管理憑證

StorageGRID software

NetApp
July 23, 2026

目錄

管理憑證

管理 StorageGRID 中的安全性憑證

安全性憑證是小型資料檔案，用於在 StorageGRID 元件之間以及 StorageGRID 元件與外部系統之間建立安全且可信任的連線。

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*。伺服器憑證用於在用戶端和伺服器之間建立安全連線，驗證伺服器對其用戶端的身分識別，並為資料傳輸提供安全的通訊路徑。伺服器和用戶端各自擁有一份憑證複本。
- *用戶端憑證*用於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驗證。用戶端憑證不會加密資料。

當用戶端使用 HTTPS 連線至伺服器時，伺服器會以包含公開金鑰的伺服器憑證進行回應。用戶端會將伺服器簽署與其憑證複本上的簽署進行比較。如果簽署相符，用戶端會使用相同的公開金鑰與伺服器建立工作階段。

StorageGRID 在某些連線中擔任伺服器（例如負載平衡器端點），或在其他連線中擔任用戶端（例如 CloudMirror 複寫服務）。

預設網格 **CA** 憑證

StorageGRID 具有內建的憑證授權單位 （CA），可在系統安裝期間產生內部 Grid CA 憑證。預設會使用 Grid CA 憑證來保護內部 StorageGRID 流量的安全。外部憑證授權單位 （CA） 可以核發完全符合您組織資訊安全性原則的自訂憑證。

在非正式作業環境中，請使用 Grid CA 憑證。若是正式作業環境，請使用由外部憑證授權單位簽署的自訂憑證。支援不使用憑證的非安全連線，但不建議使用。

- ${post_edited_translations.segment}
- 所有自訂憑證都必須符合 "${post_edited_translations.segment}"。
- ${post_edited_translations.segment}

> StorageGRID 亦包含在所有網格上均相同的作業系統 CA 憑證。在正式作業環境中，請確保指定由外部憑證授權單位簽署的自訂憑證，以取代作業系統 CA 憑證。

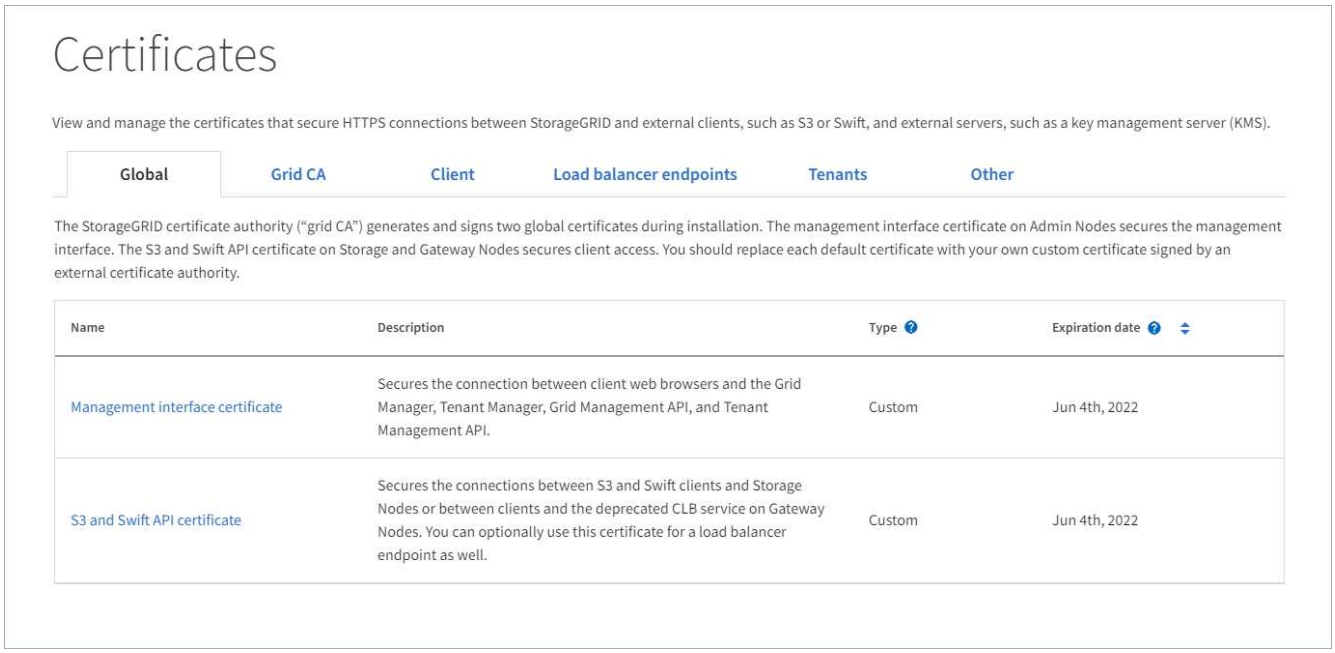
伺服器與用戶端憑證類型的變體是以多種方式實作。在您設定系統之前，您應該先準備好特定 StorageGRID 組態所需的所有憑證。

存取安全性憑證

您可以在單一位置存取所有 StorageGRID 憑證的資訊，以及每個憑證組態工作流程的連結。

步驟

1. ${post_edited_translations.segment}



—

2. 在「憑證」頁面上選取索引標籤，即可檢視每個憑證類別的資訊並存取憑證設定。如果您擁有 "${post_edited_translations.segment}"，則可以存取索引標籤。

