管理安全
StorageGRID software

NetApp
May 29, 2026

目錄

管理安全

管理安全

您可以從網格管理器配置各種安全性設定來協助保護您的StorageGRID系統。

管理加密

StorageGRID提供了多種資料加密選項。你應該"查看可用的加密方法"以確定哪些符合您的資料保護要求。

管理證書

你可以"設定和管理伺服器證書"用於 HTTP 連線或用於向伺服器驗證用戶端或使用者身分的用戶端憑證。

配置金鑰管理伺服器

使用"金鑰管理伺服器"即使設備從資料中心移除，也能保護StorageGRID資料。裝置磁碟區加密後，除非節點可以與 KMS 通信，否則您無法存取裝置上的任何資料。

> 若要使用加密金鑰管理，您必須在安裝期間、將裝置新增至電網之前為每個裝置啟用「節點加密」設定。

管理代理設定

如果您使用 S3 平台服務或雲端儲存池，您可以設定"儲存代理伺服器"儲存節點和外部 S3 端點之間。如果您使用 HTTPS 或 HTTP 傳送AutoSupport軟體包，則可以設定"管理代理伺服器"管理節點和技術支援之間。

控制防火牆

為了增強系統的安全性，您可以透過開啟或關閉特定連接埠來控制對StorageGRID管理節點的存取"外部防火牆"。您還可以透過配置每個節點來控制其網路存取"內部防火牆"。您可以阻止部署所需連接埠之外的所有連接埠的存取。

查看StorageGRID加密方法

StorageGRID提供了多種資料加密選項。您應該檢查可用的方法以確定哪些方法符合您的資料保護要求。

此表提供了StorageGRID中可用的加密方法的進階摘要。

加密選項	工作原理	適用於
Grid Manager 中的金鑰管理伺服器 (KMS)	你"配置金鑰管理伺服器"對於StorageGRID站點和 "為裝置啟用節點加密"。然後，裝置節點連接到 KMS 以請求金鑰加密金鑰 (KEK)。此金鑰對每個磁碟區上的資料加密金鑰 (DEK) 進行加密和解密。	安裝期間啟用了*節點加密*的裝置節點。設備上的所有資料都受到保護，不會發生實體遺失或從資料中心移除。 注意：僅儲存節點和服務設備支援使用 KMS 管理加密金鑰。
StorageGRID裝置安裝程式中的磁碟機加密頁面	如果裝置包含支援硬體加密的驅動器，您可以在安裝期間設定驅動器密碼。當您設定磁碟機密碼時，任何人都不可能從已從系統中刪除的磁碟機中恢復有效數據，除非他們知道密碼。在開始安裝之前，請前往*設定硬體*>*磁碟機加密*來設定適用於節點中所有StorageGRID管理的自加密磁碟機的磁碟機密碼。	包含自加密磁碟機的裝置。安全驅動器上的所有資料都受到保護，不會發生實體遺失或從資料中心移除。 磁碟機加密不適用於SANtricity管理的磁碟機。如果您擁有具有自加密磁碟機和SANtricity控制器的儲存設備，則可以在SANtricity中啟用磁碟機安全性。
推動SANtricity System Manager 的安全性	如果您的StorageGRID裝置啟用了磁碟機安全功能，則可以使用 "SANtricity系統管理員"建立和管理安全密鑰。需要密鑰才能存取安全驅動器上的資料。	具有全碟加密 (FDE) 磁碟機或自加密磁碟機的儲存裝置。安全驅動器上的所有資料都受到保護，不會發生實體遺失或從資料中心移除。不能與某些儲存設備或任何服務設備一起使用。
儲存物件加密	您啟用"儲存物件加密"網格管理器中的選項。啟用後，任何未在儲存桶層級或物件層級加密的新物件都會在攝取期間加密。	新攝取的 S3 物件資料。 現有儲存的物件未加密。對像元資料和其他敏感資料未加密。
S3 儲存桶加密	您發出 PutBucketEncryption 請求來為儲存桶啟用加密。任何未在物件層級加密的新物件都會在攝取期間加密。	僅限新攝取的 S3 物件資料。 必須為儲存桶指定加密。現有的儲存桶物件未加密。對像元資料和其他敏感資料未加密。 "對 bucket 的操作"
S3 物件伺服器端加密 (SSE)	您發出一個 S3 請求來儲存一個物件並包括 `x-amz-server-side-encryption`請求標頭。	僅限新攝取的 S3 物件資料。 必須為物件指定加密。對像元資料和其他敏感資料未加密。 StorageGRID管理金鑰。 "使用伺服器端加密"

加密選項	工作原理	適用於
使用客戶提供的金鑰對 S3 物件進行伺服器端加密 (SSE-C)	您發出 S3 請求來儲存物件並包含三個請求標頭。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	僅限新攝取的 S3 物件資料。 必須為物件指定加密。對像元資料和其他敏感資料未加密。 密鑰在StorageGRID之外進行管理。 "使用伺服器端加密"
外部磁碟區或資料儲存加密	如果您的部署平台支持，您可以使用StorageGRID以外的加密方法來加密整個磁碟區或資料儲存。	所有物件資料、元資料和系統配置資料（假設每個磁碟區或資料儲存都經過加密）。 外部加密方法可以對加密演算法和金鑰進行更嚴格的控制。可以與列出的其他方法結合使用。
StorageGRID以外的物件加密	您可以使用StorageGRID外部的加密方法在物件資料和元資料被匯入StorageGRID之前對其進行加密。	僅物件資料和元資料（系統配置資料未加密）。 外部加密方法可以對加密演算法和金鑰進行更嚴格的控制。可以與列出的其他方法結合使用。 "Amazon Simple Storage Service - 使用者指南：使用客戶端加密保護資料"

使用多種加密方法

根據您的要求，您可以一次使用多種加密方法。例如：

- 您可以使用 KMS 來保護裝置節點，也可以使用SANtricity System Manager 中的磁碟機安全功能對同一裝置中自加密磁碟機上的資料進行「雙重加密」。
- 您可以使用 KMS 來保護裝置節點上的數據，也可以使用儲存物件加密選項在提取所有物件時進行加密。

如果只有一小部分物件需要加密，請考慮在儲存桶或單一物件層級控制加密。啟用多層加密會產生額外的效能成本。

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。

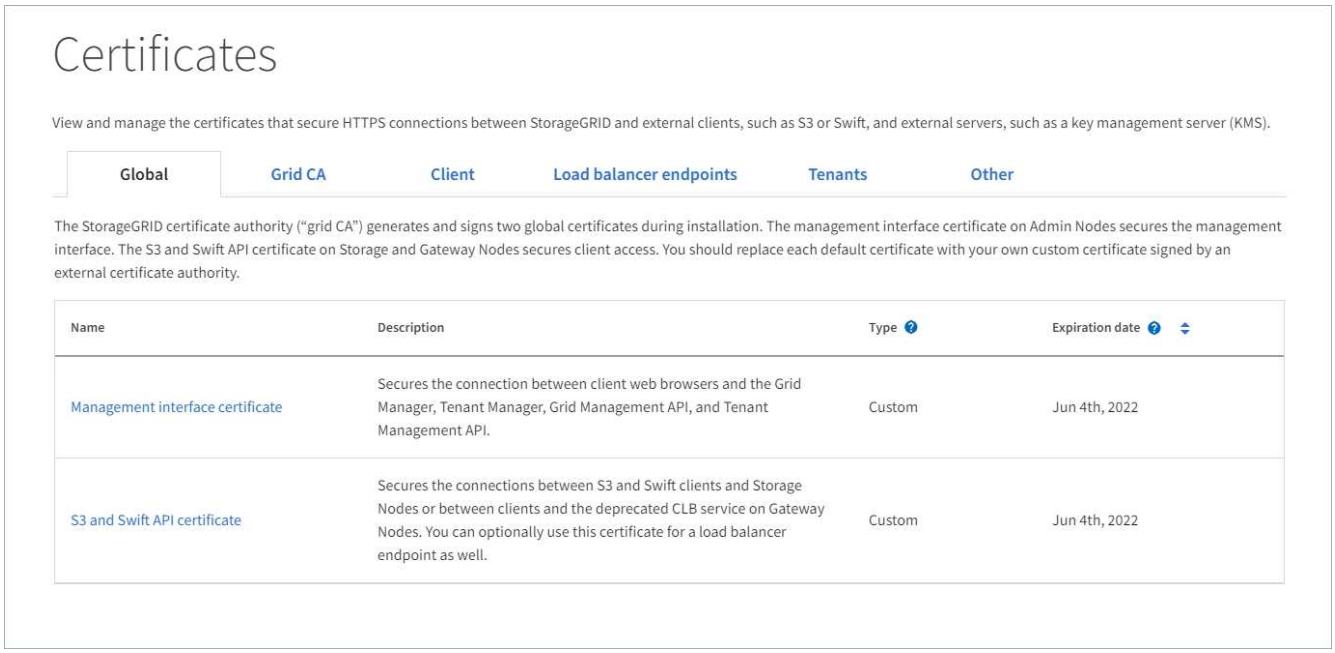
伺服器和客戶端憑證類型的變體以多種方式實現。在配置系統之前，您應該準備好特定StorageGRID配置所需的所有憑證。

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。

配置安全設定

管理 **TLS** 和 **SSH** 策略

TLS 和 SSH 原則決定使用哪些協定和密碼與用戶端應用程式建立安全的 TLS 連線以及與內部StorageGRID服務建立安全的 SSH 連線。

安全性策略控制 TLS 和 SSH 如何加密傳輸中的資料。一般來說，使用現代相容性（預設）策略，除非您的系統需要符合通用標準或您需要使用其他密碼。

> 某些StorageGRID服務尚未更新以使用這些原則中的密碼。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

