管理憑證

StorageGRID 11.7

NetApp
April 12, 2024

目錄

管理憑證

管理安全性憑證：總覽

安全證書是小型資料檔案、用於在StorageGRID 各個元件之間、StorageGRID 以及在各個元件與外部系統之間建立安全且值得信賴的連線。

使用兩種類型的安全性憑證：StorageGRID

- 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、驗證伺服器的用戶端身分、並提供安全的資料通訊路徑。伺服器和用戶端各有一份憑證複本。
- *用戶端憑證*驗證伺服器的用戶端或使用者身分、提供比僅密碼更安全的驗證。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、伺服器會以含有公開金鑰的伺服器憑證回應。用戶端會將伺服器簽章與憑證複本上的簽章進行比較、藉此驗證此憑證。如果簽名相符、用戶端會使用相同的公開金鑰啟動與伺服器的工作階段。

充當某些連線（例如負載平衡器端點）的伺服器、或作為其他連線（例如CloudMirror複寫服務）的用戶端。StorageGRID

預設**Grid CA**憑證

包含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。StorageGRID根據預設、Grid CA憑證用於保護內部StorageGRID 的不穩定流量。外部憑證授權單位（CA）可核發完全符合組織資訊安全原則的自訂憑證。雖然您可以將Grid CA憑證用於非正式作業環境、但正式作業環境的最佳做法是使用外部憑證授權單位所簽署的自訂憑證。也支援不含憑證的不安全連線、但不建議這麼做。

- 自訂 CA 憑證不會移除內部憑證；不過，自訂憑證應該是指定用於驗證伺服器連線的憑證。
- 所有自訂憑證都必須符合 "伺服器憑證的系統強化準則"。
- 支援將CA的憑證整合至單一檔案（稱為CA憑證套件）StorageGRID 。

> 此外、還包括所有網格上相同的作業系統CA憑證。StorageGRID在正式作業環境中、請務必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。

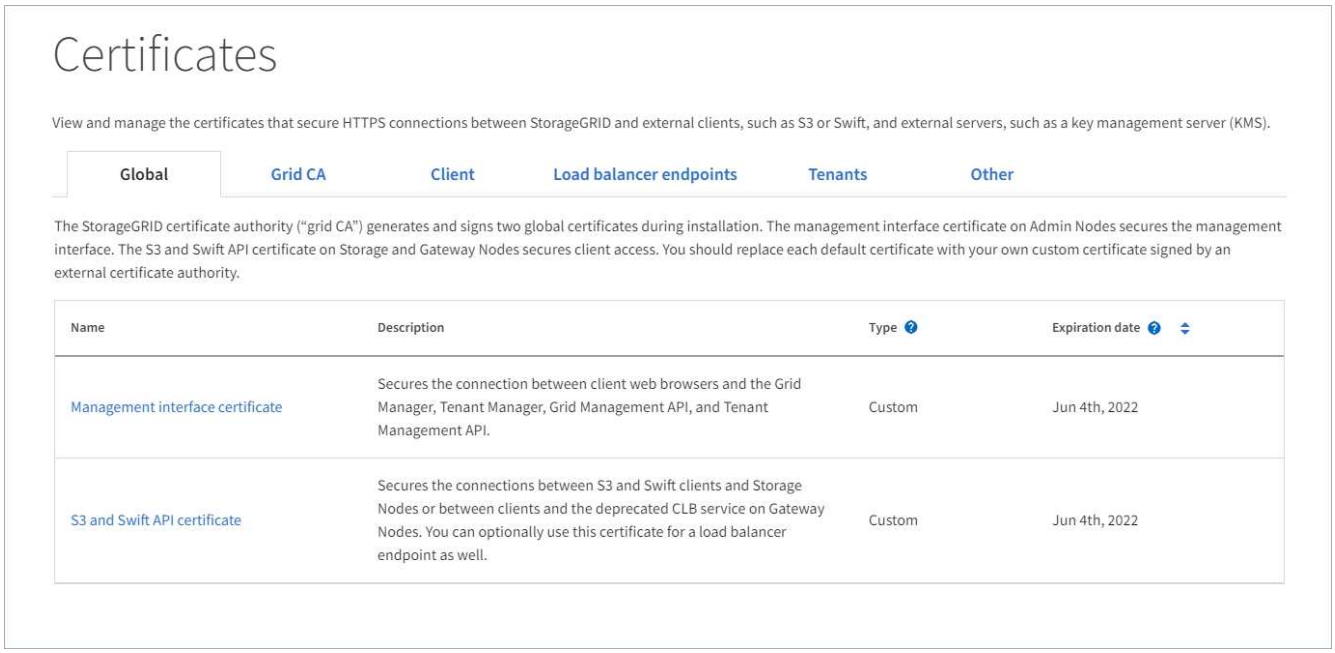
伺服器和用戶端憑證類型的變種會以多種方式實作。在設定系統之前、您應該StorageGRID 準備好特定的支援功能組態所需的所有憑證。

存取安全性憑證

您可以在StorageGRID 單一位置存取所有的資訊、以及每個憑證的組態工作流程連結。

步驟

1. 從 Grid Manager 中、選取 * 組態 * > * 安全性 * > * 憑證 * 。



2. 選取「憑證」頁面上的索引標籤、以取得每個憑證類別的相關資訊、並存取憑證設定。您只能在擁有適當權限的情況下存取索引標籤。

   - 全球：保護StorageGRID 從網頁瀏覽器和外部API用戶端進行的不受限存取。
   - * Grid CA*：保護內部StorageGRID 的不安全流量。
   - 用戶端：保護外部用戶端與StorageGRID 《The S動estetheus資料庫》之間的連線。
   - 負載平衡器端點：保護S3和Swift用戶端與StorageGRID 「平衡負載平衡器」之間的連線。
   - 租戶：保護連線至身分識別聯盟伺服器、或從平台服務端點到S3儲存資源的安全。
   - 其他：保護StorageGRID 需要特定憑證的不實連線。