   - 全域：保護來自 Web 瀏覽器和外部 API 用戶端的 StorageGRID 存取。
   - **Grid CA**：保護 StorageGRID 內部流量。
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - 租戶：保護與身分識別聯合伺服器的連線，或從平台服務端點到 S3 儲存資源的連線。
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

全球

全域憑證可保護 Web 瀏覽器和外部 S3 API 用戶端對 StorageGRID 的存取安全性。StorageGRID 憑證授權單位會在安裝期間初始產生兩個全域憑證。正式作業環境的最佳實務做法是使用由外部憑證授權單位簽署的自訂憑證。

- [管理介面憑證]: 保護用戶端網頁瀏覽器至 StorageGRID 管理介面的連線。
- <<${post_edited_translations.segment}>>：保護用戶端 API 與儲存節點、管理節點和閘道節點之間的連線，S3 用戶端應用程式使用這些連線來上傳和下載物件資料。

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- 說明
- 類型：自訂或預設。+ 為了提高網格安全性，您應該始終使用自訂憑證。
- ${post_edited_translations.segment}

您可以：

- 為了提高網格安全性，請將預設憑證替換為由外部憑證授權單位簽署的自訂憑證：
  - "${post_edited_translations.segment}" 用於 Grid Manager 和 Tenant Manager 連線。
  - "替換 S3 API 憑證"用於儲存節點和負載平衡器端點（選用）連線。
- "還原預設管理介面憑證"。
- "${post_edited_translations.segment}"。
- "${post_edited_translations.segment}"。
- 複製或下載 "管理介面憑證" 或 "${post_edited_translations.segment}"。

網格 **CA**

由 StorageGRID 憑證授權單位在安裝 StorageGRID 期間產生的 ${post_edited_translations.segment}，可保護所有內部 StorageGRID 流量。

${post_edited_translations.segment}

您可以 "${post_edited_translations.segment}"，但無法變更它。

用戶端

${post_edited_translations.segment}由外部憑證授權單位產生，可保護外部監控工具與 StorageGRID Prometheus 資料庫之間連線的安全。

憑證表中每個已設定的用戶端憑證各有一列記錄，並指示該憑證是否可用於 Prometheus 資料庫存取，以及憑證的到期日期。

您可以：

- "上傳或產生新的用戶端憑證。"
- 選取憑證名稱以顯示憑證詳細資料，您可以在其中執行以下操作：

- "變更用戶端憑證名稱。"
- "${post_edited_translations.segment}"
- "上傳並替換用戶端憑證。"
- "複製或下載用戶端憑證。"
- "${post_edited_translations.segment}"

◦ 選擇 **Actions** 可快速"編輯"、"${post_edited_translations.segment}"或"移除"用戶端憑證。您最多可以選擇 10 個用戶端憑證，並使用 **Actions** > **Remove** 一次移除它們。

負載平衡器端點

${post_edited_translations.segment} 保護 S3 用戶端與 Gateway Nodes 和 Admin Nodes 上的 StorageGRID 負載平衡器服務之間的連線安全。

負載平衡器端點表格中，每個已設定的負載平衡器端點各有一列，並指示該端點使用的是全域 S3 API 憑證還是自訂負載平衡器端點憑證。每個憑證的到期日期也會顯示於表格中。

${post_edited_translations.segment}

您可以：

◦ "${post_edited_translations.segment}"，包括其憑證詳細資料。

◦ "為 FabricPool 指定負載平衡器端點憑證。"

◦ "${post_edited_translations.segment}"而不是產生新的負載平衡器端點憑證。

${post_edited_translations.segment}

租戶可以使用 ${post_edited_translations.segment} 或 平台服務端點憑證 來保護其與 StorageGRID 的連線安全。

${post_edited_translations.segment}

您可以：

◦ "選擇租戶名稱以登入 Tenant Manager。"

◦ "選擇租戶名稱以檢視租戶身分識別聯盟詳細資訊"

◦ "選擇租戶名稱以檢視租戶平台服務詳細資料"

◦ "在建立端點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實現特定用途。這些憑證依其功能名稱列出。其他安全性憑證包括：

◦ 雲端儲存池憑證

◦ 電子郵件警示通知憑證

◦ 外部 syslog 伺服器憑證

◦ 網格同盟連線憑證

- 身分聯合憑證
- 金鑰管理伺服器 (KMS) 憑證
- <<${post_edited_translations.segment},單一登入憑證>>

資訊顯示函數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）。選擇函數名稱會開啟瀏覽器索引標籤，您可以在其中檢視和編輯憑證詳細資訊。

只有擁有 "${post_edited_translations.segment}"，才能檢視和存取其他憑證的資訊。

您可以：

- "為 S3、C2S S3 或 Azure 指定雲端儲存池憑證"
- "指定用於警示電子郵件通知的憑證"
- "為外部 syslog 伺服器使用憑證"
- "輪換網格聯盟連線憑證"
- "檢視並編輯身分識別同盟憑證"
- "上傳金鑰管理伺服器（KMS）伺服器和用戶端憑證"
- "手動為信賴方信任指定 SSO 憑證"

