憑證
SANtricity 11.6

NetApp
February 12, 2024

目錄

憑證

概念

憑證的運作方式

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。

憑證可確保Web通訊只能在指定的伺服器與用戶端之間以加密形式私下傳輸且不會變更。使用System Manager、您可以在主機管理系統（做為用戶端）上的瀏覽器與儲存系統（做為伺服器）中的控制器之間管理憑證。

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：

- root（根）-在階層頂端是根憑證、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。
- 中繼-從根目錄下分支是中繼憑證。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：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。不過、自我簽署的憑證並未使用與CA簽署的憑證相同的信任鏈結。

自我簽署的憑證並非瀏覽器的「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。

用於金鑰管理伺服器的憑證

如果您使用具有磁碟機安全功能的外部金鑰管理伺服器、也可以管理該伺服器與控制器之間的驗證憑證。

憑證術語

下列條款適用於憑證管理。

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。
憑證鏈結	將安全層新增至憑證的檔案階層。一般而言、此鏈包括階層頂端的一個根憑證、一個或多個中繼憑證、以及識別實體的伺服器憑證。
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。
中介憑證	一個或多個中繼憑證會從憑證鏈結的根目錄下分支。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。
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。
Keystore	Keystore是主機管理系統上的儲存庫、內含私密金鑰及其對應的公開金鑰和憑證。這些金鑰和憑證可識別您自己的實體、例如控制器。
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。
根憑證	根憑證位於憑證鏈結階層的頂端、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。
簽署的憑證	由憑證授權單位（CA）驗證的憑證。此資料檔案包含私密金鑰、可確保資料以加密形式透過HTTPS連線在伺服器與用戶端之間傳送。此外、已簽署的憑證還包含實體擁有者（通常是伺服器或網站）的詳細資料、以及由字母和數字組成的數位簽章。簽署的憑證使用信任鏈、因此最常用於正式作業環境。也稱為「CA簽署的憑證」或「管理憑證」。

期限	說明
自我簽署的憑證	自行簽署的憑證由實體擁有者驗證。此資料檔案包含私密金鑰、可確保資料以加密形式透過HTTPS連線在伺服器與用戶端之間傳送。其中也包含由字母和數字組成的數位簽名。自我簽署的憑證不會使用與CA簽署憑證相同的信任鏈結、因此最常用於測試環境。也稱為「預先安裝」憑證。
伺服器憑證	伺服器憑證位於憑證鏈結的底部。它會識別您的特定實體、例如網站或其他裝置。儲存系統中的每個控制器都需要個別的伺服器憑證。

使用方法

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。

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**：完成並提交控制器的**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、然後將檔案提交給憑證授權單位（CA）。

開始之前

- 您必須知道每個控制器的IP位址或DNS名稱。

關於這項工作

CSR提供組織、控制器IP位址或DNS名稱的相關資訊、以及識別控制器中Web伺服器的金鑰配對。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。

> 提交至CA後、請勿產生新的CSR。產生CSR時、系統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金鑰庫中。當您收到簽署的憑證並將其匯入Keystore時、系統會確保私密金鑰和公開金鑰都是原始配對。因此、在將新的CSR提交給CA之後、您不得產生新的CSR。如果您這麼做、控制器就會產生新的金鑰、而且您從CA收到的憑證將無法運作。

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、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. 找到下載的CSR檔案。資料夾位置取決於您的瀏覽器。
7. 將CSR檔案提交給CA、並以PEEM格式要求簽署的憑證。
8. 等待CA傳回憑證、然後前往 [步驟2：匯入控制器的簽署憑證]。

步驟**2**：匯入控制器的簽署憑證

收到簽署的憑證之後、您會匯入控制器的檔案。

開始之前

- CA傳回簽署的憑證檔案。
- 這些檔案可在您的本機系統上使用。
- 如果CA提供鏈結的憑證（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

鼠右鍵並選取*功能表：All Tasks（所有工作）[Export（匯出）]*）。匯出完成後、會針對鏈中的每個憑證檔案顯示一個CER.檔案。

關於這項工作

本工作說明如何上傳憑證檔案。

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 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。

   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。

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*）。

   此時將打開確認*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」。

   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、可在控制器做為用戶端（而非伺服器）、LDAPS憑證及身分識別聯盟憑證時、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：非常見工作**[**刪除**]**」

   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」。

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。

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、然後您可以使用它來向金鑰管理伺服器信任的CA要求已簽署的用戶端憑證。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。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. 從金鑰管理伺服器信任的CA要求已簽署的用戶端憑證。
6. 當您擁有用戶端憑證時、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。

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。
- 您有已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）、並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伺服器憑證檔案、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。

> 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。

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。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。

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. 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。

   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*）」。

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**以進行外部金鑰管理？

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金鑰管理互通性傳輸協定（KMIP）要求。若要取得用戶端憑證、請使用System Manager為儲存陣列完成CSR。然後、您可以將CSR上傳至金鑰管理伺服器、然後從該伺服器產生用戶端憑證。取得用戶端憑證後、請將該檔案複製到您要存取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。從金鑰管理伺服器擷取伺服器憑證檔案、然後將該檔案複製到您正在存取System Manager的主機。

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。