憑證
SANtricity 11.5

NetApp
February 12, 2024

目錄

憑證

概念

CA憑證的運作方式

憑證授權單位（CA）是信任的實體、可發行稱為數位憑證的電子文件、以確保網際網路安全。這些憑證可識別網站擁有者、以便在用戶端與伺服器之間進行安全連線。

當您開啟瀏覽器並嘗試透過控制器管理連接埠連線至System Manager時、瀏覽器會嘗試驗證儲存陣列的控制器是否為信任來源。如果瀏覽器找不到控制器的數位憑證、它會警示您該憑證並未由認可的授權單位簽署、並詢問您是否要繼續。如果您不想再看到此警示、則必須從CA取得已簽署的數位憑證。

如果您使用具有磁碟機安全功能的外部金鑰管理伺服器、也可以建立該伺服器與控制器之間的驗證憑證、或是從儲存陣列接受自我簽署的憑證。

若要使用來自信任授權單位的數位憑證、必須執行下列步驟：

1. 前往功能表：設定[憑證]。您的使用者登入必須包含「安全性管理」權限、否則*憑證*不會出現在頁面上。
2. 為每個控制器或金鑰管理伺服器建立憑證簽署要求（CSR）。
3. 將.csr檔案傳送至CA、然後等待它們傳送憑證給您。
4. 從CA匯入信任的（中繼和根）憑證。這些憑證可為CA階層架構建立信任點。
5. 匯入每個控制器或金鑰管理伺服器的已簽署管理憑證。

憑證術語

瞭解憑證條款如何適用於您的儲存陣列。

期限	說明
CA	憑證授權單位（CA）是信任的實體、可發行稱為數位憑證的電子文件、以確保網際網路安全。這些憑證可識別網站擁有者、以便在用戶端與伺服器之間進行安全連線。
CSR	憑證簽署要求（CSR）是一則訊息、會從申請者傳送至憑證授權單位（CA）。CSR會驗證CA核發憑證所需的資訊。
憑證	憑證可識別站台的擁有者、以確保安全性、防止攻擊者模擬站台。憑證包含網站擁有者的相關資訊、以及認證（簽署）此資訊的信任實體身分。
用戶端憑證	在安全金鑰管理方面、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IP位址。

期限	說明
金鑰管理伺服器憑證	在安全金鑰管理方面、金鑰管理伺服器憑證會驗證伺服器、因此儲存陣列可以信任其IP位址。
管理證書	管理憑證由憑證授權單位（CA）核准、可安全存取Web應用程式。也稱為「簽署的憑證」。
OCSP伺服器	線上憑證狀態傳輸協定（OCSP）伺服器會判斷憑證授權單位（CA）是否在排定的到期日之前撤銷任何憑證、然後在憑證遭撤銷時、封鎖使用者存取伺服器。
自我簽署的憑證	控制器上預先載入自我簽署的憑證。如果站台連線是自行簽署的、則會在您繼續使用網路應用程式之前開啟一則警告訊息。
信任的憑證	來自憑證授權單位（CA）的信任憑證是位於憑證階層頂端的已知憑證。也稱為「根憑證」。

使用方法

完成控制器的**CA**憑證簽署要求（**CSR**）

若要接收儲存陣列控制器的憑證授權單位（CA）憑證、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。

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

此工作說明如何產生.CSR檔案（憑證簽署要求）、以便傳送給CA、以接收控制器的已簽署管理憑證。您必須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、如果儲存陣列中只有一個控制器、則會產生一個.csr檔案、如果有兩個控制器、則會產生兩個.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。
   - 控制器備用**IP**位址-如果通用名稱是IP位址、您可以選擇輸入控制器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**A**備用**DNS**名稱-如果通用名稱是DNS名稱、請為控制器A輸入任何其他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。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、會將一個.CSR檔案下載至您的本機系統。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. 將.csr檔案傳送至CA。