安全性憑證詳細資料

以下將介紹每種類型的安全性證書，並附上實作說明的連結。

管理介面憑證

憑證類型	說明	導航位置	詳細資料
伺服器	驗證用戶端 Web 瀏覽器與 StorageGRID 管理介面之間的連線，讓使用者無需收到安全性警告即可存取 Grid Manager 和 Tenant Manager。 此憑證也可驗證 Grid Management API 和 Tenant Management API 的連線。 您可以使用安裝期間建立的預設憑證，也可以上傳自訂憑證。	**Configuration** > **Security** > **Certificates**，選擇 **Global** 索引標籤，然後選擇 **Management interface certificate**	"設定管理介面憑證"

${post_edited_translations.segment}

憑證類型	說明	導航位置	詳細資料
伺服器	驗證與儲存節點和負載平衡器端點（選用）的安全 S3 用戶端連線。	**Configuration** > **Security** > **Certificates**，選擇 **Global** 索引標籤，然後選擇 **S3 API certificate**	"設定 S3 API 憑證"

${post_edited_translations.segment}

請參閱 預設網格 CA 憑證執行摘要。

管理員用戶端憑證

憑證類型	說明	導航位置	詳細資料
用戶端	安裝在每個用戶端上，允許 StorageGRID 對外部用戶端存取進行驗證。 • 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 進行安全的監控。	**Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤	"設定用戶端憑證"

負載平衡器端點憑證

憑證類型	說明	導航位置	詳細資料
伺服器	用於驗證 S3 用戶端與 Gateway Nodes 和 Admin Nodes 上的 StorageGRID Load Balancer 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線至 StorageGRID 以儲存和擷取物件資料時，會使用此負載平衡器憑證。 您也可以使用自訂版本的全域 <<${post_edited_translations.segment}>> 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線，則無需為每個負載平衡器端點上傳或產生個別的憑證。 *注意：*用於負載平衡器驗證的憑證是 StorageGRID 正常運作期間最常用的憑證。	設定 > 網路 > 負載平衡器端點	• "設定負載平衡器端點" • "為 FabricPool 建立負載平衡器端點"

雲端儲存池端點憑證

憑證類型	說明	導航位置	詳細資料
伺服器	用於驗證從 StorageGRID 雲端儲存池到外部儲存設備位置（例如 S3 Glacier 或 Microsoft Azure Blob 儲存設備）的連線。每種雲端供應商類型都需要不同的憑證。	**ILM** > 儲存池	"建立雲端儲存池"

電子郵件警示通知憑證

憑證類型	說明	導航位置	詳細資料
伺服器和用戶端	驗證 SMTP 電子郵件伺服器與 StorageGRID 之間的連線，用於警示通知。 • 如果與 SMTP 伺服器的通訊需要傳輸層安全性協定 (TLS)，則必須指定電子郵件伺服器 CA 憑證。 • 僅當 SMTP 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。	提醒 > 郵件設定	"設定電子郵件通知以接收提醒"

外部 **syslog** 伺服器憑證

憑證類型	說明	導航位置	詳細資料
伺服器	驗證外部 syslog 伺服器與 StorageGRID 中記錄事件的本機系統日誌伺服器之間的 TLS 或 RELP/TLS 連線。 *注意：*與外部 syslog 伺服器建立 TCP、RELP/TCP 和 UDP 連線時，不需要外部 syslog 伺服器憑證。	設定 > 監控 > 稽核與 **syslog** 伺服器	"使用外部 syslog 伺服器"

網格同盟連線憑證

憑證類型	說明	導航位置	詳細資料
伺服器和用戶端	驗證並加密目前 StorageGRID 系統與網格同盟連線中另一個網格之間所傳送的資訊。	設定 > 系統 > 網格同盟	• "建立網格聯盟連線" • "輪換連線憑證"

身分聯合憑證

憑證類型	說明	導航位置	詳細資料
伺服器	驗證 StorageGRID 與外部身分供應商（例如 Active Directory、OpenLDAP 或 Oracle Directory Server）之間的連線。用於身分聯合，允許由外部系統管理管理員群組和使用者。	設定 > 存取控制 > 身分識別同盟	"${post_edited_translations.segment}"

金鑰管理伺服器 **(KMS)** 憑證

憑證類型	說明	導航位置	詳細資料
伺服器和用戶端	驗證 StorageGRID 與外部金鑰管理伺服器 (KMS) 之間的連線，該伺服器為 StorageGRID 應用裝置節點提供加密金鑰。	設定 > 安全性 > 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

憑證類型	說明	導航位置	詳細資料
伺服器	對 StorageGRID 平台服務與 S3 儲存設備資源之間的連線進行驗證。	${post_edited_translations.segment}	"${post_edited_translations.segment}" "${post_edited_translations.segment}"

${post_edited_translations.segment}

憑證類型	說明	導航位置	詳細資料
伺服器	驗證用於單一登入 （SSO） 請求的身分識別聯合服務（例如 Active Directory Federation Services （ADFS））與 StorageGRID 之間的連線。	${post_edited_translations.segment}	"設定單一登入"

證書範例

範例 **1**：負載平衡器服務

${post_edited_translations.segment}

1. 您可以在 StorageGRID 中設定負載平衡器端點並上傳或產生伺服器憑證。
2. ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. 用戶端會比較伺服器簽署與其憑證複本上的簽署。如果簽署符合，用戶端會使用相同的公開金鑰啟動工作階段。
6. ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