   每個索引標籤都會在下方說明、並提供其他憑證詳細資料的連結。

全域

全域認證可從StorageGRID 網頁瀏覽器、外部S3和Swift API用戶端安全地進行不受限的存取。安裝期間、由版本資訊驗證機構產生兩個全域憑證StorageGRID 。正式作業環境的最佳實務做法是使用外部憑證授權單位簽署的自訂憑證。

- [管理介面認證]：保護用戶端網路瀏覽器與StorageGRID 功能完善的管理介面的連線。
- S3和Swift API認證：保護用戶端API連線至儲存節點、管理節點和閘道節點的安全、S3和Swift用戶端應用程式可用來上傳和下載物件資料。

安裝的全域憑證相關資訊包括：

- 名稱：憑證名稱、含管理憑證的連結。
- 說明
- 類型：自訂或預設。+您應該永遠使用自訂憑證來改善網格安全性。
- 到期日：如果使用預設憑證、則不會顯示到期日。

您可以：

- 使用外部憑證授權單位簽署的自訂憑證來取代預設憑證、以改善網格安全性：
  - "取代預設StorageGRID產生的管理介面憑證" 用於Grid Manager和Tenant Manager連線。
  - "更換S3和Swift API認證" 用於儲存節點和負載平衡器端點（選用）連線。
- "還原預設的管理介面憑證。"
- "還原預設的S3和Swift API憑證。"
- "使用指令碼來產生新的自我簽署管理介面憑證。"
- 複製或下載 "管理介面認證" 或 "S3和Swift API認證"。

網格**CA**

。 Grid CA憑證由安裝過程中的驗證機關所產生、StorageGRID 可保護所有內部的資訊流量。StorageGRID StorageGRID

憑證資訊包括憑證到期日和憑證內容。

您可以 "複製或下載 Grid CA 憑證"但您無法加以變更。

用戶端

用戶端憑證由外部憑證授權單位所產生、可確保外部監控工具與StorageGRID VMware資料庫之間的連線安全無虞。

憑證表格中有一列用於每個已設定的用戶端憑證、並指出該憑證是否可用於Prometheus資料庫存取、以及憑證到期日。

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：

- "變更用戶端憑證名稱。"
- "設定Prometheus存取權限。"
- "上傳並取代用戶端憑證。"
- "複製或下載用戶端憑證。"
- "移除用戶端憑證。"

- 選取*「動作」即可快速執行 "編輯"、 "附加"或 "移除" 用戶端憑證。您最多可以選取**10**個用戶端憑證、並使用「動作*」>「移除」一次移除這些憑證。

負載平衡器端點

負載平衡器端點憑證 保護 S3 和 Swift 用戶端之間的連線、以及閘道節點和管理節點上的 StorageGRID 負載平衡器服務。

負載平衡器端點表針對每個已設定的負載平衡器端點都有一列、可指出端點是使用全域S3和Swift API憑證、還是使用自訂負載平衡器端點憑證。也會顯示每個憑證的到期日。

對端點憑證所做的變更、可能需要15分鐘才能套用至所有節點。

您可以：

- "檢視負載平衡器端點"，包括其憑證詳細資料。
- "指定要FabricPool 使用的負載平衡器端點憑證。"
- "使用全域S3和Swift API認證" 而非產生新的負載平衡器端點憑證。

租戶

租戶可以使用 身分識別聯盟伺服器憑證 或 平台服務端點憑證 使用StorageGRID NetApp保護連線安全。

租戶表格會針對每個租戶顯示一列、並指出每個租戶是否有權使用自己的身分識別來源或平台服務。

您可以：

- "選取要登入租戶管理程式的租戶名稱"
- "選取租戶名稱以檢視租戶身分識別聯盟詳細資料"
- "選取租戶名稱以檢視租戶平台服務詳細資料"
- "在端點建立期間指定平台服務端點憑證"

其他

針對特定用途使用其他安全性憑證。StorageGRID這些憑證會依其功能名稱列出。其他安全性憑證包括：

- 雲端儲存資源池認證
- 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
- 身分識別聯盟憑證

- 金鑰管理伺服器（KMS）憑證
- 單一登入憑證

資訊指出功能使用的憑證類型、以及適用的伺服器和用戶端憑證到期日。選取功能名稱會開啟瀏覽器索引標籤、您可以在其中檢視及編輯憑證詳細資料。

您只能在擁有適當權限的情況下檢視及存取其他憑證的資訊。

您可以：

- "指定S3、C2S S3或Azure的雲端儲存池憑證"
- "指定警示電子郵件通知的憑證"
- "指定外部syslog伺服器憑證"
- "旋轉網格同盟連線憑證"
- "檢視及編輯身分識別聯盟憑證"
- "上傳金鑰管理伺服器（KMS）伺服器和用戶端憑證"
- "手動指定依賴方信任的 SSO 憑證"

安全性憑證詳細資料

每種安全性憑證類型如下所述、並提供實作指示的連結。

管理介面認證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證用戶端網頁瀏覽器與StorageGRID RealSet管理介面之間的連線、讓使用者能夠存取Grid Manager和Tenant Manager、而不會出現安全性警告。 此憑證也會驗證Grid Management API和租戶管理API連線。 您可以使用安裝期間建立的預設憑證、或是上傳自訂憑證。	組態>*安全性*>*憑證*、選取*全域*索引標籤、然後選取*管理介面憑證*	"設定管理介面憑證"