選擇安全策略

步驟

1. 選擇*配置* > 安全 > 安全設定。

   *TLS 和 SSH 策略*標籤顯示可用的策略。目前有效的策略在策略圖塊上以綠色複選標記表示。

2. 查看圖塊以了解可用的策略。

政策	描述
現代相容性（預設）	如果您需要強加密並且除非您有特殊要求，請使用預設策略。此策略與大多數 TLS 和 SSH 用戶端相容。

政策	描述
舊版相容性	如果您需要為舊客戶端提供額外的相容性選項，請使用此原則。此策略中的附加選項可能會使其安全性低於現代相容性策略。
通用標準	如果您需要通用標準認證，請使用此政策。
FIPS 嚴格	如果您需要通用標準認證並且需要使用NetApp加密安全模組 3.0.8 將外部用戶端連接到負載平衡器端點、租用戶管理器和網格管理器，請使用此原則。使用此策略可能會降低效能。 注意：選擇此策略後，所有節點都必須"以滾動方式重啟"啟動NetApp加密安全模組。使用*維護* > *滾動重新啟動*來啟動和監控重新啟動。
風俗	如果您需要套用自己的密碼，請建立自訂原則。

3. 要查看有關每個策略的密碼、協定和演算法的詳細信息，請選擇*查看詳細資訊*。
4. 若要變更目前策略，請選擇*使用策略*。

   政策圖塊上的「目前政策」旁邊會出現一個綠色複選標記。

建立自訂安全性策略

如果您需要套用自己的密碼，您可以建立自訂原則。

步驟

1. 從與您要建立的自訂策略最相似的策略的圖塊中，選擇「查看詳細資訊」。
2. 選擇*複製到剪貼簿*，然後選擇*取消*。

3. 從*自訂策略*圖塊中，選擇*配置和使用*。
4. 貼上您複製的 JSON 並進行所需的更改。

5. 選擇*使用策略*。

   自訂策略圖塊上的「目前策略」旁邊會出現一個綠色複選標記。

6. 或者，選擇「編輯配置」對新的自訂策略進行更多變更。

暫時恢復預設安全策略

如果您設定了自訂安全性策略，且設定的 TLS 策略與"設定伺服器憑證"。

您可以暫時恢復預設安全性策略。

步驟

1. 登入管理節點：
   a. 輸入以下命令： `ssh admin@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 `#`。

2. 運行以下命令：

   ```
   restore-default-cipher-configurations
   ```

3. 從 Web 瀏覽器存取相同管理節點上的網格管理器。
4. 請依照以下步驟操作選擇安全策略重新配置策略。

設定網路和物件安全

您可以設定網路和物件安全性來加密儲存的對象，阻止某些 S3 請求，或允許用戶端連接到儲存節點使用 HTTP 而不是 HTTPS。

儲存物件加密

儲存物件加密可以對透過 S3 提取的所有物件資料進行加密。預設情況下，儲存的物件未加密，但您可以選擇使用 AES-128 或 AES-256 加密演算法來加密物件。啟用該設定後，所有新攝取的物件都會被加密，但現有儲存的物件不會發生任何變更。如果停用加密，目前加密的物件仍保持加密，但新攝取的物件不會被加密。

儲存物件加密設定僅適用於尚未透過儲存桶級或物件層級加密進行加密的 S3 物件。

有關StorageGRID加密方法的更多詳細信息，請參閱"查看StorageGRID加密方法"。

防止客戶端修改

防止客戶端修改是一個系統範圍的設定。當選擇“防止客戶端修改”選項時，以下請求將被拒絕。

S3 REST API

- DeleteBucket 請求
- 任何修改現有物件的資料、使用者定義的元資料或 S3 物件標記的請求

為儲存節點連線啟用 **HTTP**

預設情況下，客戶端應用程式使用 HTTPS 網路協定與儲存節點建立任何直接連線。您可以選擇為這些連線啟用 HTTP，例如，在測試非生產網格時。

只有當 S3 用戶端需要直接與儲存節點建立 HTTP 連線時，才使用 HTTP 進行儲存節點連線。對於僅使用 HTTPS 連線的用戶端或連線到負載平衡器服務的用戶端，您不需要使用此選項（因為您可以"配置每個負載平衡器端點"使用 HTTP 或 HTTPS)。

看"摘要：客戶端連接的 IP 位址和連接埠"了解 S3 用戶端使用 HTTP 或 HTTPS 連接到儲存節點時使用哪些連接埠。

選擇選項

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您擁有 Root 存取權限。

步驟

1. 選擇*配置* > 安全 > 安全設定。
2. 選擇“網路和物件”標籤。
3. 對於儲存對象加密，如果您不想加密儲存對象，請使用 **None**（預設）設置，或選擇 **AES-128** 或 **AES-256** 來加密儲存對象。
4. 如果您想阻止 S3 用戶端發出特定請求，可以選擇「阻止客戶端修改」。

   如果您更改此設置，則大約需要一分鐘才能應用新設置。配置的值被緩存，以提高效能和擴展性。

5. 如果用戶端直接連接到儲存節點並且您想要使用 HTTP 連接，則可以選擇*為儲存節點連接啟用 HTTP*。

   為生產網格啟用 HTTP 時要小心，因為請求將以未加密的形式傳送。

6. 選擇*儲存*。

更改介面安全設定

透過介面安全性設置，您可以控制當使用者處於非活動狀態的時間超過指定時間時是否將其註銷，以及是否在 API 錯誤回應中包含堆疊追蹤。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

關於此任務

*安全設定*頁麵包括*瀏覽器不活動逾時*和*管理 API 堆疊追蹤*設定。

瀏覽器不活動逾時

指示使用者登出之前瀏覽器可以處於非活動狀態的時間。預設值為 15 分鐘。

瀏覽器不活動逾時也受以下因素控制：

- 一個單獨的、不可設定的StorageGRID計時器，用於系統安全。每個使用者的身份驗證令牌在使用者登入 16 小時後過期。當使用者的身份驗證過期時，該使用者將自動登出，即使瀏覽器不活動逾時已停用或尚未達到瀏覽器逾時值。若要更新令牌，使用者必須重新登入。
- 身分提供者的逾時設置，假設為StorageGRID啟用了單一登入 (SSO)。

  如果啟用了 SSO 並且使用者的瀏覽器逾時，則使用者必須重新輸入其 SSO 憑證才能再次存取StorageGRID 。看"配置單一登入" 。

管理 **API** 堆疊追蹤

控制是否在網格管理器和租用戶管理器 API 錯誤回應中傳回堆疊追蹤。

預設此選項是停用的，但您可能希望為測試環境啟用此功能。一般來說，您應該在生產環境中停用堆疊追蹤，以避免在發生 API 錯誤時洩露內部軟體詳細資訊。

步驟

1. 選擇*配置* > 安全 > 安全設定。
2. 選擇“介面”選項卡。
3. 若要更改瀏覽器不活動逾時設定：
   a. 展開手風琴。
   b. 若要變更逾時期限，請指定 60 秒到 7 天之間的值。預設超時時間為 15 分鐘。
   c. 若要停用此功能，請取消選取該複選框。
   d. 選擇*儲存*。

      新設定不會影響目前已登入的使用者。使用者必須重新登入或刷新瀏覽器才能使新的逾時設定生效。
4. 若要變更管理 API 堆疊追蹤的設定：
   a. 展開手風琴。
   b. 選取該複選框以在網格管理器和租用戶管理器 API 錯誤回應中傳回堆疊追蹤。

      在生產環境中停用堆疊追蹤，以避免在發生 API 錯誤時洩露內部軟體詳細資訊。
   c. 選擇*儲存*。

配置金鑰管理伺服器

什麼是金鑰管理伺服器 (KMS)？

金鑰管理伺服器 (KMS) 是一個外部第三方系統，它使用金鑰管理互通性協定 (KMIP) 向相關StorageGRID站點上的StorageGRID設備節點提供加密金鑰。

StorageGRID僅支援某些金鑰管理伺服器。要取得受支援的產品和版本的列表，請使用 "NetApp互通性矩陣工具 (IMT)"。

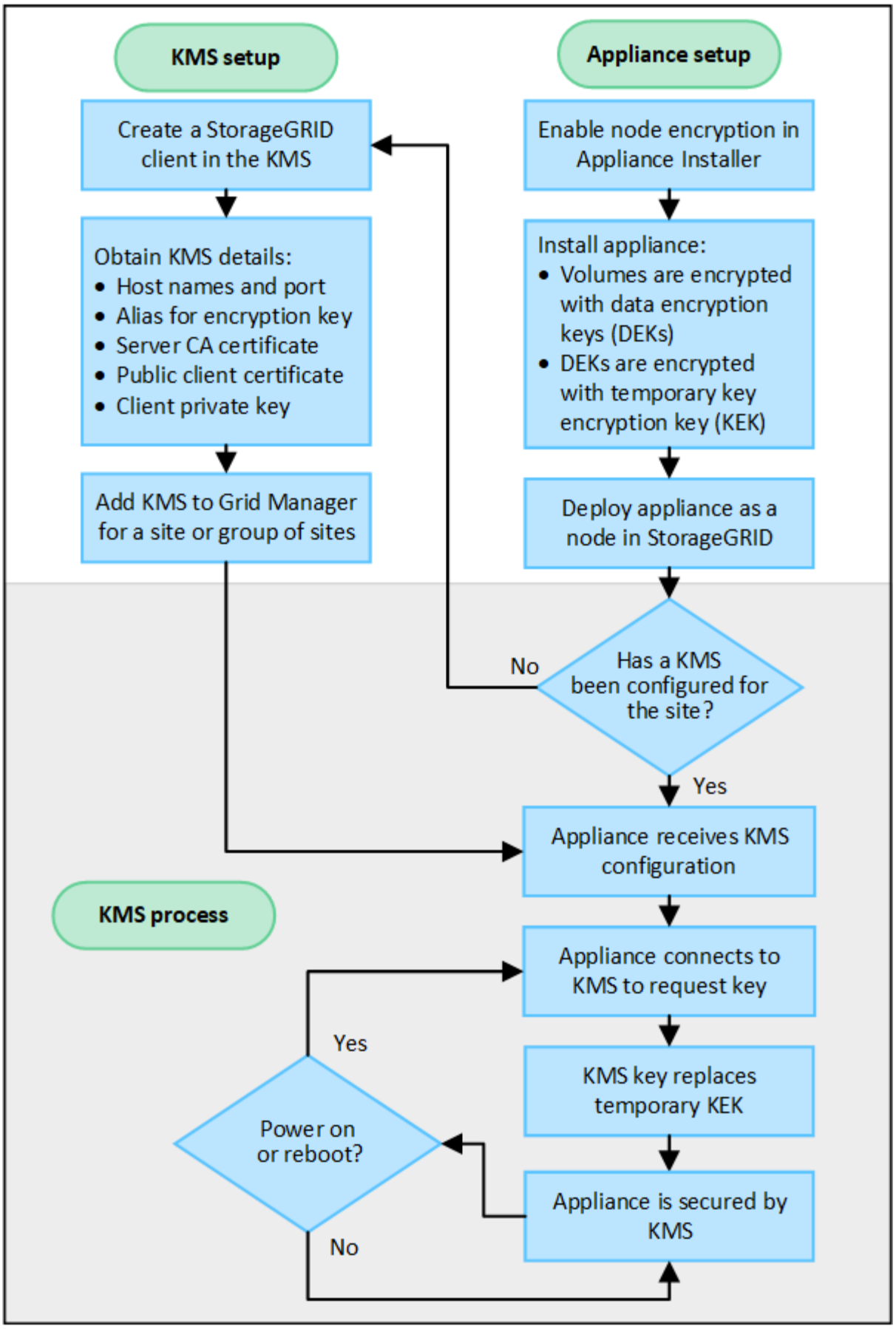
您可以使用一個或多個金鑰管理伺服器來管理在安裝期間啟用了「節點加密」設定的任何StorageGRID裝置節點的節點加密金鑰。透過將這些設備節點與金鑰管理伺服器結合使用，即使設備從資料中心移除，您也可以保護資料。裝置磁碟區加密後，除非節點可以與 KMS 通信，否則您無法存取裝置上的任何資料。

