傳輸協定（KMIP）要求。
- 您必須從金鑰管理伺服器擷取憑證檔案、然後將該檔案複製到您正在存取System Manager的主機。金鑰管理伺服器憑證會驗證金鑰管理伺服器、因此儲存陣列可以信任其IP位址。您可以將根、中繼或伺服器憑證用於金鑰管理伺服器。

> 如需伺服器憑證的詳細資訊、請參閱金鑰管理伺服器的文件。

步驟

1. 選取功能表：設定[憑證]。
2. 從「金鑰管理」索引標籤中、選取*匯入*。

   隨即開啟一個對話方塊、用於匯入憑證檔案。

3. 在* Select用戶端憑證*旁、按一下*瀏覽*按鈕、選取儲存陣列控制器的用戶端憑證檔案。

   檔案名稱會顯示在對話方塊中。

4. 在*選取金鑰管理伺服器的伺服器憑證*旁、按一下*瀏覽*按鈕、選取金鑰管理伺服器的伺服器憑證檔案。您可以為金鑰管理伺服器選擇根、中繼或伺服器憑證。

   檔案名稱會顯示在對話方塊中。

5. 按一下*匯入*。

   檔案會上傳並驗證。

匯出金鑰管理伺服器憑證

您可以將金鑰管理伺服器的憑證儲存到本機機器。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、不會顯示憑證功能。
- 必須先匯入憑證。

步驟

1. 選取功能表：設定[憑證]。
2. 選取*金鑰管理*索引標籤。
3. 從表格中選取您要匯出的憑證、然後按一下*匯出*。

   隨即開啟「儲存」對話方塊。

4. 輸入檔案名稱、然後按一下*「Save*（儲存*）」。