S3和Swift API認證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證安全的 S3 或 Swift 用戶端連線至儲存節點和負載平衡器端點（選用）。	組態>*安全性*>*憑證*、選取*全域*索引標籤、然後選取* S3和Swift API憑證*	"設定S3和Swift API憑證"

Grid CA憑證

請參閱 預設Grid CA憑證說明。

系統管理員用戶端憑證

憑證類型	說明	導覽位置	詳細資料
用戶端	安裝在每個用戶端上、StorageGRID 讓功能驗證外部用戶端存取。 • 允許授權的外部用戶端存取StorageGRID《The WilsPrometheus資料庫》。 • 允許StorageGRID 使用外部工具安全監控功能。	組態>*安全性*>*憑證*、然後選取*用戶端*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	導覽位置	詳細資料
伺服器	驗證S3或Swift用戶端之間的連線、StorageGRID 以及閘道節點和管理節點上的「RealsLoad Balancer」服務。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StorageGRID 至物件資料時、會使用負載平衡器憑證來儲存及擷取物件資料。 您也可以使用全域的自訂版本 S3和Swift API認證 用於驗證負載平衡器服務連線的憑證。如果使用全域憑證來驗證負載平衡器連線、您就不需要為每個負載平衡器端點上傳或產生個別的憑證。 *附註：*用於負載平衡器驗證的憑證、是正常StorageGRID 執行過程中最常使用的憑證。	組態>*網路*>*負載平衡器端點*	• "設定負載平衡器端點" • "建立FabricPool 負載平衡器端點以供使用"

雲端儲存資源池端點憑證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證StorageGRID 從Ss3 Glacier或Microsoft Azure Blob儲存設備等外部儲存位置的連接。每種雲端供應商類型都需要不同的憑證。	• ILM >*儲存資源池	"建立雲端儲存資源池"

電子郵件警示通知憑證

憑證類型	說明	導覽位置	詳細資料
伺服器與用戶端	驗證用於StorageGRID 警示通知的SMTP電子郵件伺服器與功能鏈之間的連線。 • 如果與SMTP伺服器的通訊需要傳輸層安全性（TLS）、您必須指定電子郵件伺服器CA憑證。 • 只有在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。	警示>*電子郵件設定*	"設定警示的電子郵件通知"

外部**syslog**伺服器憑證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證外部syslog伺服器之間的TLS或RELP/TLS連線、該伺服器會將事件記錄StorageGRID 在整個過程中。 *附註：*不需要外部系統記錄伺服器憑證、就能連接到外部系統記錄伺服器的TCP、RELP/TCP及udp連線。	組態>*監控*>*稽核與系統記錄伺服器*、然後選取*設定外部系統記錄伺服器*	"設定外部syslog伺服器"

[[grid-Federation 認證 **]] Grid** 聯盟連線憑證

憑證類型	說明	導覽位置	詳細資料
伺服器與用戶端	驗證並加密目前StorageGRID 系統與網格同盟連線中其他網格之間傳送的資訊。	• 組態 * > * 系統 * > * 網格聯盟 *	• "建立網格同盟連線" • "旋轉連線憑證"

身分識別聯盟憑證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證StorageGRID Reality與外部身分識別供應商（例如Active Directory、OpenLDAP或Oracle Directory Server）之間的連線。用於身分識別聯盟、可讓管理員群組和使用者由外部系統管理。	組態>*存取控制*>*身分識別聯盟*	"使用身分識別聯盟"

金鑰管理伺服器（**KMS**）憑證

憑證類型	說明	導覽位置	詳細資料
伺服器與用戶端	驗證StorageGRID 支援功能與外部金鑰管理伺服器（KMS）之間的連線、此伺服器可為StorageGRID 應用裝置節點提供加密金鑰。	組態>*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	導覽位置	詳細資料
伺服器	驗證StorageGRID 從SReals功能 平台服務到S3儲存資源的連線。	租戶管理程式>*儲存設備（S3）>*平台服務端點	"建立平台服務端點" "編輯平台服務端點"

單一登入（**SSO**）憑證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證身分識別聯盟服務（例如Active Directory Federation Services（AD FS））和StorageGRID 用來處理單一登入（SSO）要求的支援服務之間的連線。	組態>*存取控制*>*單一登入*	"設定單一登入"

憑證範例

範例**1**：負載平衡器服務

在此範例中StorageGRID 、用作伺服器的是功能。

1. 您可以設定負載平衡器端點、並在StorageGRID 中上傳或產生伺服器憑證。

2. 您可以設定S3或Swift用戶端連線至負載平衡器端點、然後將相同的憑證上傳至用戶端。
3. 當用戶端想要儲存或擷取資料時、會使用HTTPS連線至負載平衡器端點。
4. 以伺服器憑證做出回應、其中包含公開金鑰、並以私密金鑰為基礎提供簽名。StorageGRID
5. 用戶端會將伺服器簽章與憑證複本上的簽章進行比較、藉此驗證此憑證。如果簽名相符、用戶端就會使用相同的公開金鑰來啟動工作階段。
6. 用戶端會將物件資料傳送StorageGRID 至物件資料。

