管理證書

StorageGRID software

NetApp
May 29, 2026

目錄

管理證書 1
- 管理安全證書 1
  - 存取安全憑證 1
  - 安全證書詳細信息 5
  - 證書範例 9
- 支援的伺服器憑證類型 10
- 設定管理介面證書 10
  - 新增自訂管理介面證書 11
  - 恢復預設管理介面證書 13
  - 使用腳本產生新的自簽名管理介面證書 14
  - 下載或複製管理介面證書 15
- 配置 S3 API 證書 15
  - 新增自訂 S3 API 證書 16
  - 恢復預設的 S3 API 證書 18
  - 下載或複製 S3 API 證書 19
- 複製網格 CA 證書 20
- 為FabricPool配置StorageGRID證書 20
- 設定客戶端證書 21
  - 新增客戶端證書 22
  - 編輯客戶端證書 25
  - 附加新的客戶端憑證 25
  - 下載或複製客戶端證書 27
  - 刪除客戶端證書 27

管理證書

管理安全證書

安全性憑證是用於在StorageGRID組件之間以及StorageGRID組件與外部系統之間建立安全、可信任連接的小型資料檔案。

StorageGRID使用兩種類型的安全性憑證：

- 使用 HTTPS 連線時需要*伺服器憑證*。伺服器憑證用於在客戶端和伺服器之間建立安全連接，向客戶端驗證伺服器的身份並為資料提供安全通訊路徑。伺服器和客戶端各自擁有一份憑證副本。
- *用戶端憑證*向伺服器驗證用戶端或使用者身份，提供比單獨使用密碼更安全的身份驗證。客戶端證書不加密資料。

當客戶端使用 HTTPS 連接到伺服器時，伺服器會使用包含公鑰的伺服器憑證進行回應。用戶端透過將伺服器簽章與其憑證副本上的簽章進行比較來驗證此憑證。如果簽章匹配，客戶端將使用相同的公鑰與伺服器開始會話。

StorageGRID可作為某些連線（例如負載平衡器端點）的伺服器，或充當其他連線（例如 CloudMirror 複製服務）的用戶端。

預設網格 **CA** 憑證

StorageGRID包括一個內建憑證授權單位 (CA)，它在系統安裝期間產生內部 Grid CA 憑證。預設情況下，使用 Grid CA 憑證來保護內部StorageGRID流量。外部憑證授權單位 (CA) 可以頒發完全符合您組織的資訊安全策略的自訂憑證。雖然您可以在非生產環境中使用 Grid CA 證書，但生產環境的最佳做法是使用外部憑證授權單位簽署的自訂憑證。也支援沒有證書的不安全連接，但不建議。

- 自訂 CA 憑證不會刪除內部憑證；但是，自訂憑證應該是用於驗證伺服器連線的憑證。
- 所有客製化證書必須滿足"伺服器證書的系統強化指南"。
- StorageGRID支援將來自 CA 的憑證捆綁到單一檔案中（稱為 CA 憑證包）。

> StorageGRID還包括所有網格上相同的作業系統 CA 憑證。在生產環境中，請確保指定由外部憑證授權單位簽署的自訂憑證來取代作業系統 CA 憑證。

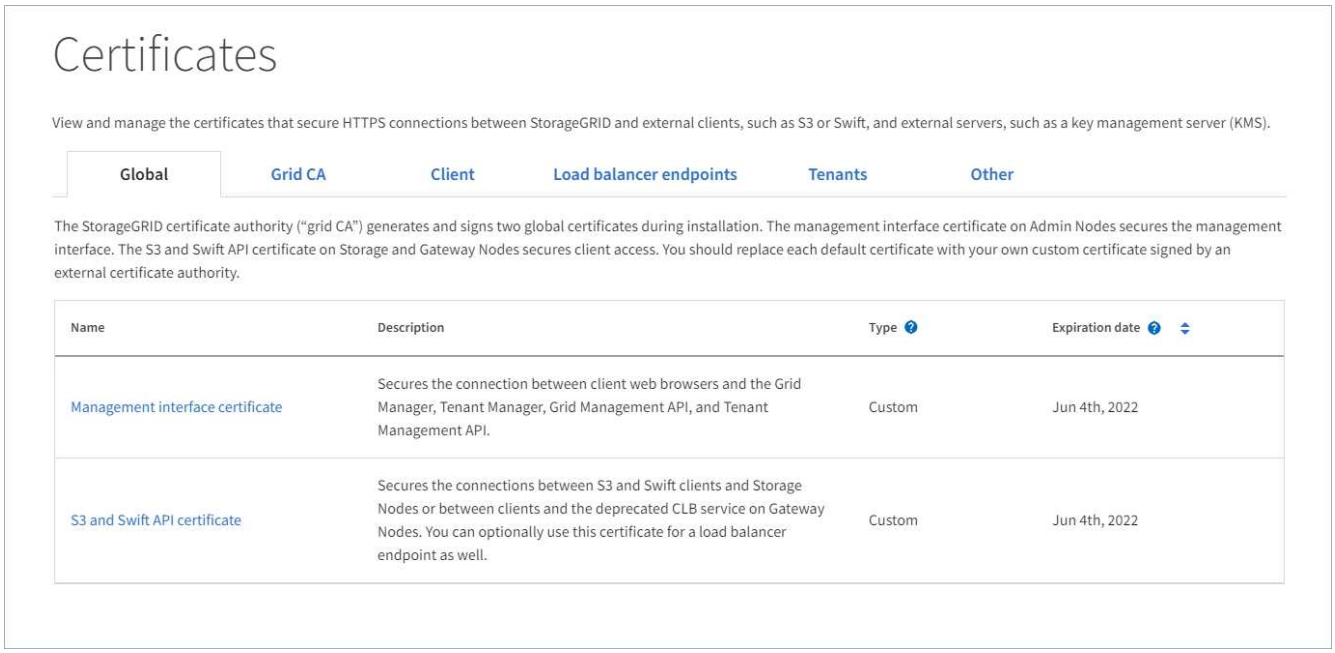
伺服器和客戶端憑證類型的變體以多種方式實現。在配置系統之前，您應該準備好特定StorageGRID配置所需的所有憑證。