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、公用用戶端憑證和用戶端憑證的私密金鑰。
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. KMS 伺服器驗證憑證簽署，並決定信任 StorageGRID。
5. ${post_edited_translations.segment}

StorageGRID 中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。

安全性原則的加密演算法類型必須與伺服器憑證類型相符。例如，RSA 加密演算法需要 RSA 憑證，而 ECDSA 加密演算法需要 ECDSA 憑證。請參閱 "管理安全性證書"。如果您設定了與伺服器憑證不相容的自訂安全性原則，您可以 "暫時回復預設安全性原則"。

如需更多關於 StorageGRID 如何保護用戶端連線安全的資訊，請參閱 "${post_edited_translations.segment}"。

在 StorageGRID 中設定管理介面憑證

您可以將預設的管理介面憑證取代為單一自訂憑證，以允許使用者存取 Grid Manager 和 Tenant Manager，而不會遇到安全性警告。您也可以回復為預設的管理介面憑證，或產生新的憑證。

關於此任務

預設情況下，每個管理節點都會獲得一個由網格 CA 簽署的憑證。這些由 CA 簽署的憑證可以替換為單一通用的自訂管理介面憑證及其對應的私鑰。

由於所有管理節點都使用單一自訂管理介面憑證，因此如果用戶端在連線至 Grid Manager 和 Tenant Manager 時需要驗證主機名稱，則必須將該憑證指定為萬用字元憑證或多網域憑證。請定義自訂憑證，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組態，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他們將用於存取 Grid Manager 和 Tenant Manager 的 Web 瀏覽器中安裝 Grid CA 憑證。

為確保伺服器憑證失效不會中斷運作，當伺服器憑證即將過期時，系統會觸發「管理介面的伺服器憑證過期」警示。如有需要，您可以透過選取 **Configuration** > **Security** > **Certificates**，然後在 Global 索引標籤上查看管理介面憑證的到期日期，來檢視目前憑證的到期時間。

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- 你${post_edited_translations.segment}。

${post_edited_translations.segment}

若要新增自訂管理介面憑證，您可以提供自己的憑證，也可以使用 Grid Manager 產生憑證。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. 選擇 **Use custom certificate**。
4. 上傳或產生憑證。

上傳證書

上傳所需的伺服器憑證檔案。

a. 選擇 **Upload certificate**。

b. 上傳所需的伺服器憑證檔案：

   - ${post_edited_translations.segment}
   - 憑證私鑰：自訂伺服器憑證私鑰檔案 (`.key`)

     EC 私鑰必須至少 224 位元。RSA 私鑰必須至少 2048 位元。

   - **CA** 套裝組合：包含來自每個中介發行憑證授權單位（CA）憑證的單一選用檔案。此檔案應包含每個 PEM 編碼的 CA 憑證檔案，並依憑證鏈順序串接。

c. 展開 憑證詳細資料 以檢視您上傳之每個憑證的中繼資料。如果您上傳了選用的 CA 套裝組合，每個憑證都會顯示在各自的索引標籤上。

   - ${post_edited_translations.segment}

     指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

   例如： `storagegrid_certificate.pem`

   - 選擇「複製憑證 PEM」或「複製 CA 套裝組合 PEM」以複製憑證內容並貼上到其他位置。

d. 選擇 **Save**。+ 自訂管理介面憑證將用於所有後續與 Grid Manager、Tenant Manager、Grid Manager API 或 Tenant Manager API 的新連線。

產生證書

產生伺服器憑證檔案。

正式作業環境的最佳實務做法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 **Generate certificate**。

b. 請提供憑證資訊：

欄位	說明
網域名稱	要包含在憑證中的一或多個完整網域名稱。使用 * 做為萬用字元來代表多個網域名稱。
IP	憑證中要包含的一個或多個 IP 位址。
${post_edited_translations.segment}	X.509 憑證擁有者的主旨或可分辨名稱 (DN)。 如果此欄位中未輸入任何值，則產生的憑證將使用第一個網域名稱或 IP 位址作為主旨通用名稱 (CN)。

欄位	說明
${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	如果選取（預設且建議），則會將金鑰用途和擴充金鑰用途擴充功能新增至產生的憑證。 這些擴充定義了憑證中包含的金鑰的用途。 ${post_edited_translations.segment}

c. 選擇 **Generate** 。

d. ${post_edited_translations.segment}

- 選取 **Download certificate** 以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

例如： `storagegrid_certificate.pem`

- 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。

e. 選擇 **Save**。+ 自訂管理介面憑證將用於所有後續與 Grid Manager、Tenant Manager、Grid Manager API 或 Tenant Manager API 的新連線。

5. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

6. 新增自訂管理介面憑證後，「管理介面憑證」頁面會顯示目前使用中憑證的詳細憑證資訊。+ 您可以根據需要下載或複製憑證 PEM。

還原預設管理介面憑證

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

   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，且無法從系統中復原。預設管理介面憑證會用於所有後續的新用戶端連線。

4. ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

開始之前

- 您有"特定存取權限"。
- 您擁有 `Passwords.txt` 檔案。

關於此任務

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
   a. 請輸入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 請輸入 `Passwords.txt`檔案中列出的密碼。
   c. 輸入以下命令以切換至根目錄： `su -`
   d. 請輸入 `Passwords.txt`檔案中列出的密碼。