範例**2**：外部金鑰管理伺服器（**KMS**）

在此範例中StorageGRID 、由客戶扮演的角色就是

1. 使用外部金鑰管理伺服器軟體、您可以將StorageGRID 效能設定為KMS用戶端、並取得CA簽署的伺服器憑證、公用用戶端憑證及用戶端憑證的私密金鑰。
2. 您可以使用Grid Manager設定KMS伺服器、並上傳伺服器和用戶端憑證及用戶端私密金鑰。
3. 當某個節點需要加密金鑰時、它會向KMS伺服器提出要求、要求其中包含來自憑證的資料、以及以私密金鑰為基礎的簽名。StorageGRID
4. KMS伺服器會驗證憑證簽章、並決定其是否值得信賴StorageGRID 。
5. KMS伺服器會使用已驗證的連線來回應。

設定伺服器憑證

支援的伺服器憑證類型

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

安全性原則的加密類型必須符合伺服器憑證類型。例如、 RSA 加密器需要 RSA 憑證、而 ECDSA 加密器則需要 ECDSA 憑證。請參閱 "管理安全性憑證"。如果您設定的自訂安全性原則與伺服器憑證不相容、您可以 "暫時恢復為預設的安全性原則"。

如需 StorageGRID 如何保護 REST API 用戶端連線的詳細資訊、請參閱 "設定 S3 REST API 的安全性" 或 "設定 Swift REST API 的安全性"。

設定管理介面憑證

您可以使用單一自訂憑證來取代預設的管理介面憑證、讓使用者能夠存取Grid Manager和租戶管理程式、而不會遇到安全性警告。您也可以還原為預設的管理介面憑證、或是產生新的憑證。

關於這項工作

根據預設、每個管理節點都會核發由網格CA簽署的憑證。這些CA簽署的憑證可由單一通用的自訂管理介面憑證和對應的私密金鑰取代。

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、則必須將憑證指定為萬用字元或多網域憑證。定義自訂憑證、使其符合網格中的所有管理節點。

您需要在伺服器上完成組態、視您使用的根憑證授權單位（CA）而定、使用者可能也需要在網頁瀏覽器中安裝Grid CA憑證、以便存取Grid Manager和租戶管理程式。

> 為了確保作業不會因伺服器憑證故障而中斷、當此伺服器憑證即將過期時、就會觸發 * 管理介面伺服器憑證過期 * 警示。如有需要、您可以選取*組態*>*安全性*>*憑證*來檢視目前憑證的到期日、並在「全域」索引標籤上查看管理介面憑證的到期日。

> 如果您使用網域名稱而非IP位址來存取Grid Manager或Tenant Manager、則瀏覽器會顯示憑證錯誤、且在發生下列任一情況時、不會出現跳過的選項：
>
> - 您的自訂管理介面憑證將過期。
> - 您 從自訂管理介面憑證還原為預設伺服器憑證。

新增自訂管理介面認證

若要新增自訂管理介面認證、您可以提供自己的認證、或使用Grid Manager產生認證。

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取*管理介面認證*。
3. 選擇*使用自訂憑證*。
4. 上傳或產生憑證。

上傳憑證

上傳所需的伺服器憑證檔案。

a. 選擇*上傳憑證*。

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）。
   - * 憑證私密金鑰 * ：自訂伺服器憑證私密金鑰檔案 (`.key`）。

     EC私密金鑰必須大於或等於224位元。RSA私密金鑰必須大於或等於2048位元。

   - * CA套裝組合*：單一選用檔案、內含來自每個中繼發行憑證授權單位（CA）的憑證。檔案應包含以憑證鏈順序串聯的每個由PEE編碼的CA憑證檔案。

c. 展開*憑證詳細資料*、即可查看您上傳之每個憑證的中繼資料。如果您上傳了選用的CA套件、每個憑證都會顯示在其各自的索引標籤上。

   - 選取*下載憑證*以儲存憑證檔案、或選取*下載CA套件*以儲存憑證套件組合。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選擇*複製憑證PEP*或*複製CA套裝組合PEP*、即可複製憑證內容以貼到其他位置。

d. 選擇*保存*。+自訂管理介面憑證可用於所有後續新連線至Grid Manager、Tenant Manager、Grid Manager API或Tenant Manager API。

產生憑證

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*產生憑證*。

b. 指定憑證資訊：

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*作為萬用字元來代表多個網域名稱。
IP	要包含在憑證中的一或多個 IP 位址。
主旨（選用）	憑證擁有者的 X.509 主體或辨別名稱（ DN ）。 如果在此欄位中未輸入任何值、則產生的憑證會使用第一個網域名稱或 IP 位址做為主體一般名稱（ CN ）。

欄位	說明
有效天數	憑證建立後過期的天數。
新增金鑰使用方式擴充功能	如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸會新增至產生的憑證。 這些延伸定義了憑證中所含金鑰的用途。 • 附註 * ：除非您在憑證包含這些副檔名時遇到舊版用戶端的連線問題、否則請保留此核取方塊。

c. 選取*產生*。

d. 選取*憑證詳細資料*以查看所產生憑證的中繼資料。

- 選取*下載憑證*以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

e. 選擇*保存*。+自訂管理介面憑證可用於所有後續新連線至Grid Manager、Tenant Manager、Grid Manager API或Tenant Manager API。

5. 重新整理頁面以確保網頁瀏覽器已更新。

上傳或產生新的憑證後、請允許清除任何相關的憑證過期警示一天。

6. 新增自訂管理介面憑證之後、「管理介面憑證」頁面會顯示使用中憑證的詳細憑證資訊。+您可以視需要下載或複製憑證PEE。

還原預設的管理介面憑證

您可以恢復使用Grid Manager和Tenant Manager連線的預設管理介面憑證。

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取*管理介面認證*。
3. 選擇*使用預設憑證*。

   當您還原預設的管理介面憑證時、您設定的自訂伺服器憑證檔案會被刪除、而且無法從系統中還原。預設的管理介面憑證會用於所有後續的新用戶端連線。

4. 重新整理頁面以確保網頁瀏覽器已更新。

使用指令碼來產生新的自我簽署管理介面憑證

如果需要嚴格的主機名稱驗證、您可以使用指令碼來產生管理介面憑證。

開始之前

- 您擁有特定的存取權限。
- 您擁有 `Passwords.txt` 檔案：

關於這項工作

正式作業環境的最佳實務做法是使用外部憑證授權單位所簽署的憑證。

步驟

1. 取得每個管理節點的完整網域名稱（FQDN）。
2. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