存取安全憑證

您可以在單一位置存取有關所有StorageGRID憑證的信息，以及每個憑證的設定工作流程的連結。

步驟

1. 從網格管理器中，選擇 配置 > 安全性 > 證書。



2. 選擇「證書」頁面上的標籤以取得有關每個證書類別的資訊並存取證書設定。如果您有"適當的許可"。

   - 全域：保護從 Web 瀏覽器和外部 API 用戶端存取StorageGRID 的安全性。
   - **Grid CA**：保護內部StorageGRID流量。
   - 客戶端：保護外部客戶端和StorageGRID Prometheus 資料庫之間的連線。
   - 負載平衡器端點：保護 S3 用戶端與StorageGRID負載平衡器之間的連線。
   - 租用戶：保護與身分識別聯合伺服器或從平台服務端點到 S3 儲存資源的連線。
   - 其他：保護需要特定憑證的StorageGRID連線。

   下面描述了每個選項卡，並提供了指向其他證書詳細資訊的連結。

全球的

全域憑證可確保從 Web 瀏覽器和外部 S3 API 用戶端存取StorageGRID 的安全性。在安裝過程中，StorageGRID憑證授權單位最初會產生兩個全域憑證。生產環境的最佳實踐是使用由外部憑證授權單位簽署的自訂憑證。

- [管理介面證書]：保護客戶端 Web 瀏覽器與StorageGRID管理介面的連線。
- S3 API 證書：保護客戶端 API 與儲存節點、管理節點和網關節點的連接，S3 用戶端應用程式使用這些連接上傳和下載物件資料。

有關已安裝的全域憑證的資訊包括：

- 名稱：證書名稱以及證書管理連結。
- 描述
- 類型：自訂或預設。 + 您應該始終使用自訂憑證來提高電網安全性。
- 到期日：如果使用預設證書，則不顯示到期日。

你可以：

- 將預設證書取代為由外部證書頒發機構簽署的自訂證書，以提高網格安全性：
  - "取代預設的StorageGRID產生的管理介面證書"用於網格管理器和租戶管理器連線。
  - "替換 S3 API 證書"用於儲存節點和負載平衡器端點（可選）連線。
- "恢復預設管理介面證書" 。
- "恢復預設的 S3 API 證書" 。
- "使用腳本產生新的自簽名管理介面證書" 。
- 複製或下載"管理介面證書"或者"S3 API 證書"。

網格**CA**

這網格CA證書由StorageGRID憑證授權單位在StorageGRID安裝期間生成，可保護所有內部StorageGRID流量。

證書資訊包括證書有效期限、證書內容等。

你可以"複製或下載 Grid CA 憑證"，但您無法更改它。

用戶端

客戶端憑證由外部憑證授權單位生成，確保外部監控工具與StorageGRID Prometheus 資料庫之間的連線安全。

證書表為每個配置的用戶端證書都有一行，並指示該證書是否可用於 Prometheus 資料庫訪問，以及證書到期日。

你可以：

- "上傳或產生新的客戶端憑證。"
- 選擇證書名稱以顯示證書詳細信息，您可以在其中：

- "更改客戶端證書名稱。"
- "設定Prometheus存取權限。"
- "上傳並替換客戶端憑證。"
- "複製或下載客戶端憑證。"
- "刪除客戶端證書。"

◦ 選擇*操作*快速"編輯"，"附" ， 或者"消除"客戶端證書。您最多可以選擇 10 個客戶端證書，並使用操作 > 刪除 一次將其刪除。

負載平衡器端點

負載平衡器端點憑證保護 S3 用戶端與網關節點和管理節點上的StorageGRID負載平衡器服務之間的連線。

負載平衡器端點表為每個配置的負載平衡器端點都有一行，並指示該端點是否使用全域 S3 API 憑證或自訂負載平衡器端點憑證。也會顯示每個憑證的到期日期。

端點憑證的變更可能需要長達 15 分鐘才能套用到所有節點。

你可以：

◦ "查看負載平衡器端點"，包括其證書詳細資訊。

◦ "為FabricPool指定負載平衡器端點憑證。"

◦ "使用全域 S3 API 證書"而不是產生新的負載平衡器端點憑證。

租戶

租戶可以使用身份聯合伺服器憑證或者平台服務端點憑證以確保與StorageGRID 的連線安全。

租戶表為每個租戶分配一行，並指示每個租戶是否有權使用自己的身份來源或平台服務。

你可以：

◦ "選擇租戶名稱以登入租戶管理器"

◦ "選擇租戶名稱以查看租戶身份聯合詳細信息"

◦ "選擇租戶名稱查看租戶平台服務詳情"

◦ "在端點建立期間指定平台服務端點憑證"

其他

StorageGRID使用其他安全性憑證來達到特定目的。這些證書按其功能名稱列出。其他安全性憑證包括：

◦ 雲端儲存池憑證

◦ 電子郵件警報通知證書

◦ 外部系統日誌伺服器證書

◦ 電網聯合連接證書

◦ 身分聯合憑證

- 金鑰管理伺服器 (KMS) 證書
- 單一登入憑證

資訊指示功能使用的憑證類型及其伺服器和用戶端憑證到期日期（如適用）。選擇函數名稱將開啟一個瀏覽器選項卡，您可以在其中查看和編輯憑證詳細資訊。

僅當您擁有"適當的許可"。

你可以：

- "為 S3、C2S S3 或 Azure 指定雲端儲存池憑證"
- "指定警報電子郵件通知的證書"
- "使用外部系統日誌伺服器的證書"
- "輪換電網聯合連接證書"
- "查看並編輯身份聯合證書"
- "上傳金鑰管理伺服器 (KMS) 伺服器和用戶端證書"
- "為信賴方信任手動指定 SSO 證書"