> StorageGRID不會建立或管理用於加密和解密裝置節點的外部金鑰。如果您打算使用外部金鑰管理伺服器來保護StorageGRID數據，則必須了解如何設定該伺服器，並且必須了解如何管理加密金鑰。執行金鑰管理任務超出了這些說明的範圍。如果您需要協助，請參閱金鑰管理伺服器的文件或聯絡技術支援。

KMS 和設備配置

在使用金鑰管理伺服器 (KMS) 保護裝置節點上的StorageGRID資料之前，您必須完成兩個設定任務：設定一個或多個 KMS 伺服器並為裝置節點啟用節點加密。當這兩個設定任務完成後，金鑰管理過程將會自動發生。

此流程圖顯示了使用 KMS 保護設備節點上的StorageGRID資料的進階步驟。



流程圖顯示 KMS 設定和裝置設定並行進行；但是，您可以根據需要在為新裝置節點啟用節點加密之前或之後設

定金鑰管理伺服器。

設定金鑰管理伺服器（**KMS**）

設定密鑰管理伺服器包括以下進階步驟。

步	參考
存取 KMS 軟體並為每個 KMS 或 KMS 叢集新增StorageGRID的用戶端。	"在 KMS 中將StorageGRID配置為客戶端"
取得 KMS 上StorageGRID客戶端所需的資訊。	"在 KMS 中將StorageGRID配置為客戶端"
將 KMS 新增至網格管理器，將其指派給單一網站或預設網站群組，上傳所需的證書，然後儲存 KMS 配置。	"新增金鑰管理伺服器 (KMS)"

設定設備

設定用於 KMS 的設備節點包括以下進階步驟。

1. 在設備安裝的硬體配置階段，使用StorageGRID設備安裝程式為設備啟用 節點加密 設定。

   > 將裝置新增至電網後，您無法啟用*節點加密*設置，且無法對未啟用節點加密的裝置使用外部金鑰管理。

2. 運行StorageGRID設備安裝程式。在安裝過程中，會為每個裝置磁碟區指派一個隨機資料加密金鑰 (DEK)，如下所示：
   - DEK 用於加密每個磁碟區上的資料。這些金鑰是使用裝置作業系統中的 Linux 統一金鑰設定 (LUKS) 磁碟加密產生的，無法變更。
   - 每個單獨的 DEK 都由主金鑰加密金鑰 (KEK) 加密。初始 KEK 是一個臨時金鑰，用於加密 DEK，直到裝置可以連接到 KMS。
3. 將設備節點新增至StorageGRID。

看 "啟用節點加密"了解詳情。

密鑰管理加密過程（自動發生）

金鑰管理加密包括以下自動執行的進階步驟。

1. 當您將啟用了節點加密的裝置安裝到網格中時， StorageGRID會決定包含新節點的網站是否存在 KMS 設定。
   - 如果已經為網站配置了 KMS，設備將接收 KMS 配置。
   - 如果尚未為網站配置 KMS，裝置上的資料將繼續由臨時 KEK 加密，直到您為網站配置 KMS 並且裝置收到 KMS 設定為止。
2. 該裝置使用 KMS 設定連接到 KMS 並請求加密金鑰。
3. KMS 向裝置發送加密金鑰。 KMS 的新金鑰取代了臨時 KEK，現在用於加密和解密裝置磁碟區的 DEK。

加密裝置節點連接到配置的 KMS 之前存在的任何資料都使用臨時金鑰加密。但是，在臨時金鑰被 KMS 加密金鑰取代之前，裝置磁碟區不應被視為受到保護，不能從資料中心移除。

4. 如果裝置開啟或重新啟動，它會重新連線到 KMS 來請求金鑰。此密鑰保存在揮發性記憶體中，斷電或重新啟動後將無法恢復。

使用金鑰管理伺服器的注意事項和要求

在設定外部金鑰管理伺服器 (KMS) 之前，您必須了解注意事項和要求。

支援哪個版本的 **KMIP**？

StorageGRID支援 KMIP 版本 1.4。

"密鑰管理互通性協定規範版本 1.4"

網路考量有哪些？

網路防火牆設定必須允許每個設備節點透過用於金鑰管理互通協定 (KMIP) 通訊的連接埠進行通訊。預設 KMIP 連接埠為 5696。

您必須確保使用節點加密的每個裝置節點都具有對您為網站配置的 KMS 或 KMS 叢集的網路存取權限。

支援哪些版本的 **TLS**？

設備節點和配置的 KMS 之間的通訊使用安全的 TLS 連線。 StorageGRID在與 KMS 或 KMS 叢集建立 KMIP 連線時，可以支援 TLS 1.2 或 TLS 1.3 協議，具體取決於 KMS 支援的內容以及"TLS 和 SSH 策略"您正在使用。

StorageGRID在建立連線時與 KMS 協商協定和密碼（TLS 1.2）或密碼套件（TLS 1.3）。要查看可用的協定版本和密碼/密碼套件，請查看 `tlsOutbound`網格的活動 TLS 和 SSH 策略部分（配置 > 安全 安全設定）。

支援哪些設備？

您可以使用金鑰管理伺服器 (KMS) 來管理網格中啟用了 節點加密 設定的任何StorageGRID裝置的加密金鑰。此設定只能在使用StorageGRID Appliance Installer 的裝置安裝硬體設定階段啟用。