      當您以root登入時、提示會從變更 `$` 至 `#`。
3. 使用StorageGRID 新的自我簽署憑證來設定功能。

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

   - 適用於 `--domains`、使用萬用字元代表所有管理節點的完整網域名稱。例如、 `*.ui.storagegrid.example.com` 使用*萬用字元表示 `admin1.ui.storagegrid.example.com` 和 `admin2.ui.storagegrid.example.com`。
   - 設定 `--type` 至 `management` 設定 Grid Manager 和 Tenant Manager 使用的管理介面憑證。
   - 根據預設、產生的憑證有效期間為一年（365天）、必須在到期前重新建立。您可以使用 `--days` 用於置換預設有效期間的引數。

     > 憑證的有效期間始於何時 `make-certificate` 執行。您必須確保管理用戶端與StorageGRID 其他來源同步、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
     ```

     產生的輸出包含管理API用戶端所需的公開憑證。
4. 選取並複製憑證。

   在您的選擇中加入開始標記和結束標記。

5. 登出命令Shell。 `$ exit`
6. 確認已設定憑證：
   a. 存取Grid Manager。
   b. 選擇*組態*>*安全性*>*憑證*
   c. 在* Global*索引標籤上、選取*管理介面認證*。
7. 設定管理用戶端使用您複製的公用憑證。包括開始和結束標記。

下載或複製管理介面憑證

您可以儲存或複製管理介面憑證內容、以便在其他地方使用。

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取*管理介面認證*。
3. 選取「伺服器」或「* CA套裝組合*」索引標籤、然後下載或複製憑證。

   下載憑證檔案或**CA**套裝組合

   下載憑證或 CA 套件 `.pem` 檔案：如果您使用選用的CA套件組合、套件中的每個憑證都會顯示在其各自的子索引標籤上。

   a. 選擇*下載憑證*或*下載CA套裝組合*。

      如果您要下載CA套件、CA套件次要索引標籤中的所有憑證都會以單一檔案下載。

   b. 指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

      例如： `storagegrid_certificate.pem`

   複製憑證或**CA**套裝組合**PEE**

   複製憑證文字以貼到其他位置。如果您使用選用的CA套件組合、套件中的每個憑證都會顯示在其各自的子索引標籤上。

   a. 選擇*複製憑證PEP*或*複製CA套裝組合PEP*。

      如果您要複製CA套件組合、CA套件中的所有憑證都會一起複製二線索引標籤。

   b. 將複製的憑證貼到文字編輯器中。
   c. 以副檔名儲存文字檔 `.pem`。

      例如： `storagegrid_certificate.pem`

設定S3和Swift API憑證

您可以取代或還原用於 S3 或 Swift 用戶端連線至儲存節點或負載平衡器端點的伺服器憑證。置換的自訂伺服器憑證是您組織專屬的。

關於這項工作

根據預設、每個儲存節點都會核發由網格CA簽署的X．509伺服器憑證。這些CA簽署的憑證可由單一通用的自訂伺服器憑證和對應的私密金鑰取代。

所有儲存節點都使用單一自訂伺服器憑證、因此如果用戶端在連線至儲存端點時需要驗證主機名稱、則必須將憑證指定為萬用字元或多網域憑證。定義自訂憑證、使其符合網格中的所有儲存節點。

在伺服器上完成組態之後、您可能還需要在S3或Swift API用戶端中安裝Grid CA憑證、以便根據所使用的根憑證授權單位（CA）來存取系統。

> 為了確保作業不會因伺服器憑證故障而中斷、當根伺服器憑證即將過期時、會觸發 S3 和 Swift API* 的 * 全域伺服器憑證過期。如有需要、您可以選取*組態*>*安全性*>*憑證*來檢視目前憑證的到期日、並在「全域」索引標籤上查看S3和Swift API憑證的到期日。

您可以上傳或產生自訂的S3和Swift API認證。

新增自訂S3和Swift API認證

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取* S3和Swift API認證*。
3. 選擇*使用自訂憑證*。
4. 上傳或產生憑證。

上傳憑證

上傳所需的伺服器憑證檔案。

a. 選擇*上傳憑證*。

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）。
   - * 憑證私密金鑰 * ：自訂伺服器憑證私密金鑰檔案 (`.key`）。

     EC私密金鑰必須大於或等於224位元。RSA私密金鑰必須大於或等於2048位元。

   - * CA套裝組合*：單一選用檔案、內含來自每個中繼發行憑證授權單位的憑證。檔案應包含以憑證鏈順序串聯的每個由PEE編碼的CA憑證檔案。

c. 選取憑證詳細資料、以顯示上傳之每個自訂S3和Swift API憑證的中繼資料和PEM。如果您上傳了選用的CA套件、每個憑證都會顯示在其各自的索引標籤上。

   - 選取*下載憑證*以儲存憑證檔案、或選取*下載CA套件*以儲存憑證套件組合。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選擇*複製憑證PEP*或*複製CA套裝組合PEP*、即可複製憑證內容以貼到其他位置。

d. 選擇*保存*。

   自訂伺服器憑證用於後續的S3和Swift用戶端連線。

產生憑證

產生伺服器憑證檔案。

a. 選擇*產生憑證*。

b. 指定憑證資訊：

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*作為萬用字元來代表多個網域名稱。
IP	要包含在憑證中的一或多個 IP 位址。
主旨（選用）	憑證擁有者的 X.509 主體或辨別名稱（ DN ）。 如果在此欄位中未輸入任何值、則產生的憑證會使用第一個網域名稱或 IP 位址做為主體一般名稱（ CN ）。