安全證書詳細信息

以下描述了每種類型的安全證書，並附有實施說明的連結。

管理介面證書

證書類型	描述	導航位置	細節
伺服器	驗證用戶端 Web 瀏覽器與StorageGRID管理介面之間的連接，允許使用者存取網格管理器和租用戶管理器而不會出現安全警告。 此憑證還驗證網格管理 API 和租用戶管理 API 連線。 您可以使用安裝期間建立的預設憑證或上傳自訂憑證。	設定 > 安全 > 憑證，選擇 全域 選項卡，然後選擇 管理介面憑證	"設定管理介面證書"

S3 API 證書

證書類型	描述	導航位置	細節
伺服器	驗證與儲存節點和負載平衡器端點的安全 S3 用戶端連線（可選）。	設定 > 安全 > 憑證，選擇 全域 選項卡，然後選擇 **S3 API** 憑證	"配置 S3 API 證書"

網格**CA**證書

查看預設網格 CA 憑證描述。

管理員客戶端憑證

證書類型	描述	導航位置	細節
用戶端	安裝在每個客戶端上，允許StorageGRID驗證外部客戶端存取。 • 允許授權的外部用戶端存取StorageGRID Prometheus 資料庫。 • 允許使用外部工具對StorageGRID進行安全監控。	配置 > 安全性 > 憑證，然後選擇 用戶端 選項卡	"設定客戶端證書"

負載平衡器端點憑證

證書類型	描述	導航位置	細節
伺服器	驗證 S3 用戶端與網關節點和管理節點上的StorageGRID負載平衡器服務之間的連線。您可以在設定負載平衡器端點時上傳或產生負載平衡器憑證。用戶端應用程式在連接到StorageGRID以儲存和檢索物件資料時使用負載平衡器憑證。 您也可以使用全域的自訂版本S3 API 證書憑證來驗證與負載平衡器服務的連線。如果使用全域憑證來驗證負載平衡器連接，則無需為每個負載平衡器端點上傳或產生單獨的憑證。 *注意：*用於負載平衡器驗證的憑證是正常StorageGRID作業期間使用最多的憑證。	配置 > 網路 > 負載平衡器端點	• "配置負載平衡器端點" • "為FabricPool建立負載平衡器端點"

雲端儲存池端點憑證

證書類型	描述	導航位置	細節
伺服器	驗證從StorageGRID雲端儲存池到外部儲存位置（例如 S3 Glacier 或 Microsoft Azure Blob 儲存體）的連線。每種雲端提供者類型都需要不同的憑證。	**ILM** > 儲存池	"建立雲端儲存池"

電子郵件警報通知證書

證書類型	描述	導航位置	細節
伺服器和客戶端	驗證用於警報通知的SMTP 電子郵件伺服器和StorageGRID之間的連線。 • 如果與 SMTP 伺服器的通訊需要傳輸層安全性 (TLS)，則必須指定電子郵件伺服器 CA 憑證。 • 僅當 SMTP 電子郵件伺服器需要用戶端憑證進行驗證時才指定用戶端憑證。	警報 > 電子郵件設定	"設定警報的電子郵件通知"

外部系統日誌伺服器證書

證書類型	描述	導航位置	細節
伺服器	對在StorageGRID中記錄事件的外部系統日誌伺服器之間的 TLS 或 RELP/TLS 連線進行驗證。 *注意：*與外部系統日誌伺服器的 TCP 、RELP/TCP 和 UDP 連線不需要外部系統日誌伺服器憑證。	配置 > 監控 > 審計和系統日誌伺服器	"使用外部系統日誌伺服器"

電網聯合連接憑證

證書類型	描述	導航位置	細節
伺服器和客戶端	對目前StorageGRID系統和網格聯合連接中的另一個網格之間所傳送的資訊進行驗證和加密。	配置 > 系統 > 網格聯合	• "建立電網聯合連接" • "輪換連接證書"

身分聯合憑證

證書類型	描述	導航位置	細節
伺服器	驗證StorageGRID與外部身分提供者（例如 Active Directory、OpenLDAP 或 Oracle Directory Server）之間的連線。用於身分聯合，允許管理群組和使用者由外部系統管理。	配置 > 存取控制 > 身份聯合	"使用身分聯合"

金鑰管理伺服器 **(KMS)** 證書

證書類型	描述	導航位置	細節
伺服器和客戶端	驗證StorageGRID與外部金鑰管理伺服器 (KMS) 之間的連接，該伺服器為StorageGRID設備節點提供加密金鑰。	配置 > 安全 > 金鑰管理伺服器	"新增金鑰管理伺服器（KMS）"

平台服務端點憑證

證書類型	描述	導航位置	細節
伺服器	驗證從StorageGRID平台服務到 S3 儲存資源的連線。	租用戶管理員 > 儲存 **(S3)** > 平台服務端點	"創建平台服務端點" "編輯平台服務端點"

單一登入 **(SSO)** 證書

證書類型	描述	導航位置	細節
伺服器	驗證用於單一登入 (SSO) 請求的身份聯合服務（例如 Active Directory 聯合驗證服務 (AD FS)）和StorageGRID之間的連線。	配置 > 存取控制 > 單一登入	"配置單一登入"

證書範例

範例 **1**：負載平衡器服務

在此範例中， StorageGRID充當伺服器。

1. 您設定負載平衡器端點並在StorageGRID中上傳或產生伺服器憑證。
2. 您配置與負載平衡器端點的 S3 用戶端連接，並將相同的憑證上傳到用戶端。
3. 當客戶端想要儲存或檢索資料時，它使用 HTTPS 連接到負載平衡器端點。

4. StorageGRID使用包含公鑰的伺服器憑證和基於私密金鑰的簽章進行回應。
5. 用戶端透過將伺服器簽章與其憑證副本上的簽章進行比較來驗證此憑證。如果簽章匹配，客戶端將使用相同的公鑰開始會話。
6. 客戶端將物件資料傳送到StorageGRID。

範例 **2**：外部金鑰管理伺服器 **(KMS)**

在此範例中， StorageGRID充當用戶端。

1. 使用外部金鑰管理伺服器軟體，您可以將StorageGRID設定為 KMS 用戶端並取得 CA 簽署的伺服器憑證、公用用戶端憑證以及用戶端憑證的私密金鑰。
2. 使用網格管理器，您可以設定 KMS 伺服器並上傳伺服器和用戶端憑證以及用戶端私鑰。
3. 當StorageGRID節點需要加密金鑰時，它會向 KMS 伺服器發出請求，其中包含來自憑證的資料和基於私密金鑰的簽章。
4. KMS 伺服器驗證憑證簽章並決定它可以信任StorageGRID。
5. KMS 伺服器使用已驗證的連線進行回應。