將裝置新增至電網後，您無法啟用節點加密，且無法對未啟用節點加密的裝置使用外部金鑰管理。

您可以將配置的 KMS 用於StorageGRID設備和設備節點。

您無法將配置的 KMS 用於基於軟體（非設備）的節點，包括以下內容：

- 部署為虛擬機器 (VM) 的節點
- 部署在 Linux 主機上的容器引擎內的節點

部署在這些其他平台上的節點可以在資料儲存或磁碟層級使用StorageGRID以外的加密。

我應該何時配置密鑰管理伺服器？

對於新安裝，您通常應該在建立租用戶之前在網格管理員中設定一個或多個金鑰管理伺服器。此順序確保在節點上儲存任何物件資料之前，節點受到保護。

您可以在安裝設備節點之前或之後在網格管理器中設定金鑰管理伺服器。

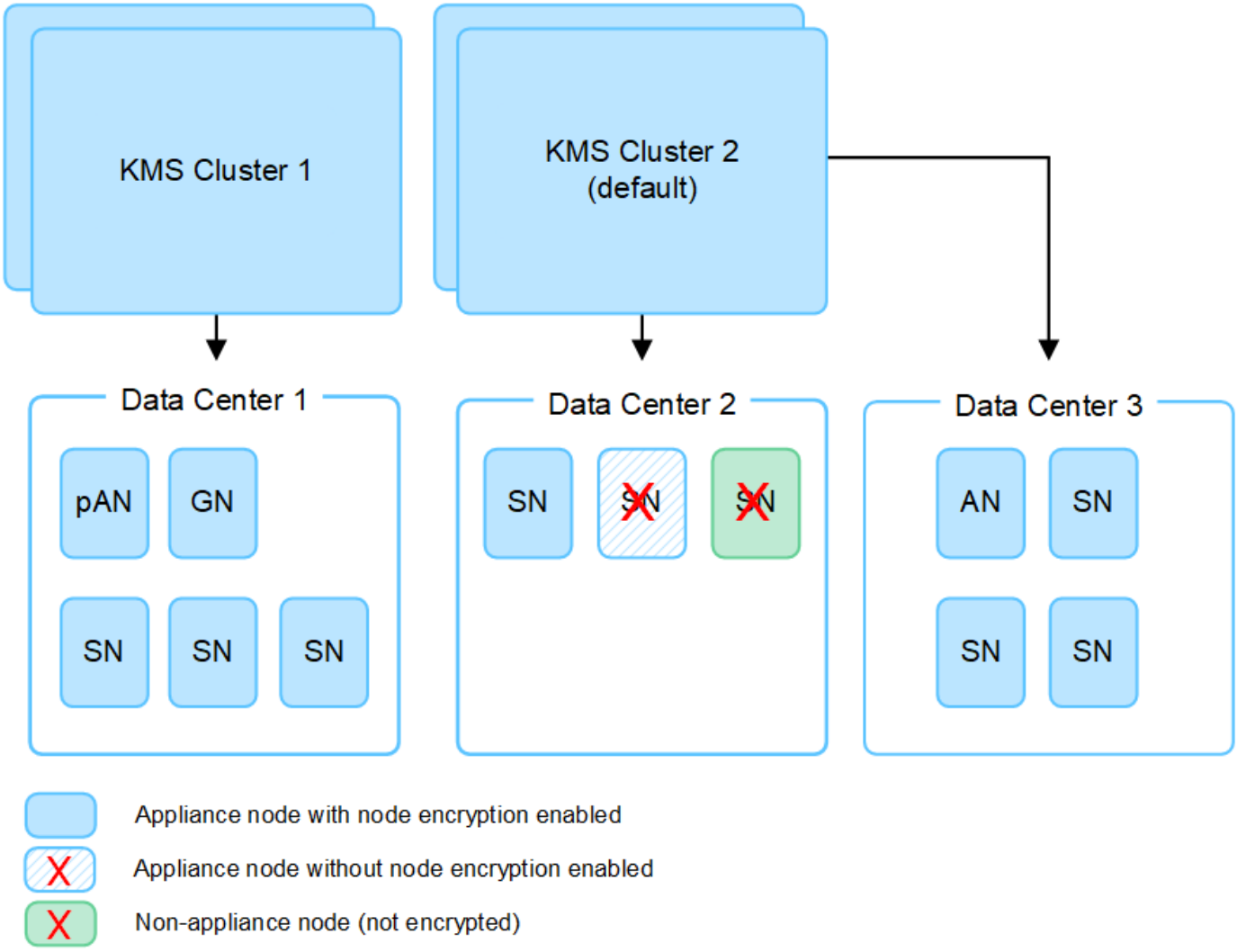
我需要多少個金鑰管理伺服器？

您可以設定一個或多個外部金鑰管理伺服器來為StorageGRID系統中的設備節點提供加密金鑰。每個 KMS 為單一站點或一組站點的StorageGRID設備節點提供單一加密金鑰。

StorageGRID支援使用 KMS 叢集。每個 KMS 叢集包含多個共用設定設定和加密金鑰的複製金鑰管理伺服器。建議使用 KMS 叢集進行金鑰管理，因為它可以提高高可用性配置的故障轉移能力。

例如，假設您的StorageGRID系統有三個資料中心站點。您可以設定 KMS 叢集來為資料中心 1 的所有裝置節點提供金鑰，並配置第二個 KMS 叢集來為所有其他網站的所有裝置節點提供金鑰。當您新增第二個 KMS 叢集時，您可以為資料中心 2 和資料中心 3 設定一個預設 KMS。

請注意，您不能將 KMS 用於非裝置節點或安裝期間未啟用 節點加密 設定的任何裝置節點。



當密鑰被旋轉時會發生什麼？

作為最佳安全做法，您應該定期"旋轉加密密鑰"由每個配置的 KMS 使用。

當新的密鑰版本可用時：

- 它會自動分發到與 KMS 關聯的網站上的加密設備節點。分發應在密鑰輪換後一小時內進行。
- 如果在分發新金鑰版本時加密裝置節點處於離線狀態，則該節點將在重新啟動後立即收到新金鑰。
- 如果因任何原因無法使用新金鑰版本加密裝置磁碟區，則會針對裝置節點觸發 **KMS** 加密金鑰輪替失敗 警報。您可能需要聯絡技術支援以取得協助來解決此警報。

設備節點加密後可以重複使用嗎？

如果需要將加密設備安裝到另一個StorageGRID系統中，則必須先停用網格節點才能將物件資料移至另一個節點。然後，您可以使用StorageGRID Appliance Installer "清除 KMS 配置" 。清除 KMS 設定將停用 節點加密 設定並刪除裝置節點與StorageGRID站點的 KMS 設定之間的關聯。

如果無法存取 KMS 加密金鑰，裝置上保留的任何資料將無法再訪問，並且會永久鎖定。

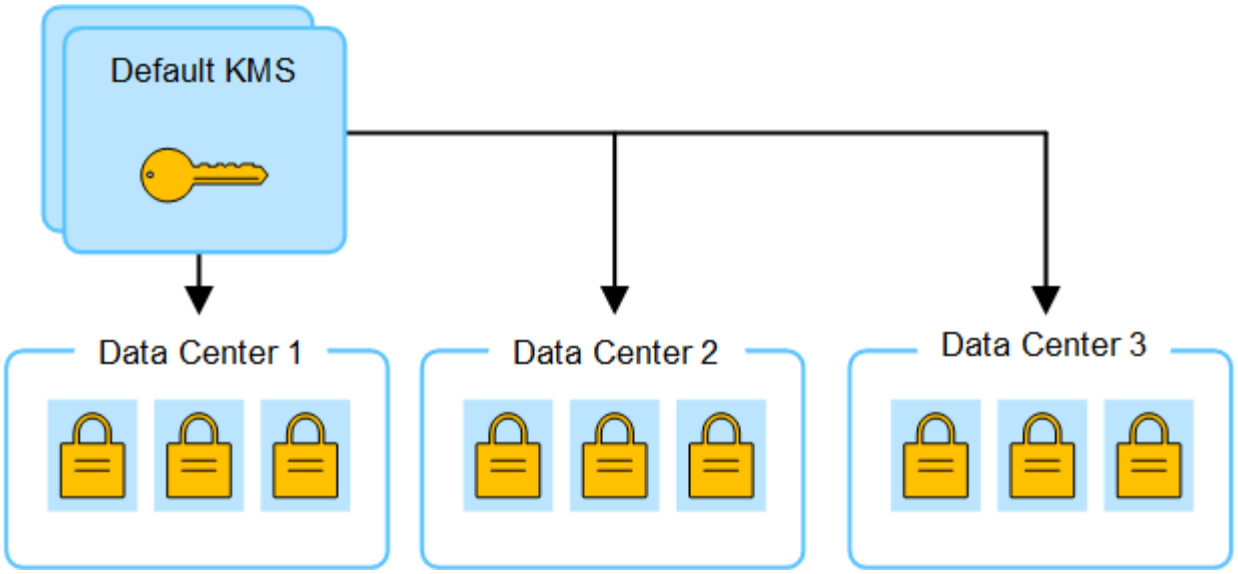
更改站點 **KMS** 的注意事項

每個金鑰管理伺服器 (KMS) 或 KMS 叢集會向單一網站或一組網站的所有裝置節點提供加密金鑰。如果您需要變更網站使用的 KMS，則可能需要將加密金鑰從一個 KMS 複製到另一個 KMS。

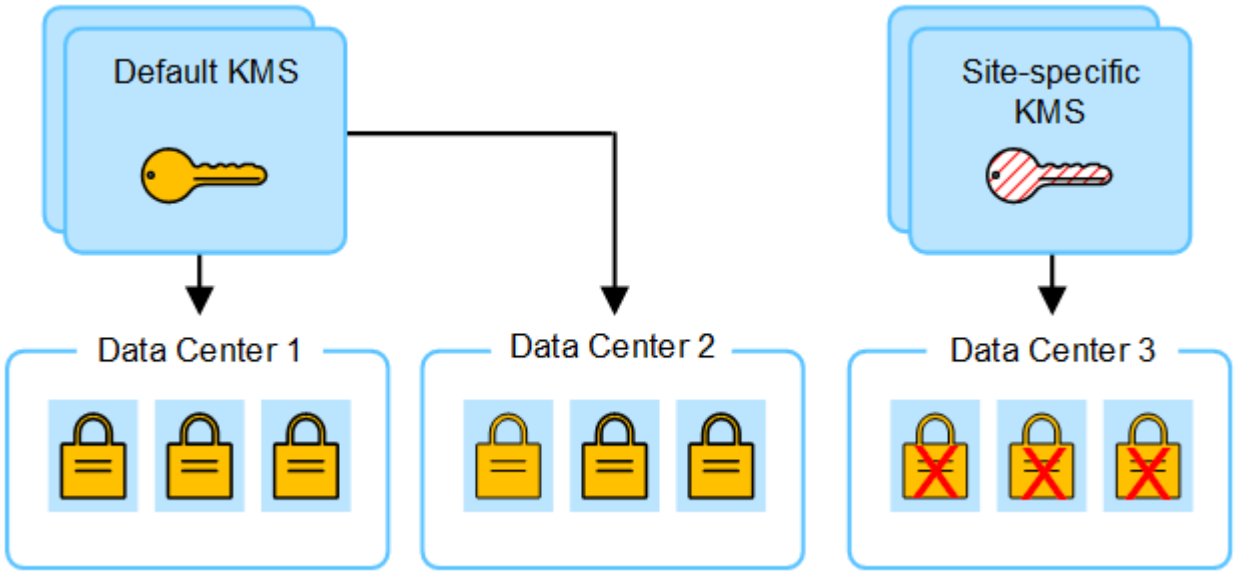
如果您變更網站所使用的 KMS，則必須確保該網站上先前加密的裝置節點可以使用儲存在新 KMS 上的金鑰解密。在某些情況下，您可能需要將目前版本的加密金鑰從原始 KMS 複製到新的 KMS。您必須確保 KMS 具有正確的金鑰來解密網站上的加密裝置節點。