欄位	說明
有效天數	憑證建立後過期的天數。
新增金鑰使用方式擴充功能	如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸會新增至產生的憑證。 這些延伸定義了憑證中所含金鑰的用途。 • 附註 * ：除非您在憑證包含這些副檔名時遇到舊版用戶端的連線問題、否則請保留此核取方塊。

c. 選取*產生*。

d. 選取*「憑證詳細資料」*以顯示所產生之自訂S3和Swift API憑證的中繼資料和PEM。

- 選取*下載憑證*以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

e. 選擇*保存*。

自訂伺服器憑證用於後續的S3和Swift用戶端連線。

5. 選取索引標籤以顯示預設StorageGRID 的還原伺服器憑證的中繼資料、已上傳的CA簽署憑證、或是已產生的自訂憑證。

   上傳或產生新的憑證後、請允許清除任何相關的憑證過期警示一天。

6. 重新整理頁面以確保網頁瀏覽器已更新。

7. 新增自訂S3和Swift API憑證之後、S3和Swift API憑證頁面會顯示使用中自訂S3和Swift API憑證的詳細憑證資訊。+您可以視需要下載或複製憑證PEE。

還原預設的**S3**和**Swift API**憑證

您可以將 S3 和 Swift 用戶端連線的預設 S3 和 Swift API 憑證還原成儲存節點。不過、您無法將預設的 S3 和 Swift API 憑證用於負載平衡器端點。

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取* S3和Swift API認證*。
3. 選擇*使用預設憑證*。

   當您還原全域 S3 和 Swift API 憑證的預設版本時、您所設定的自訂伺服器憑證檔案會遭到刪除、而且無法從

系統中還原。預設的 S3 和 Swift API 憑證將用於後續新的 S3 和 Swift 用戶端連線至儲存節點。

4. 選取*確定*以確認警告並還原預設的S3和Swift API憑證。

   如果您具有根存取權限、而且自訂S3和Swift API憑證已用於負載平衡器端點連線、則會顯示負載平衡器端點清單、無法再使用預設S3和Swift API憑證存取。前往 "設定負載平衡器端點" 可編輯或刪除受影響的端點。

5. 重新整理頁面以確保網頁瀏覽器已更新。

下載或複製**S3**和**Swift API**認證

您可以儲存或複製S3和Swift API憑證內容、以便在其他地方使用。

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取* S3和Swift API認證*。
3. 選取「伺服器」或「* CA套裝組合*」索引標籤、然後下載或複製憑證。

下載憑證檔案或**CA**套裝組合

下載憑證或 CA 套件 `.pem` 檔案：如果您使用選用的CA套件組合、套件中的每個憑證都會顯示在其各自的子索引標籤上。

a. 選擇*下載憑證*或*下載CA套裝組合*。

   如果您要下載CA套件、CA套件次要索引標籤中的所有憑證都會以單一檔案下載。

b. 指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

複製憑證或**CA**套裝組合**PEE**

複製憑證文字以貼到其他位置。如果您使用選用的CA套件組合、套件中的每個憑證都會顯示在其各自的子索引標籤上。

a. 選擇*複製憑證PEP*或*複製CA套裝組合PEP*。

   如果您要複製CA套件組合、CA套件中的所有憑證都會一起複製二線索引標籤。

b. 將複製的憑證貼到文字編輯器中。

c. 以副檔名儲存文字檔 `.pem`。

   例如： `storagegrid_certificate.pem`

相關資訊

- "使用S3 REST API"
- "使用Swift REST API"

- "設定 S3 端點網域名稱"

複製Grid CA憑證

使用內部憑證授權單位（CA）來保護內部流量。StorageGRID如果您上傳自己的憑證、此憑證不會變更。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有特定的存取權限。

關於這項工作

如果已設定自訂伺服器憑證、用戶端應用程式應使用自訂伺服器憑證來驗證伺服器。他們不應該從StorageGRID這個系統複製CA憑證。

步驟

1. 選擇*組態*>*安全性*>*憑證*、然後選取*網格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. 選擇*下載憑證*。

   b. 指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

      例如： `storagegrid_certificate.pem`

   複製憑證**PE**

   複製憑證文字以貼到其他位置。

   a. 選擇*複製憑證PEP*。

   b. 將複製的憑證貼到文字編輯器中。

   c. 以副檔名儲存文字檔 `.pem`。

      例如： `storagegrid_certificate.pem`

設定StorageGRID 適用FabricPool 的驗證

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

- 您擁有特定的存取權限。

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。

關於這項工作

建立負載平衡器端點時、您可以產生自我簽署的伺服器憑證、或是上傳由已知憑證授權單位（CA）簽署的憑證。在正式作業環境中、您應該使用由已知CA簽署的憑證。由CA簽署的憑證可在不中斷營運的情況下循環。它們也更安全、因為它們能更有效地防範攔截式攻擊。

下列步驟為使用FabricPool 支援功能的S3用戶端提供一般準則。如需詳細資訊和程序、請參閱 "設定StorageGRID 適用於FabricPool 靜態的"。