支援的伺服器憑證類型

StorageGRID系統支援使用 RSA 或 ECDSA（橢圓曲線數位簽章演算法）加密的自訂憑證。

安全性原則的密碼類型必須與伺服器憑證類型相符。例如，RSA 密碼需要 RSA 證書，ECDSA 密碼需要 ECDSA 證書。看"管理安全證書" 。如果您配置了與伺服器憑證不相容的自訂安全性原則，您可以"暫時恢復預設安全策略"。

有關StorageGRID如何保護客戶端連接的更多信息，請參閱"S3 用戶端的安全性"。

設定管理介面證書

您可以用單一自訂證書取代預設管理介面證書，該證書允許使用者存取網格管理器和租戶管理器而不會遇到安全警告。您也可以還原預設管理介面憑證或產生新的憑證。

關於此任務

預設情況下，每個管理節點都會頒發由網格 CA 簽署的憑證。這些 CA 簽署的憑證可以被單一通用自訂管理介面憑證和對應的私鑰所取代。

由於所有管理節點都使用單一自訂管理介面證書，因此如果用戶端在連接到網格管理器和租用戶管理器時需要驗證主機名，則必須將證書指定為通配符或多網域證書。定義自訂證書，使其與網格中的所有管理節點相符。

您需要在伺服器上完成配置，並且根據您使用的根憑證授權單位 (CA)，使用者可能還需要在用於存取網格管理員和租用戶管理員的 Web 瀏覽器中安裝網格 CA 憑證。

為了確保操作不會因伺服器憑證失敗而中斷，當此伺服器憑證即將過期時，會觸發*管理介面伺服器憑證過期*警報。根據需要，您可以透過選擇 **CONFIGURATION** > **Security** > **Certificates** 並查看 Global 標籤上的管理介面憑證的到期日期來查看目前憑證的到期時間。

如果您使用網域名稱而不是 IP 位址存取網格管理員或租用戶管理器，則在發生下列任一情況時，瀏覽器將顯示憑證錯誤，且沒有繞過選項：

- 您的自訂管理介面憑證已過期。
- 你從自訂管理介面證書恢復為預設伺服器憑證。

新增自訂管理介面證書

若要新增自訂管理介面證書，您可以提供自己的證書或使用網格管理器產生證書。

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*管理介面憑證*。
3. 選擇*使用自訂憑證*。
4. 上傳或產生證書。

上傳證書

上傳所需的伺服器憑證檔案。

a. 選擇*上傳證書*。

b. 上傳所需的伺服器憑證檔案：

   - 伺服器憑證：自訂伺服器憑證檔案（PEM編碼）。
   - 證書私鑰：自訂伺服器憑證私鑰文件(`.key`）。

     EC 私鑰必須為 224 位元或更大。 RSA 私鑰必須為 2048 位元或更大。

   - **CA** 包：一個可選文件，包含來自每個中間發行憑證機構 (CA) 的憑證。該文件應包含每個 PEM 編碼的 CA 憑證文件，並按憑證鏈順序連接。

c. 展開*證書詳細資訊*以查看您上傳的每個證書的元資料。如果您上傳了可選的 CA 包，則每個憑證都會顯示在其自己的標籤上。

   - 選擇*下載憑證*儲存憑證檔案或選擇*下載 CA 套件*儲存憑證套件。

     指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

   - 選擇*複製憑證 PEM*或*複製 CA 套件 PEM*以複製憑證內容以便貼上到其他地方。

d. 選擇*儲存*。+ 自訂管理介面憑證用於與網格管理器、租用戶管理員、網格管理器 API 或租用戶管理器 API 的所有後續新連接。

產生證書

產生伺服器憑證檔案。

生產環境的最佳實務是使用由外部憑證授權單位簽署的自訂管理介面憑證。

a. 選擇*產生證書*。

b. 指定證書資訊：

場地	描述
網域	證書中包含的一個或多個完全限定域名。使用 * 作為通配符來表示多個網域。
智慧財產	證書中包含的一個或多個 IP 位址。
主題（可選）	證書擁有者的 X.509 主題或專有名稱 (DN)。 如果此欄位未輸入任何值，則產生的憑證將使用第一個網域名稱或 IP 位址作為主題通用名稱 (CN)。

場地	描述
有效天數	證書建立後過期的天數。
新增密鑰使用擴展	如果選擇（預設和推薦），密鑰使用和擴展密鑰使用擴充將新增至產生的憑證。 這些擴充定義了憑證中包含的金鑰的用途。 注意：請選取此複選框，除非當憑證包含這些擴充功能時您遇到與舊用戶端的連線問題。

c. 選擇*生成*。

d. 選擇*證書詳細資訊*以查看產生的證書的元資料。

- 選擇*下載證書*儲存證書檔案。

  指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。

e. 選擇*儲存*。+ 自訂管理介面憑證用於與網格管理器、租用戶管理員、網格管理器 API 或租用戶管理器 API 的所有後續新連接。

5. 重新整理頁面以確保 Web 瀏覽器已更新。

> 上傳或產生新證書後，請等待最多一天的時間以清除所有相關的證書到期警報。

6. 新增自訂管理介面憑證後，管理介面憑證頁面將顯示正在使用的憑證的詳細憑證資訊。 +您可以根據需要下載或複製憑證PEM。

恢復預設管理介面證書

您可以還原使用網格管理器和租用戶管理器連線的預設管理介面憑證。

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*管理介面憑證*。
3. 選擇*使用預設證書*。

   當您還原預設管理介面憑證時，您設定的自訂伺服器憑證檔案將會被刪除，並且無法從系統中復原。所有後續的新用戶端連線均使用預設管理介面憑證。

4. 重新整理頁面以確保 Web 瀏覽器已更新。

使用腳本產生新的自簽名管理介面證書

如果需要嚴格的主機名稱驗證，您可以使用腳本產生管理介面憑證。

開始之前

- 你有"特定存取權限"。
- 你有 `Passwords.txt`文件。

關於此任務

生產環境的最佳實務是使用由外部憑證授權單位簽署的憑證。

步驟

1. 取得每個管理節點的完全限定網域名稱 (FQDN)。
2. 登入主管理節點：
   a. 輸入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入 `Passwords.txt`文件。
   c. 輸入以下命令切換到root： `su -`
   d. 輸入 `Passwords.txt`文件。