例如：

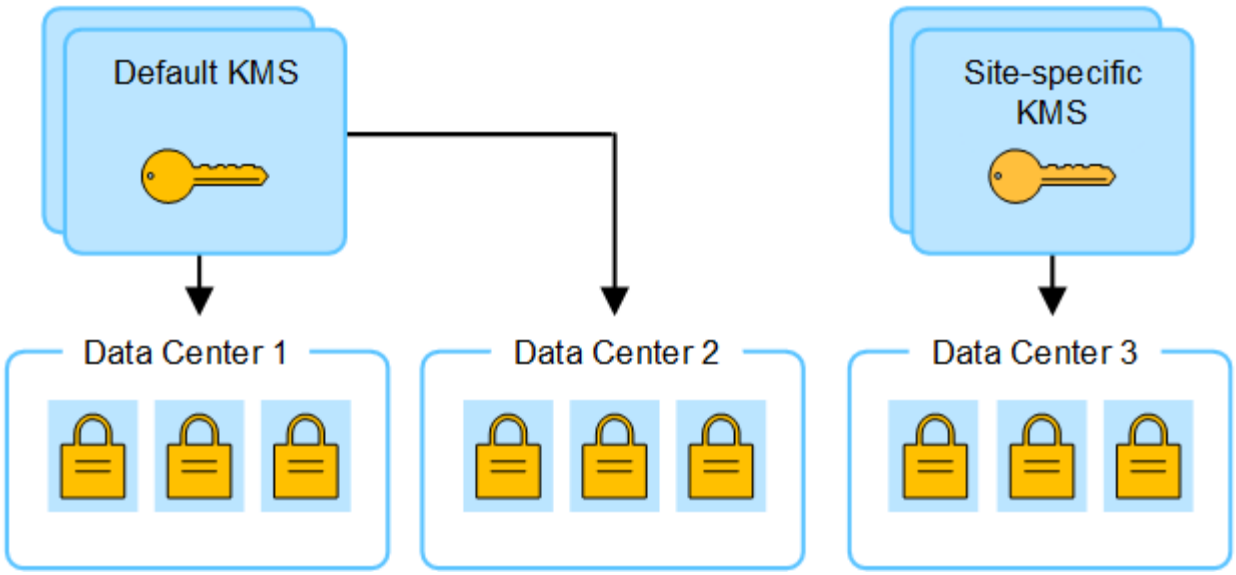
1. 您最初配置一個適用於所有沒有專用 KMS 的網站的預設 KMS。
2. 儲存 KMS 後，所有啟用了 節點加密 設定的裝置節點都會連接到 KMS 並要求加密金鑰。此金鑰用於加密所有網站的設備節點。也必須使用相同的金鑰來解密這些裝置。



3. 您決定為一個站點（圖中的資料中心 3）新增特定於站點的 KMS。但是，由於裝置節點已加密，因此當您嘗試儲存網站特定 KMS 的設定時會發生驗證錯誤。發生該錯誤的原因是網站特定的 KMS 沒有正確的金鑰來解密該網站的節點。



4. 為了解決這個問題，您可以將目前版本的加密金鑰從預設 KMS 複製到新的 KMS。 （從技術上講，您將原始金鑰複製到具有相同別名的新金鑰。原始密鑰將成為新密鑰的先前版本。）網站特定的 KMS 現在具有解密資料中心 3 的裝置節點的正確金鑰，因此可以將其保存在StorageGRID中。



更改網站所用 **KMS** 的用例

該表總結了更改站點 KMS 的最常見情況所需的步驟。

更改網站 **KMS** 的用例	必要步驟
您有一個或多個特定於網站的 KMS 條目，並且想要使用其中一個作為預設 KMS。	編輯特定於站點的 KMS。在「管理金鑰」欄位中，選擇「未由其他 KMS 管理的網站（預設為 KMS）」。站點特定的 KMS 現在將用作預設 KMS。它將適用於任何沒有專用 KMS 的網站。 "編輯金鑰管理伺服器 (KMS)"
您有一個預設的 KMS，並且在擴充功能中新增了一個新網站。您不想對新網站使用預設的 KMS。	1. 如果新網站的裝置節點已由預設 KMS 加密，請使用 KMS 軟體將目前版本的加密金鑰從預設 KMS 複製到新的 KMS。 2. 使用網格管理器新增新的 KMS 並選擇網站。 "新增金鑰管理伺服器 (KMS)"
您希望網站的 KMS 使用不同的伺服器。	1. 如果網站上的裝置節點已被現有 KMS 加密，請使用 KMS 軟體將目前版本的加密金鑰從現有 KMS 複製到新的 KMS。 2. 使用網格管理器，編輯現有的 KMS 設定並輸入新的主機名稱或 IP 位址。 "新增金鑰管理伺服器 (KMS)"

在 **KMS** 中將**StorageGRID**配置為客戶端

您必須先將StorageGRID配置為每個外部金鑰管理伺服器或 KMS 叢集的用戶端，然後才能將 KMS 新增至StorageGRID。

這些說明適用於 Thales CipherTrust Manager 和 Hashicorp Vault。要取得受支援的產品和版本的列表，請使用 "NetApp互通性矩陣工具 (IMT)"。

步驟

1. 從 KMS 軟體中，為您計劃使用的每個 KMS 或 KMS 叢集建立一個StorageGRID用戶端。

   每個 KMS 管理單一站點或一組站點的StorageGRID設備節點的單一加密金鑰。

2. 使用以下兩種方法之一建立金鑰：
   - 使用您的 KMS 產品的金鑰管理頁面。為每個 KMS 或 KMS 叢集建立一個 AES 加密金鑰。

     加密金鑰必須為 2,048 位元或更多，且必須可匯出。

   - 讓StorageGRID建立金鑰。測試並儲存後會提示你"上傳客戶端證書"。
3. 記錄每個 KMS 或 KMS 群集的以下資訊。

   將 KMS 新增至StorageGRID時需要此資訊：

   - 每個伺服器的主機名稱或 IP 位址。
   - KMS 使用的 KMIP 連接埠。
   - KMS 中加密金鑰的金鑰別名。
4. 對於每個 KMS 或 KMS 集群，取得由憑證授權單位 (CA) 簽署的伺服器憑證或包含每個 PEM 編碼的 CA 憑證檔案的憑證包，按憑證連結順序連接。

   伺服器憑證允許外部 KMS 向StorageGRID進行身份驗證。

   - 憑證必須使用隱私增強郵件 (PEM) Base-64 編碼的 X.509 格式。
   - 每個伺服器憑證中的主題備用名稱 (SAN) 欄位必須包含StorageGRID將連接到的完全限定網域名稱 (FQDN) 或 IP 位址。

     在StorageGRID中設定 KMS 時，必須在 **Hostname** 欄位中輸入相同的 FQDN 或 IP 位址。

   - 伺服器憑證必須與 KMS 的 KMIP 介面使用的憑證匹配，後者通常使用連接埠 5696。
5. 取得外部 KMS 頒發給StorageGRID 的公共用戶端憑證以及用戶端憑證的私密金鑰。

   用戶端憑證允許StorageGRID向 KMS 驗證自身身分。

新增金鑰管理伺服器 (KMS)

您可以使用StorageGRID金鑰管理伺服器精靈新增每個 KMS 或 KMS 叢集。

開始之前

- 您已審閱"使用金鑰管理伺服器的注意事項和要求"。
- 你有"在 KMS 中將StorageGRID配置為客戶端"，並且您擁有每個 KMS 或 KMS 叢集所需的資訊。

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

關於此任務

如果可能，請在配置適用於所有未由其他 KMS 管理的網站的預設 KMS 之前配置任何特定於網站的金鑰管理伺服器。如果您先建立預設 KMS，則網格中的所有節點加密裝置都將由預設 KMS 加密。如果您以後想要建立特定於網站的 KMS，則必須先將目前版本的加密金鑰從預設 KMS 複製到新的 KMS。看"更改站點 KMS 的注意事項"了解詳情。

步驟 **1**：**KMS** 詳細信息

在新增金鑰管理伺服器精靈的步驟 1（KMS 詳細資料）中，您需要提供有關 KMS 或 KMS 叢集的詳細資訊。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。

   出現密鑰管理伺服器頁面，其中已選取配置詳細資訊標籤。

2. 選擇“創建”。

   出現新增金鑰管理伺服器精靈的第 1 步（KMS 詳細資訊）。

3. 為 KMS 和在該 KMS 中配置的StorageGRID用戶端輸入以下資訊。

場地	描述
KMS 名稱	協助您識別此 KMS 的描述性名稱。必須介於 1 到 64 個字元之間。
鍵名稱	KMS 中StorageGRID客戶端的精確金鑰別名。必須介於 1 到 255 個字元之間。 注意：如果您尚未使用 KMS 產品建立金鑰，系統將提示您讓StorageGRID建立金鑰。
管理密鑰	將與此 KMS 關聯的StorageGRID站點。如果可能，您應該在配置適用於所有未由其他 KMS 管理的網站的預設 KMS 之前配置任何特定於網站的金鑰管理伺服器。 • 如果此 KMS 將管理特定站點的裝置節點的加密金鑰，請選擇一個站點。 • 選擇*未由其他 KMS 管理的網站（預設 KMS）*來配置一個預設 KMS，該預設 KMS 將套用於任何沒有專用 KMS 的網站以及您在後續擴充中新增的任何網站。 *注意：*如果您選擇先前由預設 KMS 加密的網站但未向新 KMS 提供目前版本的原始加密金鑰，則在儲存 KMS 設定時將發生驗證錯誤。

場地	描述
港口	KMS 伺服器用於金鑰管理互通協定 (KMIP) 通訊的連接埠。預設為 5696，這是 KMIP 標準連接埠。
主機名稱	KMS 的完全限定網域名稱或 IP 位址。 *注意：*伺服器憑證的主題備用名稱 (SAN) 欄位必須包含您在此輸入的 FQDN 或 IP 位址。否則， StorageGRID將無法連接到 KMS 或 KMS 叢集中的所有伺服器。

4. 如果您正在配置 KMS 集群，請選擇「新增另一個主機名稱」為集群中的每個伺服器新增一個主機名稱。
5. 選擇*繼續*。

步驟**2**：上傳伺服器憑證

在新增金鑰管理伺服器精靈的第 2 步（上傳伺服器憑證）中，您可以上傳 KMS 的伺服器憑證（或憑證包）。伺服器憑證允許外部 KMS 向StorageGRID進行身份驗證。

步驟

1. 從*步驟 2（上傳伺服器憑證）*開始，瀏覽到已儲存的伺服器憑證或憑證包的位置。
2. 上傳證書檔案。

   出現伺服器憑證元資料。

   如果您上傳了憑證包，則每個憑證的元資料都會顯示在自己的標籤上。

3. 選擇*繼續*。

步驟 **3**：上傳客戶端憑證

在新增金鑰管理伺服器精靈的步驟 3（上傳用戶端憑證）中，上傳用戶端憑證和用戶端憑證私鑰。用戶端憑證允許StorageGRID向 KMS 驗證自身身分。

步驟

1. 從*步驟 3（上傳客戶端憑證）*開始，瀏覽到客戶端憑證的位置。
2. 上傳客戶端證書檔案。

   出現客戶端證書元資料。

3. 瀏覽到客戶端憑證的私鑰的位置。
4. 上傳私鑰檔案。
5. 選擇*測試並儲存*。

   如果金鑰不存在，系統會提示您讓StorageGRID建立一個。

   測試金鑰管理伺服器和設備節點之間的連線。如果所有連線均有效，並且在 KMS 上找到了正確的金鑰，則

新的金鑰管理伺服器將會新增至金鑰管理伺服器頁面的表中。

新增 KMS 後，金鑰管理伺服器頁面上的憑證狀態立即顯示為未知。 StorageGRID可能需要長達 30 分鐘才能取得每個憑證的實際狀態。您必須刷新 Web 瀏覽器才能查看目前狀態。