      當您以根目錄身分登入時，提示符號會從 `$`變為 `#`。
3. ${post_edited_translations.segment}

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

   - 對於 `--domains`，請使用萬用字元來代表所有管理節點的完整網域名稱。例如，`*.ui.storagegrid.example.com` 使用 * 萬用字元來代表 `admin1.ui.storagegrid.example.com` 和 `admin2.ui.storagegrid.example.com`。
   - 設定 `--type`為 `management`以設定管理介面憑證，此憑證由 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），必須在過期前重新產生。您可以使用 `--days` 參數來置換預設的有效期。

     憑證的有效期自執行 `make-certificate` 時開始。您必須確保管理用戶端與 StorageGRID 同步至相同的時間來源；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
     ```

     輸出結果包含管理 API 用戶端所需的公開憑證。
4. ${post_edited_translations.segment}

   ${post_edited_translations.segment}
5. 登出命令 shell。 `$ exit`

6. ${post_edited_translations.segment}
    a. ${post_edited_translations.segment}
    b. ${post_edited_translations.segment}
    c. ${post_edited_translations.segment}
7. 設定您的管理用戶端以使用您複製的公開憑證。請包含 BEGIN 和 END 標記。

${post_edited_translations.segment}

您可以儲存或複製管理介面憑證的內容以供其他地方使用。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

下載憑證檔案或 **CA** 套裝組合

下載憑證或 CA 套裝組合 `.pem`檔案。如果您使用的是選用的 CA 套裝組合，則套裝組合中的每個憑證都會顯示在各自的子索引標籤中。

a. 選擇「下載憑證」或「下載 CA 套裝組合」。

   如果您正在下載 CA 套裝組合，則 CA 套裝組合二級標籤中的所有憑證將下載為單一檔案。

b. 指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

   例如： `storagegrid_certificate.pem`

複製憑證或 **CA** 套裝組合 **PEM**

複製憑證文字以貼到其他地方。如果您使用的是選用 CA 套裝組合，套裝組合中的每個憑證都會顯示在各自的子索引標籤上。

a. 選擇「複製憑證 PEM」或「複製 CA 套裝組合 PEM」。

   如果您要複製 CA 套裝組合，則 CA 套裝組合次要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. 將文字檔案以副檔名 `.pem`儲存。

   例如： `storagegrid_certificate.pem`

在 **StorageGRID** 中設定 **S3 API** 憑證

您可以替換或還原用於 S3 用戶端連線至儲存節點或負載平衡器端點的伺服器憑證。替換後的自訂伺服器憑證專屬於您的組織。

此版本的文件網站已移除 Swift 相關細節。請參閱 "${post_edited_translations.segment}"。

關於此任務

預設情況下，每個 Storage Node 都會獲發由網格 CA 簽署的 X.509 伺服器憑證。這些 CA 簽署的憑證可以替換為單一常用的自訂伺服器憑證和對應的私密金鑰。

所有 Storage Nodes 均使用單一自訂伺服器憑證，因此，如果用戶端在連線至儲存設備端點時需要驗證主機名稱，則必須將該憑證指定為萬用字元憑證或多網域憑證。請定義自訂憑證，使其與網格中的所有 Storage Nodes 相符。

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

為確保伺服器憑證失效不會中斷運行，當根目錄伺服器憑證即將過期時，系統會觸發「S3 API 全域伺服器憑證即將過期」警報。如有需要，您可以透過選取「組態」>「安全性」>「憑證」，然後在「全域」標籤上查看 S3 API 憑證的到期日期，來檢視目前憑證的到期時間。

您可以上傳或產生自訂 S3 API 憑證。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. 選擇 **Use custom certificate**。
4. 上傳或產生憑證。

上傳證書

上傳所需的伺服器憑證檔案。

a. 選擇 **Upload certificate**。

b. 上傳所需的伺服器憑證檔案：

   - ${post_edited_translations.segment}
   - 憑證私鑰：自訂伺服器憑證私鑰檔案 (`.key`)

     EC 私鑰必須至少 224 位元。RSA 私鑰必須至少 2048 位元。

   - **CA** 套裝組合：包含來自每個中介發行憑證授權單位憑證的單一選用檔案。此檔案應包含每個 PEM 編碼的 CA 憑證檔案，並依憑證鏈順序串聯。

c. 選取憑證詳細資料，以顯示已上傳之每個自訂 S3 API 憑證的中繼資料與 PEM。如果您上傳了選用的 CA 套裝組合，每個憑證都會顯示在各自的索引標籤上。

   - ${post_edited_translations.segment}

     指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

     例如： `storagegrid_certificate.pem`

   - 選擇「複製憑證 PEM」或「複製 CA 套裝組合 PEM」以複製憑證內容並貼上到其他位置。

d. 選取 **Save** 。

   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 **Generate certificate**。

b. 請提供憑證資訊：

欄位	說明
網域名稱	要包含在憑證中的一或多個完整網域名稱。使用 * 做為萬用字元來代表多個網域名稱。
IP	憑證中要包含的一個或多個 IP 位址。
${post_edited_translations.segment}	X.509 憑證擁有者的主旨或可分辨名稱 (DN)。 如果此欄位中未輸入任何值，則產生的憑證將使用第一個網域名稱或 IP 位址作為主旨通用名稱 (CN)。

欄位	說明
${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	如果選取（預設且建議），則會將金鑰用途和擴充金鑰用途擴充功能新增至產生的憑證。 這些擴充定義了憑證中包含的金鑰的用途。 ${post_edited_translations.segment}

c. 選擇 **Generate** 。

d. ${post_edited_translations.segment}

- 選取 **Download certificate** 以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