   當您以 root 身分登入時，提示字元將從 `$`到 `#`。
3. 使用新的自簽章憑證設定StorageGRID 。

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - 為了 `--domains`，使用通配符來表示所有管理節點的完全限定網域名稱。例如， `*.ui.storagegrid.example.com`使用 `*` 通配符來表示 `admin1.ui.storagegrid.example.com`和 `admin2.ui.storagegrid.example.com`。
   - 放 `--type`到 `management`配置管理介面證書，供Grid Manager和Tenant Manager使用。
   - 預設情況下，產生的憑證有效期為一年（365 天），必須在到期前重新建立。您可以使用 `--days`參數來覆蓋預設有效期。

     > ⓘ 證書有效期限從 `make-certificate`正在運行。您必須確保管理用戶端與StorageGRID同步到相同時間來源；否則，用戶端可能會拒絕該憑證。

     ```
     $ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
     ```

     結果輸出包含管理 API 用戶端所需的公共憑證。
4. 選擇並複製證書。

   在您的選擇中包含 BEGIN 和 END 標籤。
5. 退出命令 shell。 `$ exit`

6. 確認證書已設定：
   a. 存取網格管理器。
   b. 選擇 設定 > 安全 > 憑證
   c. 在*全域*標籤上，選擇*管理介面憑證*。
7. 配置您的管理用戶端以使用您複製的公共憑證。包括 BEGIN 和 END 標籤。

下載或複製管理介面證書

您可以儲存或複製管理介面證書內容以供其他地方使用。

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*管理介面憑證*。
3. 選擇“伺服器”或“**CA** 套件”選項卡，然後下載或複製憑證。

下載憑證檔案或 **CA** 套件

下載憑證或 CA 套件 `.pem`文件。如果您使用可選的 CA 捆綁包，捆綁包中的每個憑證都會顯示在其自己的子選項卡上。

a. 選擇*下載憑證*或*下載 CA 套件*。

   如果您正在下載 CA 捆綁包，則 CA 捆綁包二級標籤中的所有憑證都會作為單一檔案下載。

b. 指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

複製憑證或 **CA** 捆綁包 **PEM**

複製證書文字並貼上到其他地方。如果您使用可選的 CA 捆綁包，捆綁包中的每個憑證都會顯示在其自己的子選項卡上。

a. 選擇*複製憑證 PEM*或*複製 CA 套件 PEM*。

   如果您正在複製 CA 捆綁包，則 CA 捆綁包輔助標籤中的所有憑證都會一起複製。

b. 將複製的憑證貼到文字編輯器中。
c. 儲存帶有擴展名的文字文件 `.pem`。

   例如： `storagegrid_certificate.pem`

配置 **S3 API** 證書

您可以替換或還原用於 S3 用戶端連接到儲存節點或負載平衡器端點的伺服器憑證。替換

的自訂伺服器憑證特定於您的組織。

此版本的文件網站已刪除 Swift 詳細資訊。看 "StorageGRID 11.8：設定 S3 和 Swift API 證書"。

關於此任務

預設情況下，每個儲存節點都會頒發由網格 CA 簽署的 X.509 伺服器憑證。這些 CA 簽署的憑證可以被單一通用自訂伺服器憑證和相應的私鑰所取代。

所有儲存節點都使用單一自訂伺服器證書，因此如果用戶端在連接到儲存端點時需要驗證主機名，則必須將證書指定為通配符或多網域證書。定義自訂證書，使其與網格中的所有儲存節點相符。

在伺服器上完成設定後，您可能還需要在用於存取系統的 S3 API 用戶端中安裝 Grid CA 證書，具體取決於您使用的根憑證授權單位 (CA)。

為了確保操作不會因伺服器憑證失敗而中斷，當根伺服器憑證即將過期時，會觸發*S3 API 的全域伺服器憑證過期*警報。根據需要，您可以透過選擇 **CONFIGURATION** > **Security** > **Certificates** 並查看 Global 標籤上 S3 API 憑證的到期日期來查看目前憑證的到期時間。

您可以上傳或產生自訂 S3 API 憑證。

新增自訂 **S3 API** 證書

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*S3 API 憑證*。
3. 選擇*使用自訂憑證*。
4. 上傳或產生證書。

上傳證書

上傳所需的伺服器憑證檔案。

a. 選擇*上傳證書*。

b. 上傳所需的伺服器憑證檔案：

- 伺服器憑證：自訂伺服器憑證檔案（PEM編碼）。
- 證書私鑰：自訂伺服器憑證私鑰文件(`.key`）。

> EC 私鑰必須為 224 位元或更大。 RSA 私鑰必須為 2048 位元或更大。

- **CA** 包：一個可選文件，包含來自每個中間頒發憑證機構的憑證。該文件應包含每個 PEM 編碼的 CA 憑證文件，並按憑證鏈順序連接。

c. 選擇憑證詳細資訊以顯示已上傳的每個自訂 S3 API 憑證的元資料和 PEM。如果您上傳了可選的 CA 包，則每個憑證都會顯示在其自己的標籤上。

- 選擇*下載憑證*儲存憑證檔案或選擇*下載 CA 套件*儲存憑證套件。

  指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選擇*複製憑證 PEM*或*複製 CA 套件 PEM*以複製憑證內容以便貼上到其他地方。

d. 選擇*儲存*。

自訂伺服器憑證用於後續新的 S3 用戶端連線。

產生證書

產生伺服器憑證檔案。

a. 選擇*產生證書*。

b. 指定證書資訊：

場地	描述
網域	證書中包含的一個或多個完全限定域名。使用 * 作為通配符來表示多個網域。
智慧財產	證書中包含的一個或多個 IP 位址。
主題（可選）	證書擁有者的 X.509 主題或專有名稱 (DN)。 如果此欄位未輸入任何值，則產生的憑證將使用第一個網域名稱或 IP 位址作為主題通用名稱 (CN)。
有效天數	證書建立後過期的天數。