6. 如果在選擇“測試並儲存”時出現錯誤訊息，請查看訊息詳細信息，然後選擇“確定”。

   例如，如果連線測試失敗，您可能會收到 422：無法處理的實體錯誤。

7. 如果需要儲存目前配置而不測試外部連接，請選擇*強制儲存*。

   選擇「強制儲存」將儲存 KMS 配置，但不會測試從每個裝置到該 KMS 的外部連線。如果設定有問題，您可能無法重新啟動在受影響網站上啟用了節點加密的裝置節點。在問題解決之前，您可能會無法存取您的資料。

8. 查看確認警告，如果確定要強制儲存配置，請選擇「確定」。

   KMS 配置已儲存，但未測試與 KMS 的連線。

管理 KMS

管理金鑰管理伺服器 (KMS) 包括查看或編輯詳細資訊、管理憑證、查看加密節點以及在不再需要時刪除 KMS。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"所需的存取權限"。

查看 KMS 詳細信息

您可以查看有關StorageGRID系統中每個金鑰管理伺服器 (KMS) 的信息，包括金鑰詳細資訊以及伺服器和用戶端憑證的目前狀態。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。

   出現密鑰管理伺服器頁面並顯示以下資訊：

   - 配置詳細資訊標籤列出了已設定的所有金鑰管理伺服器。
   - 加密節點標籤列出了所有啟用了節點加密的節點。

2. 若要查看特定 KMS 的詳細資訊並對該 KMS 執行操作，請選擇該 KMS 的名稱。 KMS 的詳細資訊頁面列出了以下資訊：

場地	描述
管理密鑰	與 KMS 關聯的StorageGRID站點。 此欄位顯示特定StorageGRID站點或*未由其他 KMS 管理的站點（預設 KMS）*的名稱。
主機名稱	KMS 的完全限定網域名稱或 IP 位址。 如果有兩個金鑰管理伺服器的集群，則會列出兩個伺服器的完全限定網域名稱或 IP 位址。如果叢集中有兩個以上的金鑰管理伺服器，則會列出第一個 KMS 的完全限定網域名稱或 IP 位址以及叢集中其他金鑰管理伺服器的數量。 例如： `10.10.10.10 and 10.10.10.11`或者 `10.10.10.10 and 2 others`。 若要查看叢集中的所有主機名，請選擇 KMS 並選擇 編輯 或 操作 > 編輯。

3. 選擇 KMS 詳細資料頁面上的標籤以查看以下資訊：

Tab	場地	描述
關鍵細節	鍵名稱	KMS 中StorageGRID客戶端的金鑰別名。
密鑰 UID	密鑰最新版本的唯一識別碼。	上次修改時間
密鑰最新版本的日期和時間。	伺服器憑證	元數據
證書的元數據，例如序號、到期日和時間以及證書 PEM。	證書 PEM	證書的 PEM（隱私增強郵件）文件的內容。
客戶端憑證	元數據	證書的元數據，例如序號、到期日和時間以及證書 PEM。

4. 根據組織的安全實務要求，選擇*輪替金鑰*，或使用 KMS 軟體來建立金鑰的新版本。

當密鑰輪換成功時，密鑰 UID 和上次修改欄位將被更新。

如果您使用 KMS 軟體輪替加密金鑰，請將其從金鑰的最後使用的版本輪替為相同金鑰的新版本。不要旋轉到完全不同的鍵。

切勿嘗試透過更改 KMS 的金鑰名稱（別名）來輪換密鑰。 StorageGRID要求所有先前使用的金鑰版本（以及任何未來的版本）都可以使用相同的金鑰別名從 KMS 存取。如果您變更已設定的 KMS 的金鑰別名， StorageGRID可能無法解密您的資料。

管理證書

及時解決任何伺服器或客戶端證書問題。如果可能，請在證書過期之前更換證書。

您必須盡快解決任何憑證問題以維持資料存取。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。
2. 在表格中，查看每個 KMS 的憑證到期值。
3. 如果任何 KMS 的憑證到期日期未知，請等待最多 30 分鐘，然後重新整理您的 Web 瀏覽器。
4. 如果憑證過期列指示憑證已過期或即將過期，請選擇 KMS 前往 KMS 詳細資料頁面。
   a. 選擇*伺服器憑證*並驗證「到期日」欄位的值。
   b. 若要取代證書，請選擇*編輯證書*上傳新證書。
   c. 重複這些子步驟並選擇*客戶端憑證*而不是伺服器憑證。
5. 當觸發*KMS CA 憑證過期*、*KMS 用戶端憑證過期*和*KMS 伺服器憑證過期*警報時，請注意每個警報的描述並執行建議的操作。

   StorageGRID可能需要長達 30 分鐘才能取得憑證過期更新。刷新您的網頁瀏覽器以查看當前值。

如果您獲得的狀態為*伺服器憑證狀態未知*，請確保您的 KMS 允許取得伺服器憑證而無需用戶端憑證。

查看加密節點

您可以查看有關StorageGRID系統中啟用了 節點加密 設定的裝置節點的資訊。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。

   出現密鑰管理伺服器頁面。配置詳細資訊標籤顯示已設定的任何金鑰管理伺服器。

2. 從頁面頂部，選擇“加密節點”標籤。

   「加密節點」標籤列出了StorageGRID系統中啟用了「節點加密」設定的裝置節點。

3. 查看表中每個設備節點的資訊。

柱子	描述
節點名稱	設備節點的名稱。
節點類型	節點類型：儲存、管理或網關。
地點	安裝節點的StorageGRID站點的名稱。

柱子	描述
KMS 名稱	用於節點的 KMS 的描述性名稱。 如果沒有列出 KMS，請選擇設定詳細資料標籤以新增 KMS。 "新增金鑰管理伺服器 (KMS)"
密鑰 UID	用於加密和解密裝置節點上資料的加密金鑰的唯一 ID。若要查看整個密鑰 UID，請選擇文字。 破折號 (--) 表示金鑰 UID 未知，可能是由於裝置節點和 KMS 之間的連線問題。
地位	KMS 與裝置節點之間的連線狀態。如果節點已連接，則時間戳記每 30 分鐘更新一次。 KMS 配置變更後，連線狀態可能需要幾分鐘才能更新。 *注意：*刷新您的網頁瀏覽器以查看新值。

4. 如果狀態列指示 KMS 問題，請立即解決該問題。

   在正常的 KMS 操作期間，狀態將為 已連接到 **KMS**。如果節點與電網斷開連接，則會顯示節點連接狀態（管理關閉或未知）。

   其他狀態訊息對應於具有相同名稱的StorageGRID警報：

   - KMS 配置載入失敗
   - KMS 連線錯誤
   - 未找到 KMS 加密金鑰名稱
   - KMS 加密金鑰輪換失敗
   - KMS 金鑰解密裝置磁碟區失敗
   - 未配置 KMS

   針對這些警報執行建議的操作。

   您必須立即解決任何問題，以確保您的資料受到充分保護。

編輯 **KMS**

例如，如果憑證即將過期，您可能需要編輯金鑰管理伺服器的設定。

開始之前

- 如果您計劃更新為 KMS 選擇的站點，則您已查看"更改站點 KMS 的注意事項"。
- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。

   出現金鑰管理伺服器頁面，其中顯示所有已設定的金鑰管理伺服器。

2. 選擇要編輯的 KMS，然後選擇*操作* > 編輯。

   您也可以透過選擇表格中的 KMS 名稱並在 KMS 詳細資料頁面上選擇 編輯 來編輯 KMS。

3. 或者，更新編輯金鑰管理伺服器精靈的*步驟 1（KMS 詳細資料）*中的詳細資訊。

場地	描述
KMS 名稱	協助您識別此 KMS 的描述性名稱。必須介於 1 到 64 個字元之間。
鍵名稱	KMS 中StorageGRID客戶端的精確金鑰別名。必須介於 1 到 255 個字元之間。 您只需在極少數情況下編輯密鑰名稱。例如，如果別名在 KMS 中被重新命名，或者先前密鑰的所有版本都已複製到新別名的版本歷史記錄中，則必須編輯密鑰名稱。
管理密鑰	如果您正在編輯特定於網站的 KMS，並且還沒有預設 KMS，則可以選擇 未由其他 **KMS** 管理的網站（預設 **KMS**）。此選擇將網站特定的 KMS 轉換為預設 KMS，這將適用於所有沒有專用 KMS 的網站以及擴充功能中新增的任何網站。 *注意：*如果您正在編輯特定於網站的 KMS，則不能選擇其他網站。如果您正在編輯預設 KMS，則無法選擇特定網站。
港口	KMS 伺服器用於金鑰管理互通協定 (KMIP) 通訊的連接埠。預設為 5696，這是 KMIP 標準連接埠。
主機名稱	KMS 的完全限定網域名稱或 IP 位址。 *注意：*伺服器憑證的主題備用名稱 (SAN) 欄位必須包含您在此輸入的 FQDN 或 IP 位址。否則， StorageGRID將無法連接到 KMS 或 KMS 叢集中的所有伺服器。