步驟

1. 或者、設定高可用度（HA）群組FabricPool 以供使用。
2. 建立S3負載平衡器端點FabricPool 以供使用。

   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、憑證私密金鑰及選用的CA套件組合。

3. 在StorageGRID 整個過程中附加作雲端層的功能。ONTAP

   指定負載平衡器端點連接埠、以及您上傳的CA憑證所使用的完整網域名稱。然後提供CA憑證。

   如果中介CA核發StorageGRID 了此資訊證書、您必須提供中繼CA憑證。如果StorageGRID 此驗證是由根CA直接發出、您必須提供根CA憑證。

設定用戶端憑證

用戶端憑證可讓獲授權的外部用戶端存取StorageGRID 《The》《The VMware資料庫》、為外部工具提供安全的監控StorageGRID 方式。

如果您需要StorageGRID 使用外部監控工具存取功能、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。

請參閱 "管理安全性憑證" 和 "設定自訂伺服器憑證"。

為了確保作業不會因伺服器憑證故障而中斷、當此伺服器憑證即將過期時、會觸發「憑證頁面 * 」警示上設定的 * 用戶端憑證到期日。如有需要、您可以選取*組態*>*安全性*>*憑證*來檢視目前憑證的到期日、並在「用戶端」索引標籤上查看用戶端憑證的到期日。

如果您使用金鑰管理伺服器（KMS）來保護特殊設定應用裝置節點上的資料、請參閱相關的特定資訊 "上傳KMS用戶端憑證"。

開始之前

- 您擁有root存取權限。
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 若要設定用戶端憑證：
  - 您擁有管理節點的IP位址或網域名稱。
  - 如果您已設定StorageGRID 完整套管理介面認證、則會使用CA、用戶端認證和私密金鑰來設定管理介面

認證。

- 若要上傳您自己的憑證、您可以在本機電腦上取得該憑證的私密金鑰。
- 私密金鑰必須在建立時已儲存或記錄。如果您沒有原始的私密金鑰、則必須建立新的私密金鑰。

- 若要編輯用戶端憑證：
  - 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的憑證、您的本機電腦上可以使用私密金鑰、用戶端憑證和CA（如果使用）。

新增用戶端憑證

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發行的用戶端憑證
- 從Grid Manager產生憑證

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來設定管理介面憑證、請使用此程序來新增用戶端憑證。

步驟

1. 在Grid Manager中、選取*組態*>*安全性*>*憑證*、然後選取*用戶端*索引標籤。
2. 選取*「Add*」。
3. 輸入憑證名稱。
4. 若要使用您的外部監控工具存取 Prometheus* 指標、請選取 * 允許 Prometheus* 。
5. 選擇*繼續*。
6. 對於 * 附加憑證 * 步驟、請上傳管理介面憑證。
   a. 選擇*上傳憑證*。
   b. 選取 * 瀏覽 * 並選取管理介面憑證檔案 (`.pem`) 。
      - 選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。
      - 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。
   c. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

      新的憑證會顯示在「用戶端」索引標籤上。
7. 設定外部監控工具例如 Grafana 。

CA發行的用戶端憑證

如果未設定管理介面憑證、且您計畫新增使用CA發行用戶端憑證和私密金鑰的Prometheus用戶端憑證、請使用此程序來新增管理員用戶端憑證。

步驟

1. 執行步驟至 "設定管理介面憑證"。
2. 在Grid Manager中、選取*組態*>*安全性*>*憑證*、然後選取*用戶端*索引標籤。
3. 選取*「Add*」。
4. 輸入憑證名稱。
5. 若要使用您的外部監控工具存取 Prometheus* 指標、請選取 * 允許 Prometheus* 。
6. 選擇*繼續*。
7. 對於 * 附加憑證 * 步驟、請上傳用戶端憑證、私密金鑰和 CA 套裝組合檔案：
   a. 選擇*上傳憑證*。
   b. 選取 * 瀏覽 * 並選取用戶端憑證、私密金鑰和 CA 套件檔案 (`.pem`) 。
      - 選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。
      - 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。
   c. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

      新的憑證會顯示在「用戶端」索引標籤上。
8. 設定外部監控工具例如 Grafana 。

從**Grid Manager**產生憑證

如果管理介面憑證尚未設定、且您計畫在Grid Manager中新增使用產生憑證功能的Prometheus用戶端憑證、請使用此程序來新增管理員用戶端憑證。

步驟

1. 在Grid Manager中、選取*組態*>*安全性*>*憑證*、然後選取*用戶端*索引標籤。
2. 選取*「Add*」。
3. 輸入憑證名稱。
4. 若要使用您的外部監控工具存取 Prometheus* 指標、請選取 * 允許 Prometheus* 。
5. 選擇*繼續*。
6. 對於 * 附加憑證 * 步驟、請選取 * 產生憑證 * 。
7. 指定憑證資訊：
   - * 主旨 *（選用）：憑證擁有者的 X.509 主體或辨別名稱（ DN ）。
   - * 有效天數 * ：產生的憑證自產生之日起有效的天數。
   - * 新增金鑰使用方式延伸 * ：如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸功能會新增至產生的憑證。

     這些延伸定義了憑證中所含金鑰的用途。

     除非您在憑證包含這些副檔名時、遇到舊版用戶端的連線問題、否則請保留此核取方塊。
8. 選取*產生*。

9. [Client_cert詳細資料]選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。

   關閉對話方塊後、您將無法檢視憑證私密金鑰。將金鑰複製或下載到安全位置。

   - 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。
   - 選取*下載憑證*以儲存憑證檔案。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選取*複製私密金鑰*以複製憑證私密金鑰、以便貼到其他位置。
   - 選取*下載私密金鑰*將私密金鑰儲存為檔案。