場地	描述
新增密鑰使用擴展	如果選擇（預設和推薦），密鑰使用和擴展密鑰使用擴充將新增至產生的憑證。 這些擴充定義了憑證中包含的金鑰的用途。 注意：請選取此複選框，除非當憑證包含這些擴充功能時您遇到與舊用戶端的連線問題。

c. 選擇*生成*。

d. 選擇*證書詳細資訊*以顯示產生的自訂 S3 API 證書的元資料和 PEM。

- 選擇*下載證書*儲存證書檔案。

  指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。

e. 選擇*儲存*。

自訂伺服器憑證用於後續新的 S3 用戶端連線。

5. 選擇一個標籤以顯示預設StorageGRID伺服器憑證、已上傳的 CA 簽章憑證或產生的自訂憑證的元資料。

   上傳或產生新證書後，請等待最多一天的時間以清除所有相關的證書到期警報。

6. 重新整理頁面以確保 Web 瀏覽器已更新。

7. 新增自訂 S3 API 憑證後，S3 API 憑證頁面將顯示正在使用的自訂 S3 API 憑證的詳細憑證資訊。 +您可以根據需要下載或複製憑證PEM。

恢復預設的 **S3 API** 證書

您可以恢復使用預設 S3 API 憑證來將 S3 用戶端連接到儲存節點。但是，您不能將預設的 S3 API 憑證用於負載平衡器端點。

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*S3 API 憑證*。
3. 選擇*使用預設證書*。

   當您還原全域 S3 API 憑證的預設版本時，您設定的自訂伺服器憑證檔案將會被刪除，並且無法從系統中復原。預設 S3 API 憑證將用於後續新的 S3 用戶端與儲存節點的連接。

4. 選擇「確定」確認警告並恢復預設的 S3 API 憑證。

如果您具有 Root 存取權限，並且自訂 S3 API 憑證用於負載平衡器端點連接，則會顯示負載平衡器端點列表，這些端點將無法再使用預設 S3 API 憑證進行存取。前往"配置負載平衡器端點"編輯或刪除受影響的端點。

5. 重新整理頁面以確保 Web 瀏覽器已更新。

下載或複製 **S3 API** 證書

您可以儲存或複製 S3 API 憑證內容以供在其他地方使用。

步驟

1. 選擇 設定 > 安全 > 憑證。
2. 在*全域*標籤上，選擇*S3 API 憑證*。
3. 選擇“伺服器”或“**CA** 套件”選項卡，然後下載或複製憑證。

下載憑證檔案或 **CA** 套件

下載憑證或 CA 套件 `.pem`文件。如果您使用可選的 CA 捆綁包，捆綁包中的每個憑證都會顯示在其自己的子選項卡上。

a. 選擇*下載憑證*或*下載 CA 套件*。

   如果您正在下載 CA 捆綁包，則 CA 捆綁包二級標籤中的所有憑證都會作為單一檔案下載。

b. 指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

複製憑證或 **CA** 捆綁包 **PEM**

複製證書文字並貼上到其他地方。如果您使用可選的 CA 捆綁包，捆綁包中的每個憑證都會顯示在其自己的子選項卡上。

a. 選擇*複製憑證 PEM*或*複製 CA 套件 PEM*。

   如果您正在複製 CA 捆綁包，則 CA 捆綁包輔助標籤中的所有憑證都會一起複製。

b. 將複製的憑證貼到文字編輯器中。
c. 儲存帶有擴展名的文字文件 `.pem`。

   例如： `storagegrid_certificate.pem`

相關資訊

- "使用 S3 REST API"
- "配置 S3 端點域名"

複製網格 CA 證書

StorageGRID使用內部憑證授權單位 (CA) 來保護內部流量。如果您上傳自己的證書，此證書不會改變。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。

關於此任務

如果已配置自訂伺服器證書，則用戶端應用程式應使用自訂伺服器證書來驗證伺服器。他們不應該從StorageGRID系統複製 CA 憑證。

步驟

1. 選擇 **CONFIGURATION** > **Security** > **Certificates**，然後選擇 **Grid CA** 選項卡。
2. 在 證書 **PEM** 部分，下載或複製證書。

   下載證書文件

   下載證書 `.pem`文件。

   a. 選擇*下載證書*。
   b. 指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

      例如： `storagegrid_certificate.pem`

   複製證書 **PEM**

   複製證書文字並貼上到其他地方。

   a. 選擇*複製憑證 PEM*。
   b. 將複製的憑證貼到文字編輯器中。
   c. 儲存帶有擴展名的文字文件 `.pem`。

      例如： `storagegrid_certificate.pem`

為FabricPool配置StorageGRID證書

對於執行嚴格主機名稱驗證且不支援停用嚴格主機名稱驗證的 S3 用戶端（例如使用FabricPool的ONTAP用戶端），您可以在設定負載平衡器端點時產生或上傳伺服器憑證。

開始之前

- 你有"特定存取權限"。

- 您已使用"支援的網頁瀏覽器"。

關於此任務

建立負載平衡器端點時，您可以產生自簽章伺服器憑證或上傳已知憑證授權單位 (CA) 簽署的憑證。在生產環境中，您應該使用已知 CA 簽署的憑證。由 CA 簽署的憑證可以不間斷地輪替。它們也更安全，因為它們可以更好地防禦中間人攻擊。