完成後

收到數位憑證時、請匯入CA傳送給您的適當憑證檔案。

匯入控制器的信任憑證

從憑證授權單位（CA）接收數位憑證之後、您可以匯入控制器的憑證鏈結（中繼和根）。

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。
- 您已產生憑證簽署要求（.CSR檔案）、並將其傳送至CA。
- CA傳回信任的憑證檔案。
- 憑證檔案會安裝在您的本機系統上。

關於這項工作

本工作說明如何上傳儲存陣列控制器的信任憑證。

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。

完成後

匯入管理憑證。

匯入控制器的管理憑證

匯入信任的憑證鏈結之後、您會為儲存陣列中的每個控制器匯入管理（簽署）憑證檔案。

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。
- 信任的憑證已匯入。
- CA傳回每個控制器的管理憑證檔案。
- 管理憑證檔案可在您的本機系統上使用。

關於這項工作

本工作說明如何上傳管理憑證檔案以進行控制器驗證。

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 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*以選取控制器A的檔案如果有兩個控制器、請按第二個*瀏覽*按鈕、選取控制器B的檔案

   檔案名稱會顯示在對話方塊中。

4. 按一下*匯入*。

   檔案已上傳並驗證。

結果

工作階段會自動終止。您必須再次登入、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。

檢視匯入的憑證資訊

您可以從「憑證」頁面檢視憑證類型、發行授權單位、以及先前匯入的憑證有效日期範圍。

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。

關於這項工作

此工作說明如何檢視使用者安裝或預先安裝之憑證的資訊。

步驟

1. 選取功能表：設定[憑證]。
2. 選取其中一個索引標籤、即可檢視金鑰管理伺服器的控制器、信任的憑證和憑證管理憑證相關資訊。

索引標籤	說明
陣列管理	檢視所有為控制器匯入的伺服器憑證資訊。
值得信賴	檢視所有為控制器匯入的信任（根）憑證相關資訊。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（包括信任的憑證、LDAPS憑證及身分識別聯盟憑證）。 • 預先安裝。儲存陣列隨附的憑證。
金鑰管理	檢視所有匯入外部金鑰管理伺服器的管理（簽署）憑證資訊。

刪除信任的憑證

您可以刪除任何使用者匯入的憑證。

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。

> 如果您在匯入替換憑證之前、刪除用於驗證儲存陣列管理憑證或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匯入的憑證。無法刪除預先定義的憑證。

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「刪除」、然後按一下「刪除」。

重設管理憑證

您可以將儲存陣列上的管理憑證還原為原廠自我簽署狀態。

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。

關於這項工作

重設儲存陣列上的管理憑證、會從每個控制器刪除目前的管理憑證。重設憑證之後、控制器會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*）。

   此時將打開一個*確認重置管理證書*對話框。

3. 在欄位中輸入「重設」、然後按一下「重設」。

結果

瀏覽器重新整理之後、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。

完成金鑰伺服器的**CA**憑證簽署要求（**CSR**）

若要接收金鑰管理伺服器的憑證授權單位（CA）憑證、您必須先產生憑證簽署要求（CSR）檔案。

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

此工作說明如何產生.CSR檔案（憑證簽署要求）、以便傳送給CA、以接收金鑰管理伺服器的簽署憑證。在此工作期間、您必須提供組織的相關資訊。

步驟

1. 選取功能表：設定[憑證]。
2. 從*金鑰管理*索引標籤、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. 將.csr檔案傳送至CA。

完成後

當您從金鑰管理伺服器取得用戶端和伺服器憑證時、請將其匯入以供儲存陣列控制器進行驗證。

匯入金鑰管理伺服器憑證

對於外部金鑰管理、您可以在儲存陣列和金鑰管理伺服器之間匯入驗證憑證、讓兩個實體彼此信任。憑證有兩種類型：用戶端憑證會驗證控制器、金鑰管理伺服器憑證則會驗證伺服器。