     指定私密金鑰檔案名稱和下載位置。

10. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

    新的憑證會顯示在「用戶端」索引標籤上。

11. 在Grid Manager中、選取*組態*>*安全性*>*憑證*、然後選取*全域*索引標籤。
12. 選擇*管理介面認證*。
13. 選擇*使用自訂憑證*。
14. 從上傳認證.pem和Private金鑰.pem檔案 用戶端憑證詳細資料 步驟。不需要上傳CA套裝組合。
    a. 選擇*上傳認證*、然後選擇*繼續*。
    b. 上傳每個憑證檔案 (`.pem`）。
    c. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

       新的憑證會顯示在「用戶端」索引標籤上。

15. 設定外部監控工具例如 Grafana 。

設定外部監控工具

步驟

1. 在外部監控工具（例如Grafana）上設定下列設定。
   a. 名稱：輸入連線名稱。

      不需要此資訊、但您必須提供名稱來測試連線。StorageGRID

   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用戶端驗證*和* CA認證*。
   d. 在「TLS/SSL驗證詳細資料」下、複製並貼上：+

- 管理介面CA憑證至「**CA認證」
- 用戶端認證至*用戶端認證
- 用於**用戶端金鑰*的私密金鑰

e. 伺服器名稱：輸入管理節點的網域名稱。

伺服器名稱必須符合管理介面憑證中顯示的網域名稱。

2. 儲存並測試您從StorageGRID 餐廳或本機檔案複製的憑證和私密金鑰。

您現在可以StorageGRID 使用外部監控工具、從功能表上存取Prometheus指標。

如需度量的相關資訊、請參閱 "監控StorageGRID 功能說明"。

編輯用戶端憑證

您可以編輯系統管理員用戶端憑證來變更其名稱、啟用或停用Prometheus存取、或是在目前憑證過期時上傳新的憑證。

步驟

1. 選擇*組態*>*安全性*>*憑證*、然後選擇*用戶端*索引標籤。

下表列出憑證到期日和Prometheus存取權限。如果憑證即將到期或已過期、表格中會出現訊息、並觸發警示。

2. 選取您要編輯的憑證。
3. 選取*編輯*、然後選取*編輯名稱和權限*
4. 輸入憑證名稱。
5. 若要使用您的外部監控工具存取 Prometheus* 指標、請選取 * 允許 Prometheus* 。
6. 選擇*繼續*以在Grid Manager中儲存憑證。

更新的憑證會顯示在「用戶端」索引標籤上。

附加新的用戶端憑證

您可以在目前的憑證過期時上傳新的憑證。

步驟

1. 選擇*組態*>*安全性*>*憑證*、然後選擇*用戶端*索引標籤。

下表列出憑證到期日和Prometheus存取權限。如果憑證即將到期或已過期、表格中會出現訊息、並觸發警示。

2. 選取您要編輯的憑證。
3. 選取*編輯*、然後選取編輯選項。

上傳憑證

複製憑證文字以貼到其他位置。

a. 選擇*上傳認證*、然後選擇*繼續*。

b. 上傳用戶端憑證名稱 (`.pem`) 。

   選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。

   - 選取*下載憑證*以儲存憑證檔案。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

c. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

   更新的憑證會顯示在「用戶端」索引標籤上。

產生憑證

產生要貼到其他位置的憑證文字。

a. 選擇*產生憑證*。

b. 指定憑證資訊：

   - * 主旨 * （選用）：憑證擁有者的 X.509 主體或辨別名稱（ DN ）。
   - * 有效天數 * ：產生的憑證自產生之日起有效的天數。
   - * 新增金鑰使用方式延伸 * ：如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸功能會新增至產生的憑證。

     這些延伸定義了憑證中所含金鑰的用途。

     除非您在憑證包含這些副檔名時、遇到舊版用戶端的連線問題、否則請保留此核取方塊。

c. 選取*產生*。

d. 選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。

   關閉對話方塊後、您將無法檢視憑證私密金鑰。將金鑰複製或下載到安全位置。

   - 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。
   - 選取*下載憑證*以儲存憑證檔案。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

例如： `storagegrid_certificate.pem`

- 選取*複製私密金鑰*以複製憑證私密金鑰、以便貼到其他位置。
- 選取*下載私密金鑰*將私密金鑰儲存為檔案。

  指定私密金鑰檔案名稱和下載位置。

e. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

新的憑證會顯示在「用戶端」索引標籤上。

下載或複製用戶端憑證

您可以下載或複製用戶端憑證、以便在其他地方使用。

步驟

1. 選擇*組態*>*安全性*>*憑證*、然後選擇*用戶端*索引標籤。
2. 選取您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. 選擇*下載憑證*。

b. 指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

例如： `storagegrid_certificate.pem`

複製憑證

複製憑證文字以貼到其他位置。

a. 選擇*複製憑證PEP*。

b. 將複製的憑證貼到文字編輯器中。

c. 以副檔名儲存文字檔 `.pem`。

例如： `storagegrid_certificate.pem`

移除用戶端憑證

如果不再需要系統管理員用戶端憑證、您可以將其移除。

步驟

1. 選擇*組態*>*安全性*>*憑證*、然後選擇*用戶端*索引標籤。
2. 選取您要移除的憑證。
3. 選擇*刪除*、然後確認。

若要移除最多10個憑證、請在「用戶端」索引標籤上選取要移除的每個憑證、然後選取*「動作」>「刪除」*。

移除憑證後、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 《The動ePrometheus資料庫》。