以下步驟為使用FabricPool的 S3 用戶端提供了一般準則。如需更多詳細資訊和步驟，請參閱"為FabricPool配置StorageGRID"。

步驟

1. 或者，配置一個高可用性 (HA) 群組供FabricPool使用。
2. 建立一個 S3 負載平衡器端點供FabricPool使用。

   當您建立 HTTPS 負載平衡器端點時，系統會提示您上傳伺服器憑證、憑證私鑰和選用 CA 套件。

3. 將StorageGRID作為雲層附加到ONTAP。

   指定您上傳的 CA 憑證中所使用的負載平衡器端點連接埠和完全限定網域名稱。然後，提供 CA 憑證。

   如果中間 CA 頒發了StorageGRID證書，則必須提供中間 CA 證書。如果StorageGRID憑證是由根 CA 直接頒發的，則必須提供根 CA 憑證。

設定客戶端證書

用戶端憑證允許授權的外部用戶端存取StorageGRID Prometheus 資料庫，為外部工具監控StorageGRID提供一種安全的方式。

如果需要使用外部監控工具存取StorageGRID ，則必須使用 Grid Manager 上傳或產生用戶端證書，並將證書資訊複製到外部工具。

看"管理安全證書"和"配置自訂伺服器證書"。

為了確保操作不會因伺服器憑證失敗而中斷，當此伺服器憑證即將過期時，將觸發*憑證頁面上配置的用戶端憑證過期*警報。根據需要，您可以透過選擇 設定 > 安全 > 憑證 並查看用戶端標籤上的用戶端憑證的到期日期來查看目前憑證的到期時間。

如果您使用金鑰管理伺服器 (KMS) 來保護特殊配置的設備節點上的數據，請參閱有關"上傳 KMS 用戶端證書"。

開始之前

- 您擁有 Root 存取權限。
- 您已使用"支援的網頁瀏覽器"。
- 要設定客戶端憑證：
  - 您擁有管理節點的 IP 位址或網域名稱。
  - 如果您已設定StorageGRID管理介面證書，則您擁有用於設定管理介面憑證的 CA、用戶端憑證和私密金

鑰。

- 要上傳您自己的證書，該證書的私鑰可以在您的本機電腦上找到。
- 私鑰在創建時必須被保存或記錄。如果您沒有原始私鑰，則必須建立一個新的私鑰。

- 若要編輯客戶端憑證：
  - 您擁有管理節點的 IP 位址或網域名稱。
  - 要上傳您自己的證書或新證書，您的本機電腦上需要有私鑰、用戶端證書和 CA（如果使用）。

新增客戶端證書

若要新增客戶端證書，請使用下列步驟之一：

- [管理介面憑證已配置]
- CA核發的客戶端證書
- [從網格管理器產生的證書]

管理介面憑證已配置

如果已使用客戶提供的 CA、用戶端證書和私鑰配置了管理介面證書，請使用此程序新增用戶端證書。

步驟

1. 在網格管理員中，選擇 配置 > 安全性 > 憑證，然後選擇 用戶端 標籤。
2. 選擇“新增”。
3. 輸入證書名稱。
4. 若要使用外部監控工具存取 Prometheus 指標，請選擇 允許 **prometheus**。
5. 選擇*繼續*。
6. 對於*附加憑證*步驟，上傳管理介面憑證。
   a. 選擇*上傳證書*。
   b. 選擇*瀏覽*並選擇管理介面憑證文件(`.pem`）。
      - 選擇*用戶端憑證詳細資料*以顯示憑證元資料和憑證 PEM。
      - 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。
   c. 選擇*建立*將憑證保存在網格管理員中。

      新證書出現在客戶端選項卡上。
7. 設定外部監控工具，例如 Grafana。

CA核發的客戶端證書

如果未設定管理介面證書，且您計劃為 Prometheus 新增使用 CA 頒發的用戶端憑證和私鑰的用戶端證書，請使用此流程新增管理員用戶端憑證。

步驟

1. 執行以下步驟"設定管理介面證書"。
2. 在網格管理員中，選擇 配置 > 安全性 > 憑證，然後選擇 用戶端 標籤。
3. 選擇“新增”。
4. 輸入證書名稱。
5. 若要使用外部監控工具存取 Prometheus 指標，請選擇 允許 **prometheus**。
6. 選擇*繼續*。
7. 對於*附加憑證*步驟，上傳客戶端憑證、私密金鑰和 CA 捆綁檔案：
   a. 選擇*上傳證書*。
   b. 選擇「瀏覽」並選擇用戶端憑證、私鑰和 CA 捆綁文件(`.pem`）。
      - 選擇*用戶端憑證詳細資料*以顯示憑證元資料和憑證 PEM。
      - 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。
   c. 選擇*建立*將憑證保存在網格管理員中。

      新證書出現在客戶端選項卡上。
8. 設定外部監控工具，例如 Grafana。

從網格管理器產生的證書

如果未設定管理介面證書，且您計劃為使用 Grid Manager 中的產生憑證功能的 Prometheus 新增用戶端證書，請使用此流程新增管理員用戶端憑證。

步驟

1. 在網格管理員中，選擇 配置 > 安全性 > 憑證，然後選擇 用戶端 標籤。
2. 選擇“新增”。
3. 輸入證書名稱。
4. 若要使用外部監控工具存取 Prometheus 指標，請選擇 允許 **prometheus**。
5. 選擇*繼續*。
6. 對於*附加憑證*步驟，選擇*產生憑證*。
7. 指定證書資訊：
   - 主題（可選）：證書擁有者的 X.509 主題或專有名稱 (DN)。
   - 有效天數：產生的憑證從產生時開始的有效天數。
   - 新增金鑰使用擴充功能：如果選擇（預設和建議），則金鑰使用和擴充金鑰使用擴充將新增至產生的憑證中。

     這些擴充定義了憑證中包含的金鑰的用途。

     除非憑證包含這些擴充功能時遇到與舊客戶端的連線問題，否則請選取此核取方塊。
8. 選擇*生成*。

9. 選擇*用戶端憑證詳細資料*以顯示憑證元資料和憑證 PEM。

   關閉對話方塊後，您將無法查看憑證私鑰。將金鑰複製或下載到安全位置。

   - 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。
   - 選擇*下載證書*儲存證書檔案。

     指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選擇*複製私密金鑰*複製憑證私鑰以便貼到其他地方。
   - 選擇*下載私鑰*將私鑰儲存為檔案。