例如： `storagegrid_certificate.pem`

- 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。

e. 選取 **Save** 。

自訂伺服器憑證用於後續新的 S3 用戶端連線。

5. ${post_edited_translations.segment}

${post_edited_translations.segment}

6. ${post_edited_translations.segment}
7. 新增自訂 S3 API 憑證後，S3 API 憑證頁面會顯示目前使用中自訂 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。

${post_edited_translations.segment}

您可以回復使用預設的 S3 API 憑證來建立 S3 用戶端與儲存節點的連線。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. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

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，且無法從系統中復原。預設的 S3 API 憑證將用於後續與儲存節點的新 S3 用戶端連線。

4. ${post_edited_translations.segment}

   如果您擁有根目錄存取權限，並且使用了自訂 S3 API 憑證來連接負載平衡器端點，則會顯示負載平衡器端點清單，這些端點將無法再使用預設 S3 API 憑證存取。請前往 "設定負載平衡器端點" 編輯或移除受影響的端點。

5. ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以儲存或複製 S3 API 憑證內容以供其他地方使用。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

   下載憑證檔案或 **CA** 套裝組合

   下載憑證或 CA 套裝組合 `.pem`檔案。如果您使用的是選用的 CA 套裝組合，則套裝組合中的每個憑證都會顯示在各自的子索引標籤中。

   a. 選擇「下載憑證」或「下載 CA 套裝組合」。

      如果您正在下載 CA 套裝組合，則 CA 套裝組合二級標籤中的所有憑證將下載為單一檔案。

   b. 指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

      例如： `storagegrid_certificate.pem`

   複製憑證或 **CA** 套裝組合 **PEM**

   複製憑證文字以貼到其他地方。如果您使用的是選用 CA 套裝組合，套裝組合中的每個憑證都會顯示在各自的子索引標籤上。

   a. 選擇「複製憑證 PEM」或「複製 CA 套裝組合 PEM」。

      如果您要複製 CA 套裝組合，則 CA 套裝組合次要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. 將文字檔案以副檔名 `.pem`儲存。

      例如： `storagegrid_certificate.pem`

相關資訊

- "使用 S3 REST API"
- "設定 S3 端點網域名稱"

複製 StorageGRID Grid CA 憑證

StorageGRID 使用內部憑證授權單位 (CA) 來保護內部流量。即使您上傳了自己的憑證，此憑證也不會變更。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"特定存取權限"。

關於此任務

如果已設定自訂伺服器憑證，用戶端應用程式應使用該自訂伺服器憑證驗證伺服器。它們不應從 StorageGRID 系統複製 CA 憑證。

步驟

1. 選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Grid CA** 索引標籤。
2. 在「憑證 PEM」區段中，下載或複製憑證。

   下載憑證檔案

   下載憑證 `.pem`檔案。

   a. 選取 **Download certificate**。
   b. 指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

      例如： `storagegrid_certificate.pem`

   複製憑證 **PEM**

   複製證書文字並貼上到其他位置。

   a. 選擇 **Copy certificate PEM**。
   b. 將複製的憑證貼到文字編輯器中。
   c. 將文字檔案以副檔名 `.pem`儲存。

      例如： `storagegrid_certificate.pem`

為 FabricPool 設定 StorageGRID 憑證

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

- 您有"特定存取權限"。

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。

關於此任務

當您建立負載平衡器端點時，可以產生自我簽署的伺服器憑證，或上傳由已知憑證授權單位（CA）簽署的憑證。在生產環境中，您應該使用由已知 CA 簽署的憑證。由 CA 簽署的憑證可以不中斷地進行輪替。它們也更為安全，因為能針對中間人攻擊提供更好的保護。

以下步驟為使用 FabricPool 的 S3 用戶端提供一般性指導原則。如需更詳細的資訊和程序，請參閱 "設定 StorageGRID 以供 FabricPool 使用"。

步驟

1. 選擇性地設定高可用度（HA）群組以供 FabricPool 使用。
2. 建立供 FabricPool 使用的 S3 負載平衡器端點。

   建立 HTTPS 負載平衡器端點時，系統會提示您上傳伺服器憑證、憑證私密金鑰和選用的 CA 套裝組合。

3. 將 StorageGRID 作為雲端層附加至 ONTAP。

   請指定負載平衡器端點連接埠以及您上傳的 CA 憑證中所使用的完整網域名稱。然後，請提供 CA 憑證。

> ⓘ 如果 StorageGRID 憑證是由中間 CA 核發的，則必須提供該中間 CA 憑證。如果 StorageGRID 憑證是由根 CA 直接核發的，則必須提供該根 CA 憑證。

在 StorageGRID 中設定用戶端憑證

用戶端憑證可讓授權的外部用戶端存取 StorageGRID Prometheus 資料庫，為外部工具監控 StorageGRID 提供安全的方式。

如果您需要使用外部監控工具存取 StorageGRID，則必須使用 Grid Manager 上傳或產生用戶端憑證，並將憑證資訊複製到外部工具。

參見 "管理安全性證書" 和 "設定自訂伺服器憑證"。

> ⓘ 為確保伺服器憑證失效不會中斷執行，當伺服器憑證即將過期時，系統會觸發*憑證頁面上設定的用戶端憑證過期*警報。如有需要，您可以透過選擇 **Configuration** > **Security** > **Certificates**，然後在 Client 標籤上查看用戶端憑證的過期日期，來檢視目前憑證的到期時間。