4. 如果您正在配置 KMS 集群，請選擇「新增另一個主機名稱」為集群中的每個伺服器新增一個主機名稱。
5. 選擇*繼續*。

   出現編輯金鑰管理伺服器精靈的第 2 步（上傳伺服器憑證）。

6. 如果需要更換伺服器證書，請選擇*瀏覽*並上傳新檔案。
7. 選擇*繼續*。

   出現編輯金鑰管理伺服器精靈的步驟 3（上傳用戶端憑證）。

8. 如果需要更換用戶端憑證和用戶端憑證私鑰，請選擇*瀏覽*並上傳新檔案。
9. 選擇*測試並儲存*。

測試金鑰管理伺服器和受影響網站的所有節點加密設備節點之間的連線。如果所有節點連接均有效，並且在 KMS 上找到了正確的金鑰，則金鑰管理伺服器將新增至金鑰管理伺服器頁面的表中。

10. 如果出現錯誤訊息，請查看訊息詳細訊息，然後選擇「確定」。

    例如，如果您為此 KMS 選擇的網站已由另一個 KMS 管理，或連線測試失敗，您可能會收到 422：無法處理的實體錯誤。

11. 如果您需要在解決連線錯誤之前儲存目前配置，請選擇*強制儲存*。

    > 選擇「強制儲存」將儲存 KMS 配置，但不會測試從每個裝置到該 KMS 的外部連線。如果設定有問題，您可能無法重新啟動在受影響網站上啟用了節點加密的裝置節點。在問題解決之前，您可能會無法存取您的資料。

    KMS 配置已儲存。

12. 查看確認警告，如果確定要強制儲存配置，請選擇「確定」。

    KMS 配置已儲存，但未測試與 KMS 的連線。

刪除金鑰管理伺服器 (KMS)

在某些情況下，您可能想要刪除金鑰管理伺服器。例如，如果您已退役該站點，則可能想要刪除特定於站點的 KMS。

開始之前

- 您已審閱"使用金鑰管理伺服器的注意事項和要求"。
- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

關於此任務

您可以在以下情況下刪除 KMS：

- 如果網站已退役或網站不包含啟用了節點加密的裝置節點，則可以刪除網站特定的 KMS。
- 如果每個啟用了節點加密的裝置節點的網站都已存在網站特定的 KMS，則可以刪除預設 KMS。

步驟

1. 選擇 設定 > 安全 > 金鑰管理伺服器。

   出現金鑰管理伺服器頁面，其中顯示所有已設定的金鑰管理伺服器。

2. 選擇要刪除的 KMS，然後選擇*操作* > 刪除。

   您也可以透過選擇表格中的 KMS 名稱並從 KMS 詳細資料頁面中選擇 刪除 來刪除 KMS。

3. 確認以下內容屬實：
   - 您正在刪除沒有啟用節點加密的裝置節點的網站特定 KMS。
   - 您正在刪除預設的 KMS，但每個具有節點加密的網站已經存在網站特定的 KMS。

4. 選擇“是”。

   KMS 配置已被刪除。

管理代理設定

配置儲存代理

如果您正在使用平台服務或雲端儲存池，則可以在儲存節點和外部 S3 端點之間設定非透明代理。例如，您可能需要一個非透明代理來允許將平台服務訊息傳送到外部端點，例如網路上的端點。

> 配置的儲存代理設定不適用於 Kafka 平台服務端點。

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

您可以配置單一儲存代理程式的設定。

步驟

1. 選擇*配置* > 安全 > 代理設定。
2. 在「儲存」標籤上，選取「啟用儲存代理程式」複選框。
3. 選擇儲存代理的協定。
4. 輸入代理伺服器的主機名稱或 IP 位址。
5. 或者，輸入用於連接代理伺服器的連接埠。

   將此欄位留空以使用協定的預設連接埠：HTTP 為 80，SOCKS5 為 1080。

6. 選擇*儲存*。

   儲存儲存代理程式後，可以設定和測試平台服務或雲端儲存池的新端點。

   > 代理更改最多可能需要 10 分鐘才能生效。

7. 檢查代理伺服器的設置，以確保來自StorageGRID 的平台服務相關訊息不會被封鎖。
8. 如果您需要停用儲存代理，請清除複選框，然後選擇*儲存*。

配置管理代理設定

如果您使用 HTTP 或 HTTPS 傳送AutoSupport套件，則可以在管理節點和技術支援（AutoSupport）之間設定非透明代理伺服器。

有關AutoSupport的更多信息，請參閱"配置AutoSupport"。

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

您可以配置單一管理代理程式的設定。

步驟

1. 選擇*配置* > 安全 > 代理設定。

   出現“代理設定”頁面。預設情況下，在選項卡選單中選擇“儲存”。

2. 選擇“管理”標籤。
3. 選取“啟用管理代理”複選框。
4. 輸入代理伺服器的主機名稱或 IP 位址。
5. 輸入用於連接代理伺服器的連接埠。
6. （可選）輸入代理伺服器的使用者名稱和密碼。

   如果您的代理伺服器不需要使用者名稱或密碼，請將這些欄位留空。

7. 選擇下列選項之一：

   - 如果您想確保與管理代理程式的連線安全，請選擇*驗證代理證書*。上傳 CA 套件以驗證管理代理伺服器提供的 SSL 憑證的真實性。

     如果驗證了代理證書，則按需AutoSupport、透過StorageGRID 的E 系列AutoSupport以及StorageGRID升級頁面上的更新路徑確定將無法運作。

     上傳 CA 包後，其元資料就會出現。

   - 如果您不想在與管理代理伺服器通訊時驗證證書，請選擇*不驗證代理證書*。

8. 選擇*儲存*。

   儲存管理代理程式後，管理節點和技術支援之間的代理伺服器就配置好了。

   代理更改最多可能需要 10 分鐘才能生效。

9. 如果您需要停用管理代理，請清除*啟用管理代理*複選框，然後選擇*儲存*。

控制防火牆

控制外部防火牆的訪問

您可以在外部防火牆處開啟或關閉特定連接埠。

您可以透過開啟或關閉外部防火牆上的特定連接埠來控制對StorageGRID管理節點上的使用者介面和 API 的存取。例如，除了使用其他方法來控制系統存取之外，您可能還希望阻止租戶連接到防火牆處的網格管理器。

如果要設定StorageGRID內部防火牆，請參閱"配置內部防火牆"。

港口	描述	如果連接埠開放...
443	管理節點的預設 HTTPS 連接埠	Web 瀏覽器和管理 API 用戶端可以存取網格管理器、網格管理 API、租用戶管理器和租用戶管理 API。 *注意：*連接埠 443 也用於一些內部流量。
8443	管理節點上的網格管理器連接埠受限	• Web 瀏覽器和管理 API 用戶端可以使用 HTTPS 存取網格管理器和網格管理 API。 • Web 瀏覽器和管理 API 用戶端無法存取租用戶管理器或租用戶管理 API。 • 內部內容請求將被拒絕。
9443	管理節點上的限制租用戶管理器端口	• Web 瀏覽器和管理 API 用戶端可以使用 HTTPS 存取租用戶管理器和租用戶管理 API。 • Web 瀏覽器和管理 API 用戶端無法存取網格管理器或網格管理 API。 • 內部內容請求將被拒絕。

受限的網格管理器或租戶管理器連接埠上不提供單一登入 (SSO)。如果您希望使用者透過單一登入進行驗證，則必須使用預設 HTTPS 連接埠 (443)。

相關資訊

- "Sign in入網格管理器"
- "建立租用戶帳戶"
- "外部溝通"

管理內部防火牆控制

StorageGRID在每個節點上都包含一個內部防火牆，透過讓您能夠控制對節點的網路存取來增強網格的安全性。使用防火牆阻止除特定網格部署所需連接埠之外的所有連接埠的網路存取。您在防火牆控制頁面上所做的設定變更將部署到每個節點。

使用防火牆控制頁面上的三個標籤來自訂網格所需的存取權限。

- 特權位址清單：使用此標籤允許選擇存取已關閉的連接埠。您可以使用「管理外部存取」標籤以 CIDR 表示法新增可存取已關閉連接埠的 IP 位址或子網路。
- 管理外部存取：使用此選項卡關閉預設開啟的端口，或重新開啟先前關閉的端口。
- 不受信任的客戶端網路：使用此選項卡指定節點是否信任來自客戶端網路的入站流量。

此標籤上的設定將覆蓋「管理外部存取」標籤中的設定。

- 具有不受信任的客戶端網路的節點將僅接受該節點上配置的負載平衡器端點連接埠（全域、節點介面和節點類型綁定端點）上的連線。
- 無論「管理外部網路」標籤上的設定為何，負載平衡器端點連接埠都是不受信任的用戶端網路上唯一開放的連接埠。
- 當受信任時，管理外部存取標籤下開啟的所有連接埠以及用戶端網路上開啟的任何負載平衡器端點都是可存取的。

> ⓘ 您在一個選項卡上所做的設定可能會影響您在另一個選項卡上所做的存取變更。請務必檢查所有選項卡上的設置，以確保您的網路按照您預期的方式運作。

若要設定內部防火牆控制，請參閱"配置防火牆控制"。

有關外部防火牆和網路安全的更多信息，請參閱"控制外部防火牆的訪問"。

特權地址清單和管理外部存取選項卡

特權位址清單標籤可讓您註冊一個或多個被授予存取已關閉的網格連接埠的 IP 位址。管理外部存取標籤可讓您關閉對選定外部連接埠或所有開啟的外部連接埠（外部連接埠是預設非網格節點可存取的連接埠）的外部存取。這兩個選項卡通常可以一起使用，以自訂您需要允許電網的精確網路存取。

> ⓘ 預設情況下，特權 IP 位址沒有內部網格連接埠存取權限。

範例 **1**：使用跳轉主機執行維護任務

假設您想使用跳轉主機（安全強化的主機）進行網路管理。您可以使用以下一般步驟：

1. 使用特權位址清單標籤新增跳轉主機的IP位址。
2. 使用“管理外部存取”標籤來阻止所有連接埠。

> ⚠ 在封鎖連接埠 443 和 8443 之前新增特權 IP 位址。任何目前連接到被封鎖連接埠的使用者（包括您）都將失去對網格管理器的存取權限，除非他們的 IP 位址已新增至特權位址清單中。