     指定私鑰檔案名稱和下載位置。

10. 選擇*建立*將憑證保存在網格管理員中。

    新證書出現在客戶端選項卡上。

11. 在網格管理員中，選擇 配置 > 安全性 > 憑證，然後選擇 全域 標籤。
12. 選擇*管理介面證書*。
13. 選擇*使用自訂憑證*。
14. 從上傳 certificate.pem 和 private_key.pem 文件客戶端證書詳細信息步。無需上傳 CA 包。
    a. 選擇*上傳憑證*，然後選擇*繼續*。
    b. 上傳每個證書文件(`.pem`）。
    c. 選擇*儲存*將憑證儲存在網格管理員中。

       新證書出現在管理介面證書頁面上。

15. 設定外部監控工具，例如 Grafana。

設定外部監控工具

步驟

1. 在您的外部監控工具（例如 Grafana）上設定以下設定。
   a. 名稱：輸入連線的名稱。

      StorageGRID不需要此信息，但您必須提供名稱來測試連接。

   b. **URL**：輸入管理節點的網域名稱或 IP 位址。指定 HTTPS 和連接埠 9091。

      例如： `https://admin-node.example.com:9091`

   c. 啟用 **TLS** 用戶端身份驗證 和 使用 **CA** 憑證。
   d. 在 TLS/SSL 身份驗證詳細資訊下，複製並貼上：+

- 管理介面CA憑證到**CA Cert**
- 客戶端證書到客戶端證書
- 客戶端金鑰的私鑰

e. **ServerName**：輸入管理節點的網域名稱。

ServerName 必須與管理介面憑證中顯示的網域名稱相符。

2. 儲存並測試從StorageGRID或本機檔案複製的憑證和私密金鑰。

現在您可以使用外部監控工具從StorageGRID存取 Prometheus 指標。

有關指標的信息，請參閱"StorageGRID監控說明"。

編輯客戶端證書

您可以編輯管理員用戶端憑證以變更其名稱、啟用或停用 Prometheus 訪問，或在目前憑證過期時上傳新憑證。

步驟

1. 選擇 設定 > 安全 > 憑證，然後選擇 用戶端 標籤。

表中列出了證書到期日期和 Prometheus 存取權限。如果憑證即將過期或已經過期，表中會出現一則訊息並觸發警報。

2. 選擇您要編輯的憑證。
3. 選擇*編輯*，然後選擇*編輯名稱和權限*
4. 輸入證書名稱。
5. 若要使用外部監控工具存取 Prometheus 指標，請選擇 允許 **prometheus**。
6. 選擇“繼續”將憑證儲存在網格管理員中。

更新後的憑證顯示在客戶端標籤上。

附加新的客戶端憑證

當前證書過期後，您可以上傳新證書。

步驟

1. 選擇 設定 > 安全 > 憑證，然後選擇 用戶端 標籤。

表中列出了證書到期日期和 Prometheus 存取權限。如果憑證即將過期或已經過期，表中會出現一則訊息並觸發警報。

2. 選擇您要編輯的憑證。
3. 選擇*編輯*，然後選擇編輯選項。

上傳證書

複製證書文字並貼上到其他地方。

a. 選擇*上傳憑證*，然後選擇*繼續*。

b. 上傳客戶端憑證名稱(`.pem`）。

   選擇*用戶端憑證詳細資料*以顯示憑證元資料和憑證 PEM。

   - 選擇*下載證書*儲存證書檔案。

     指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。

c. 選擇*建立*將憑證保存在網格管理員中。

   更新後的憑證顯示在客戶端標籤上。

產生證書

產生證書文字以貼上到其他地方。

a. 選擇*產生證書*。

b. 指定證書資訊：

   - 主題（可選）：證書擁有者的 X.509 主題或專有名稱 (DN)。
   - 有效天數：產生的憑證從產生時開始的有效天數。
   - 新增金鑰使用擴充功能：如果選擇（預設和建議），則金鑰使用和擴充金鑰使用擴充將新增至產生的憑證中。

     這些擴充定義了憑證中包含的金鑰的用途。

     除非憑證包含這些擴充功能時遇到與舊客戶端的連線問題，否則請選取此核取方塊。

c. 選擇*生成*。

d. 選擇*用戶端憑證詳細資料*以顯示憑證元資料和憑證 PEM。

   關閉對話方塊後，您將無法查看憑證私鑰。將金鑰複製或下載到安全位置。

   - 選擇*複製證書 PEM* 以複製證書內容並貼上到其他地方。
   - 選擇*下載證書*儲存證書檔案。

     指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

- 選擇*複製私密金鑰*複製憑證私鑰以便貼到其他地方。
- 選擇*下載私鑰*將私鑰儲存為檔案。

  指定私鑰檔案名稱和下載位置。

e. 選擇*建立*將憑證保存在網格管理員中。

新證書出現在客戶端選項卡上。

下載或複製客戶端證書

您可以下載或複製客戶端憑證以供其他地方使用。

步驟

1. 選擇 設定 > 安全 > 憑證，然後選擇 用戶端 標籤。
2. 選擇您要複製或下載的憑證。
3. 下載或複製證書。

下載證書文件

下載證書 `.pem`文件。

a. 選擇*下載證書*。
b. 指定證書檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

影印證書

複製證書文字並貼上到其他地方。

a. 選擇*複製憑證 PEM*。
b. 將複製的憑證貼到文字編輯器中。
c. 儲存帶有擴展名的文字文件 `.pem`。

   例如： `storagegrid_certificate.pem`

刪除客戶端證書

如果您不再需要管理員用戶端證書，您可以將其刪除。

步驟

1. 選擇 設定 > 安全 > 憑證，然後選擇 用戶端 標籤。

2. 選擇您要刪除的憑證。
3. 選擇*刪除*然後確認。

> 若要刪除最多 10 個證書，請在「用戶端」標籤上選擇要刪除的每個證書，然後選擇「操作」>「刪除」。

刪除憑證後，使用該憑證的用戶端必須指定新的用戶端憑證才能存取StorageGRID Prometheus 資料庫。