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。
- 儲存陣列可使用用戶端憑證。

> 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IP位址。若要取得用戶端憑證、您必須完成儲存陣列的CSR、然後將其上傳至金鑰管理伺服器。從伺服器產生用戶端憑證。

- 金鑰管理伺服器憑證可供使用。

> 金鑰管理伺服器憑證會驗證伺服器、因此儲存陣列可以信任其IP位址。若要取得金鑰管理伺服器憑證、您必須從金鑰管理伺服器產生。

關於這項工作

本工作說明如何上傳憑證檔案、以便在儲存陣列控制器與金鑰管理伺服器之間進行驗證。

步驟

1. 選取功能表：設定[憑證]。

2. 從*金鑰管理*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*按鈕以選取檔案。

   檔案名稱會顯示在對話方塊中。

4. 按一下*匯入*。

   檔案已上傳並驗證。

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*）」。

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。如果憑證授權單位（CA）未適當核發憑證、或私密金鑰遭入侵、自動撤銷檢查功能就很有幫助。

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

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。

常見問題集

為什麼會出現「無法存取其他控制器」對話方塊？

當您執行某些與CA憑證相關的作業（例如匯入憑證）時、可能會看到一個對話方塊、提示您接受第二個控制器的自我簽署憑證。

在具有兩個控制器（雙工組態）的儲存陣列中、SANtricity 如果無法與第二個控制器通訊、或是瀏覽器在作業的某個時間點無法接受憑證、有時會出現此對話方塊。

如果此對話方塊開啟、請按一下*「接受自我簽署的憑證*」繼續。如果另一個對話方塊提示您輸入密碼、請輸入您用於存取System Manager的管理員密碼。

如果此對話方塊再次出現、且您無法完成憑證工作、請嘗試下列其中一個程序：

- 使用不同的瀏覽器類型來存取此控制器、接受憑證並繼續。
- 使用System Manager存取第二個控制器、接受自我簽署的憑證、然後返回第一個控制器並繼續。

如何知道需要將哪些憑證上傳至**System Manager**？

對於外部金鑰管理、您可以匯入兩種類型的憑證、以便在儲存陣列和金鑰管理伺服器之間進行驗證、讓兩個實體彼此信任。

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IP位址。若要取得用戶端憑證、您必須完成儲存陣列的CSR、然後將其上傳至金鑰管理伺服器。從伺服器產生用戶端憑證、然後使用System Manager匯入。

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。若要取得金鑰管理伺服器憑證、您必須從金鑰管理伺服器產生。

關於憑證撤銷檢查、我需要知道什麼？

System Manager可讓您使用線上憑證狀態傳輸協定（OCSP）伺服器來檢查撤銷的憑證、而非上傳憑證撤銷清單（CRL）。

撤銷的憑證不應再受到信任。憑證可能會因數種原因而遭撤銷；例如、如果憑證授權單位（CA）未適當核發憑證、私密金鑰遭洩漏、或是識別的實體未遵守原則要求。

在System Manager中建立OCSP伺服器的連線之後、儲存陣列會在連線至AutoSupport 某個伺服器、外部金鑰管理伺服器（EKMS）、SSL上的輕量型目錄存取傳輸協定（LDAPS）伺服器或Syslog伺服器時、執行撤銷檢查。儲存陣列會嘗試驗證這些伺服器的憑證、以確保這些憑證尚未撤銷。然後伺服器會傳回該憑證的「好」、「已撤銷」或「未知」值。如果憑證已撤銷、或陣列無法聯絡OCSP伺服器、則連線會遭到拒絕。

> 在System Manager或命令列介面（CLI）中指定OCSP回應程式位址、會覆寫在憑證檔案中找到的OCSP位址。

哪些類型的伺服器會啟用撤銷檢查？

儲存陣列會在連線AutoSupport 至某個伺服器、外部金鑰管理伺服器（EKMS）、輕量型SSL目錄存取傳輸協定（LDAPS）伺服器或Syslog伺服器時、執行撤銷檢查。