> ⓘ 如果您使用金鑰管理伺服器 (KMS) 來保護特殊設定的應用裝置節點上的資料，請參閱有關 "上傳 KMS 用戶端憑證" 的具體資訊。

開始之前

- 您擁有根目錄存取權限。
- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 設定用戶端憑證：
  - 您擁有管理節點的 IP 位址或網域名稱。
  - 如果您已設定 StorageGRID 管理介面憑證，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。

- 若要上傳您自己的憑證，憑證的私密金鑰必須存放在您的本機電腦上。
- 私鑰必須在建立時儲存或記錄。如果您沒有原始私鑰，則必須建立新的私鑰。

- 編輯用戶端憑證：
  - 您擁有管理節點的 IP 位址或網域名稱。
  - 若要上傳您自己的憑證或新憑證，私密金鑰、用戶端憑證和 CA （如果使用）都位於您的本機電腦上。

新增用戶端證書

若要新增用戶端憑證，請使用下列其中一個程序：

- [管理介面憑證已設定]
- CA 核發的用戶端證書
- 從 Grid Manager 產生的憑證

管理介面憑證已設定

如果已使用客戶提供的 CA、用戶端憑證和私密金鑰設定了管理介面憑證，請使用此程序新增用戶端憑證。

步驟

1. 在 Grid Manager 中，選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。
2. 選擇 **Add** 。
3. 請輸入憑證名稱。
4. 若要使用外部監控工具存取 Prometheus 計量，請選擇 * 允許 prometheus*。
5. 選擇 **Continue** 。
6. 在「附加憑證」步驟中，上傳管理介面憑證。
   a. 選擇 **Upload certificate**。
   b. 選擇 **Browse** ，然後選擇管理介面憑證檔案(`.pem`) 。
      - 選擇「用戶端憑證詳細資料」以顯示憑證中繼資料和憑證 PEM。
      - 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。
   c. 選擇 **Create** 以將憑證儲存在 Grid Manager 中。

      新證書會顯示在「用戶端」標籤上。
7. 設定外部監控工具，例如 Grafana。

CA 核發的用戶端證書

如果未設定管理介面憑證，且您計劃為 Prometheus 新增使用 CA 頒發的用戶端憑證和私密金鑰的用戶端憑證，請使用此程序新增系統管理員用戶端憑證。

步驟

1. 執行以下步驟"設定管理介面憑證"。
2. 在 Grid Manager 中，選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。
3. 選擇 **Add** 。
4. 請輸入憑證名稱。
5. 若要使用外部監控工具存取 Prometheus 計量，請選擇 * 允許 prometheus*。
6. 選擇 **Continue** 。
7. 在「附加憑證」步驟中，上傳用戶端憑證、私鑰和 CA 套裝組合檔案：
   a. 選擇 **Upload certificate**。
   b. 選擇 **Browse** ，然後選擇用戶端憑證、私鑰和 CA 套裝組合檔案(`.pem`) 。
      - 選擇「用戶端憑證詳細資料」以顯示憑證中繼資料和憑證 PEM。
      - 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。
   c. 選擇 **Create** 以將憑證儲存在 Grid Manager 中。

      新證書會顯示在「用戶端」標籤上。
8. 設定外部監控工具，例如 Grafana。

從 **Grid Manager** 產生的憑證

如果未設定管理介面憑證，且您計劃為 Prometheus 新增用戶端憑證（此憑證使用 Grid Manager 中的產生憑證功能），請使用此程序新增系統管理員用戶端憑證。

步驟

1. 在 Grid Manager 中，選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。
2. 選擇 **Add** 。
3. 請輸入憑證名稱。
4. 若要使用外部監控工具存取 Prometheus 計量，請選擇 * 允許 prometheus*。
5. 選擇 **Continue** 。
6. 在「附加憑證」步驟中，選取「產生憑證」。
7. 請提供憑證資訊：
   - 主旨（可選）：憑證擁有者的 X.509 主旨或可分辨名稱 (DN)。
   - 有效天數：產生的憑證自產生時起有效的天數。
   - 新增金鑰用途擴充：如果選取（預設且建議），則會將金鑰用途和擴充金鑰用途擴充功能新增至產生的憑證。

     這些擴充定義了憑證中包含的金鑰的用途。

     除非您在使用包含這些擴充功能的憑證時，舊版用戶端發生連線問題，否則請保持選取此核取方塊。

8. 選擇 **Generate** 。
9. 選擇 用戶端憑證詳細資料 以顯示憑證中繼資料和憑證 PEM。

   關閉對話方塊後，您將無法檢視憑證私鑰。請將金鑰複製或下載到安全位置。

   - 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。
   - 選取 **Download certificate** 以儲存憑證檔案。

     指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

     例如： `storagegrid_certificate.pem`

   - 選擇 **Copy private key** 以複製憑證私鑰，以便貼上到其他位置。
   - 選擇 **Download private key** 將私密金鑰儲存為檔案。