儲存配置後，網格中管理節點上的所有外部連接埠都將被阻止，跳轉主機除外。然後，您可以使用跳轉主機更安全地在電網上執行維護任務。

範例 **2**：鎖定敏感端口

假設您想要鎖定敏感連接埠和該連接埠上的服務（例如，連接埠 22 上的 SSH）。您可以使用以下一般步驟：

1. 使用特權位址清單標籤僅向需要存取該服務的主機授予存取權限。
2. 使用“管理外部存取”標籤來阻止所有連接埠。

> ⚠ 在阻止存取指派給網格管理器和租用戶管理員的任何連接埠（預設連接埠為 443 和 8443）之前，請新增特權 IP 位址。任何目前連接到被封鎖連接埠的使用者（包括您）都將失去對網格管理器的存取權限，除非他們的 IP 位址已新增至特權位址清單中。

儲存配置後，連接埠 22 和 SSH 服務將可供特權位址清單上的主機使用。無論請求來自哪個接口，所有其他主

機都將被拒絕存取該服務。

範例 **3**：停用對未使用的服務的訪問

在網路級別，您可以停用一些您不想使用的服務。例如，要阻止 HTTP S3 用戶端流量，您可以使用「管理外部存取」標籤上的切換按鈕來封鎖連接埠 18084。

不受信任的客戶端網路選項卡

如果您使用用戶端網絡，則可以透過僅在明確配置的端點上接受入站用戶端流量來協助保護StorageGRID免受惡意攻擊。

預設情況下，每個網格節點上的客戶端網路都是_受信任的_。也就是說，預設情況下， StorageGRID信任所有"可用的外部連接埠"。

您可以透過指定每個節點上的用戶端網路為_不受信任的_來減少對StorageGRID系統的惡意攻擊的威脅。如果節點的用戶端網路不受信任，則該節點僅接受明確配置為負載平衡器端點的連接埠上的入站連線。看"配置負載平衡器端點"和"配置防火牆控制"。

範例 **1**：網關節點僅接受 **HTTPS S3** 請求

假設您希望網關節點拒絕用戶端網路上除 HTTPS S3 請求之外的所有入站流量。您將執行以下常規步驟：

1. 從"負載平衡器端點"頁面上，在連接埠 443 上透過 HTTPS 為 S3 配置負載平衡器端點。
2. 從防火牆控制頁面中，選擇不受信任以指定網關節點上的用戶端網路不受信任。

儲存設定後，網關客戶端網路上的所有入站流量都將被丟棄，但連接埠 443 上的 HTTPS S3 請求和 ICMP 回顯（ping）請求除外。

範例 **2**：儲存節點發送 **S3** 平台服務請求

假設您想要啟用來自儲存節點的出站 S3 平台服務流量，但您想要阻止用戶端網路上到該儲存節點的任何入站連線。您將執行以下常規步驟：

- 從防火牆控制頁面的不受信任的用戶端網路標籤中，指示儲存節點上的用戶端網路不受信任。

儲存配置後，儲存節點不再接受客戶端網路上的任何傳入流量，但它繼續允許向配置的平台服務目標發出出站請求。

範例 **3**：將對網格管理器的存取限制在子網路內

假設您只想允許 Grid Manager 存取特定子網路。您將執行以下步驟：

1. 將管理節點的客戶端網路附加到子網路。
2. 使用不受信任的客戶端網路標籤將客戶端網路配置為不受信任。
3. 建立管理介面負載平衡器端點時，輸入連接埠並選擇該連接埠將存取的管理介面。
4. 對於不受信任的客戶端網絡，選擇「是」。
5. 使用「管理外部存取」標籤來封鎖所有外部連接埠（無論是否為該子網路外的主機設定了特權 IP 位址）。

儲存配置後，只有您指定的子網路上的主機才能存取網格管理器。所有其他主機均被封鎖。

配置內部防火牆

您可以設定StorageGRID防火牆來控制對StorageGRID節點上特定連接埠的網路存取。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 您已查看了"管理防火牆控制"和"網路指南"。
- 如果您希望管理節點或網關節點僅在明確配置的端點上接受入站流量，則您已定義負載平衡器端點。

> 變更客戶端網路的配置時，如果尚未配置負載平衡器端點，則現有客戶端連線可能會失敗。

關於此任務

StorageGRID在每個節點上都包含一個內部防火牆，可讓您開啟或關閉網格節點上的某些連接埠。您可以使用防火牆控制標籤來開啟或關閉網格網路、管理網路和用戶端網路上預設開啟的連接埠。您也可以建立可以存取已關閉的網格連接埠的特權 IP 位址清單。如果您使用用戶端網絡，您可以指定節點是否信任來自客戶端網路的入站流量，並且可以設定客戶端網路上特定連接埠的存取。

將對網格外部 IP 位址開放的連接埠數量限制為僅絕對必要的端口，可增強網格的安全性。您使用三個防火牆控制標籤上的設定來確保僅開啟所需的連接埠。

有關使用防火牆控制的詳細資訊（包括範例），請參閱"管理防火牆控制"。

有關外部防火牆和網路安全的更多信息，請參閱"控制外部防火牆的訪問"。

存取防火牆控制

步驟

1. 選擇*設定* > 安全 > 防火牆控制。

   此頁面上的三個選項卡的描述如下"管理防火牆控制"。

2. 選擇任意選項卡來配置防火牆控制。

   您可以按任意順序使用這些選項卡。您在一個選項卡上設定的配置不會限制您在其他選項卡上可以執行的操作；但是，您在一個選項卡上所做的配置更改可能會更改在其他選項卡上配置的連接埠的行為。

特權地址列表

您可以使用「特權位址清單」標籤授予主機對預設關閉或透過「管理外部存取」標籤上的設定關閉的連接埠的存取權。

預設情況下，特權 IP 位址和子網路沒有內部網格存取權限。此外，即使在「管理外部存取」標籤中被阻止，也可以存取在「特權位址清單」標籤中開啟的負載平衡器端點和其他連接埠。

> 「特權位址清單」標籤上的設定不能覆蓋「不受信任的用戶端網路」標籤上的設定。

步驟

1. 在特權位址清單標籤上，輸入要授予對封閉連接埠的存取權限的位址或 IP 子網路。
2. 或者，選擇*以 CIDR 表示法新增另一個 IP 位址或子網路*來新增其他特權用戶端。

   將盡可能少的地址添加到特權清單中。

3. 或者，選擇*允許特權 IP 位址存取StorageGRID內部連接埠*。看"StorageGRID內部連接埠" 。

   此選項刪除了一些內部服務的保護。如果可能的話，將其保持禁用狀態。

4. 選擇*儲存*。

管理外部訪問

當在「管理外部存取」標籤中關閉某個端口時，任何非網格 IP 位址都無法存取該端口，除非您將該 IP 位址新增至特權位址清單。您只能關閉預設開啟的端口，並且只能打開您已關閉的端口。

「管理外部存取」標籤上的設定不能覆蓋「不受信任的用戶端網路」標籤上的設定。例如，如果某個節點不受信任，則即使在「管理外部存取」標籤上開啟了連接埠 SSH/22，該連接埠也會在用戶端網路上被封鎖。不受信任的客戶端網路標籤上的設定將覆蓋客戶端網路上的已關閉連接埠（例如 443、8443、9443）。

步驟

1. 選擇*管理外部存取*。此標籤顯示一個表，其中包含網格中節點的所有外部連接埠（預設非網格節點可存取的連接埠）。
2. 使用以下選項配置要開啟和關閉的連接埠：

   - 使用每個連接埠旁邊的開關來開啟或關閉選定的連接埠。
   - 選擇*開啟所有顯示的連接埠*以開啟表中列出的所有連接埠。
   - 選擇*關閉所有顯示的連接埠*以關閉表中列出的所有連接埠。

   如果您關閉 Grid Manager 連接埠 443 或 8443，則目前連接到封鎖連接埠的任何使用者（包括您）都會失去對 Grid Manager 的存取權限，除非他們的 IP 位址已新增至特權位址清單中。

   使用表格右側的捲軸確保您已查看所有可用連接埠。使用搜尋欄位輸入連接埠號碼來尋找任何外部連接埠的設定。您可以輸入部分連接埠號碼。例如，如果輸入 **2**，則會顯示名稱中包含字串「2」的所有連接埠。

3. 選擇“儲存”

不受信任的客戶端網絡

如果節點的用戶端網路不受信任，則該節點僅接受配置為負載平衡器端點的連接埠上的入站流量，以及（可選）您在此標籤上選擇的其他連接埠。您也可以使用此標籤指定擴充功能中新增的新節點的預設值。

如果尚未配置負載平衡器端點，現有客戶端連線可能會失敗。

您在「不受信任的用戶端網路」標籤上所做的設定變更將覆蓋「管理外部存取」標籤上的設定。

步驟

1. 選擇*不受信任的客戶端網路*。
2. 在「設定新節點預設值」部分中，指定在擴充過程中將新節點新增至網格時的預設設定。
   - 受信任（預設）：當在擴充功能中新增節點時，其客戶端網路是受信任的。
   - 不受信任：當在擴展中添加節點時，其客戶端網路不受信任。

   根據需要，您可以返回此選項卡來更改特定新節點的設定。

   此設定不會影響StorageGRID系統中的現有節點。
3. 使用下列選項來選擇應僅允許在明確配置的負載平衡器端點或其他選定連接埠上進行用戶端連線的節點：
   - 選擇*不信任顯示的節點*將表中顯示的所有節點新增至不受信任的客戶端網路清單。
   - 選擇「信任顯示的節點」以從不受信任的客戶端網路清單中刪除表中顯示的所有節點。
   - 使用每個節點旁邊的切換按鈕將所選節點的客戶端網路設定為受信任或不受信任。

   例如，您可以選擇*不信任顯示的節點*將所有節點新增至不受信任的用戶端網路清單中，然後使用單一節點旁的切換按鈕將該單一節點新增至受信任的用戶端網路清單。

   使用表格右側的捲軸確保您已查看所有可用節點。使用搜尋欄位輸入節點名稱來尋找任何節點的設定。您可以輸入部分名稱。例如，如果輸入 **GW**，則會顯示名稱中包含字串「GW」的所有節點。
4. 選擇*儲存*。

新的防火牆設定將立即套用並強制執行。如果尚未配置負載平衡器端點，現有客戶端連線可能會失敗。