     指定私鑰檔案名稱和下載位置。
10. 選擇 **Create** 以將憑證儲存在 Grid Manager 中。

    新證書會顯示在「用戶端」標籤上。
11. 在 Grid Manager 中，選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Global** 索引標籤。
12. 選擇 **Management Interface certificate**。
13. 選擇 **Use custom certificate**。
14. 從用戶端憑證詳細資料步驟上傳 certificate.pem 和 private_key.pem 檔案。無需上傳 CA 套裝組合。
    a. 選擇 **Upload certificate**，然後選擇 **Continue**。
    b. 上傳每個憑證檔案 (`.pem`) 。
    c. 選擇 **Save** 以將憑證儲存至 Grid Manager 中。

       新證書將顯示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. 請在外部監控工具（例如 Grafana）上設定以下設定。
   a. 名稱：請輸入連線的名稱。

      StorageGRID 不需要此資訊，但您必須提供名稱才能測試連線。
   b. **URL**：輸入管理節點的網域名稱或 IP 位址。請指定 HTTPS 和連接埠 9091。

      例如： `https://admin-node.example.com:9091`
   c. 啟用 **TLS Client Auth** 和 **With CA Cert**。

d. 在 TLS/SSL 驗證詳細資訊下，複製並貼上：+
   - 管理介面 CA 憑證到 **CA Cert**
   - 用戶端憑證至 **Client Cert**
   - **Client Key** 的私鑰
e. **ServerName**：請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一致。

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存取 StorageGRID 中的 Prometheus 計量。

   有關計量的資訊，請參閱 "監控 StorageGRID 的說明"。

編輯用戶端憑證

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

步驟

1. 選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。

   憑證到期日和 Prometheus 存取權限列於表中。如果憑證即將到期或已過期，表中將顯示一則訊息，並觸發警示。

2. 選擇要編輯的憑證。
3. 選擇*編輯*，然後選擇*編輯名稱和權限*。
4. 請輸入憑證名稱。
5. 若要使用外部監控工具存取 Prometheus 計量，請選擇 * 允許 prometheus*。
6. 選擇 **Continue** 以將憑證儲存在 Grid Manager 中。

   更新後的憑證顯示在「用戶端」索引標籤上。

附加新用戶端證書

當現有憑證過期時，您可以上傳新憑證。

步驟

1. 選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。

   憑證到期日和 Prometheus 存取權限列於表中。如果憑證即將到期或已過期，表中將顯示一則訊息，並觸發警示。

2. 選擇要編輯的憑證。
3. 選擇 **Edit**，然後選擇編輯選項。

上傳證書

複製證書文字並貼上到其他位置。

a. 選擇 **Upload certificate**，然後選擇 **Continue**。

b. 上傳用戶端憑證名稱(`.pem`）。

   選擇「用戶端憑證詳細資料」以顯示憑證中繼資料和憑證 PEM。

   - 選取 **Download certificate** 以儲存憑證檔案。

     指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

     例如： `storagegrid_certificate.pem`

   - 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。

c. 選擇 **Create** 以將憑證儲存在 Grid Manager 中。

   更新後的憑證顯示在「用戶端」索引標籤上。

產生證書

產生憑證文字，以便貼到其他位置。

a. 選擇 **Generate certificate**。

b. 請提供憑證資訊：

   - 主旨（可選）：憑證擁有者的 X.509 主旨或可分辨名稱 (DN)。
   - 有效天數：產生的憑證自產生時起有效的天數。
   - 新增金鑰用途擴充：如果選取（預設且建議），則會將金鑰用途和擴充金鑰用途擴充功能新增至產生的憑證。

     這些擴充定義了憑證中包含的金鑰的用途。

     除非您在使用包含這些擴充功能的憑證時，舊版用戶端發生連線問題，否則請保持選取此核取方塊。

c. 選擇 **Generate** 。

d. 選擇「用戶端憑證詳細資料」以顯示憑證中繼資料和憑證 PEM。

   關閉對話方塊後，您將無法檢視憑證私鑰。請將金鑰複製或下載到安全位置。

   - 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。
   - 選取 **Download certificate** 以儲存憑證檔案。

     指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

   例如： `storagegrid_certificate.pem`

- 選擇 **Copy private key** 以複製憑證私鑰，以便貼上到其他位置。
- 選擇 **Download private key** 將私密金鑰儲存為檔案。

  指定私鑰檔案名稱和下載位置。

e. 選擇 **Create** 以將憑證儲存在 Grid Manager 中。

新證書會顯示在「用戶端」標籤上。

下載或複製用戶端憑證

您可以下載或複製用戶端憑證以供其他地方使用。

步驟

1. 選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。
2. 選取要複製或下載的憑證。
3. 下載或複製憑證。

下載憑證檔案

下載憑證 `.pem`檔案。

a. 選取 **Download certificate**。
b. 指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

   例如： `storagegrid_certificate.pem`

複製憑證

複製證書文字並貼上到其他位置。

a. 選擇 **Copy certificate PEM**。
b. 將複製的憑證貼到文字編輯器中。
c. 將文字檔案以副檔名 `.pem`儲存。

   例如： `storagegrid_certificate.pem`

移除用戶端憑證

如果您不再需要系統管理員用戶端憑證，可以將其移除。

步驟

1. 選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。
2. 選取要移除的憑證。

3. 選取 **Delete** ，然後確認。

> 若要移除最多 10 個憑證，請在「用戶端」索引標籤上選擇要移除的每個憑證，然後選擇 **Actions** > **Delete**。

憑證移除後，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。