管理安全性
StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/storagegrid-117/admin/manage-security.html on November 04, 2025. Always check docs.netapp.com for the latest.

目錄

管理安全性 1
管理安全性：總覽 1
管理加密 1
管理憑證 1
設定金鑰管理伺服器 1
管理Proxy設定 1
控制防火牆 1
檢閱StorageGRID 功能加密方法 1
使用多種加密方法 3
管理憑證 3
管理安全性憑證：總覽 4
設定伺服器憑證 13
設定用戶端憑證 24
設定安全性設定 31
管理 TLS 和 SSH 原則 31
設定網路和物件安全性 33
變更瀏覽器閒置逾時 34
設定金鑰管理伺服器 35
設定金鑰管理伺服器：總覽 35
KMS與應用裝置組態總覽 36
使用金鑰管理伺服器的考量與要求 39
變更網站KMS的考量事項 41
在StorageGRID KMS中設定以用戶端身份執行的功能 43
新增金鑰管理伺服器（KMS） 44
檢視KMS詳細資料 51
檢視加密節點 52
編輯金鑰管理伺服器（KMS） 53
移除金鑰管理伺服器（KMS） 55
管理Proxy設定 56
設定儲存Proxy設定 56
設定管理Proxy設定 57
控制防火牆 59
控制外部防火牆的存取 59
管理內部防火牆控制 60
設定內部防火牆 62

管理安全性

管理安全性：總覽

您可以從Grid Manager設定各種安全性設定、以協助保護StorageGRID 您的作業系統。

管理加密

StorageGRID 提供數種加密資料的選項。您應該 "檢閱可用的加密方法" 判斷哪些符合您的資料保護需求。

管理憑證

您可以 "設定及管理伺服器憑證" 用於 HTTP 連線或用於驗證伺服器用戶端或使用者身分識別的用戶端憑證。

設定金鑰管理伺服器

使用 "金鑰管理伺服器" 即使從資料中心移除應用裝置、也能保護 StorageGRID 資料。應用裝置磁碟區加密後、除非節點可以與 KMS 通訊、否則您無法存取應用裝置上的任何資料。

> ⓘ 若要使用加密金鑰管理、您必須在安裝期間、在將應用裝置新增至網格之前、為每個應用裝置啟用*節點加密*設定。

管理**Proxy**設定

如果您使用的是 S3 平台服務或雲端儲存集區、則可以設定 "儲存 Proxy 伺服器" 儲存節點與外部 S3 端點之間的連接。如果您使用 HTTPS 或 HTTP 傳送 AutoSupport 訊息、則可以設定 "管理 Proxy 伺服器" 管理節點與技術支援之間的關係。

控制防火牆

若要增強系統的安全性、您可以開啟或關閉的特定連接埠、以控制對 StorageGRID 管理節點的存取 "外部防火牆"。您也可以透過設定每個節點的網路存取控制 "內部防火牆"。您可以防止存取所有連接埠、但部署所需的連接埠除外。

檢閱**StorageGRID** 功能加密方法

StorageGRID 提供數種加密資料的選項。您應該檢閱可用的方法、以判斷哪些方法符合您的資料保護需求。

下表提供StorageGRID 有關支援的加密方法的高階摘要。

加密選項	運作方式	適用於
Grid Manager中的金鑰管理伺服器（KMS）	您 "設定金鑰管理伺服器" 適用於 StorageGRID 網站和 "啟用應用裝置的節點加密"。然後、應用裝置節點會連線至KMS、以要求金鑰加密金鑰（KEK）。此金鑰會加密及解密每個Volume上的資料加密金鑰（DEK）。	安裝期間啟用*節點加密*的應用裝置節點。應用裝置上的所有資料都能受到保護、避免資料中心的實體遺失或移除。 使用 KMS 管理加密金鑰僅支援儲存節點和服務應用裝置。
在《支援資料保護系統》中提升安全性SANtricity	如果 SG5700 或 SG6000 儲存設備已啟用磁碟機安全功能、您可以使用 "系統管理程式SANtricity" 以建立及管理安全金鑰。存取受保護磁碟機上的資料需要金鑰。	具有全磁碟加密（ FDE ）磁碟機或 FIPS 磁碟機的儲存設備。安全磁碟機上的所有資料都能受到保護、避免實體遺失或從資料中心移除。無法與某些儲存設備或任何服務應用裝置搭配使用。
儲存的物件加密	您可以啟用 "儲存的物件加密" Grid Manager 中的選項。啟用時、在貯體層級或物件層級未加密的任何新物件、都會在擷取期間加密。	新擷取的S3和Swift物件資料。 現有儲存的物件不會加密。物件中繼資料和其他敏感資料不會加密。
S3儲存區加密	您發出一個「放入庫位」加密要求、以啟用庫位加密。在物件層級未加密的任何新物件、都會在擷取期間加密。	僅限新擷取的S3物件資料。 必須為儲存區指定加密。現有的貯體物件不會加密。物件中繼資料和其他敏感資料不會加密。 "在貯體上作業"
S3物件伺服器端加密（SSe）	您發出S3要求來儲存物件並納入 `x-amz-server-side-encryption` 要求標頭：	僅限新擷取的S3物件資料。 必須為物件指定加密。物件中繼資料和其他敏感資料不會加密。 可管理金鑰。StorageGRID "使用伺服器端加密"

加密選項	運作方式	適用於
S3物件伺服器端加密、使用客戶提供的金鑰（SSE-C）	您發出S3要求以儲存物件、並包含三個要求標頭。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	僅限新擷取的S3物件資料。 必須為物件指定加密。物件中繼資料和其他敏感資料不會加密。 金鑰是在StorageGRID 非功能性的範圍內管理。 "使用伺服器端加密"
外部Volume或資料存放區加密	如果StorageGRID 您的部署平台支援、您可以使用不屬於支援的加密方法來加密整個磁碟區或資料存放區。	所有物件資料、中繼資料和系統組態資料、假設每個磁碟區或資料存放區都已加密。 外部加密方法可更嚴密地控制加密演算法和金鑰。可與其他列出的方法結合使用。
物件加密不StorageGRID 包括在內	您可以在StorageGRID 物件資料和中繼資料被擷取到StorageGRID 資料之前、使用非功能性的加密方法來加密物件資料和中繼資料。	僅限物件資料和中繼資料（系統組態資料未加密）。 外部加密方法可更嚴密地控制加密演算法和金鑰。可與其他列出的方法結合使用。 "Amazon Simple Storage Service - 開發人員指南：使用用戶端加密來保護資料"

使用多種加密方法

視您的需求而定、您一次可以使用多種加密方法。例如：

- 您可以使用KMS來保護應用裝置節點、也可以使用SANtricity 支援系統管理程式中的磁碟機安全功能、在同一個應用裝置中的自我加密磁碟機上「雙重加密」資料。
- 您可以使用 KMS 來保護應用裝置節點上的資料、也可以使用儲存的物件加密選項來加密擷取的所有物件。

如果只有一小部分物件需要加密、請考慮改為在儲存區或個別物件層級控制加密。啟用多層加密會增加效能成本。

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。

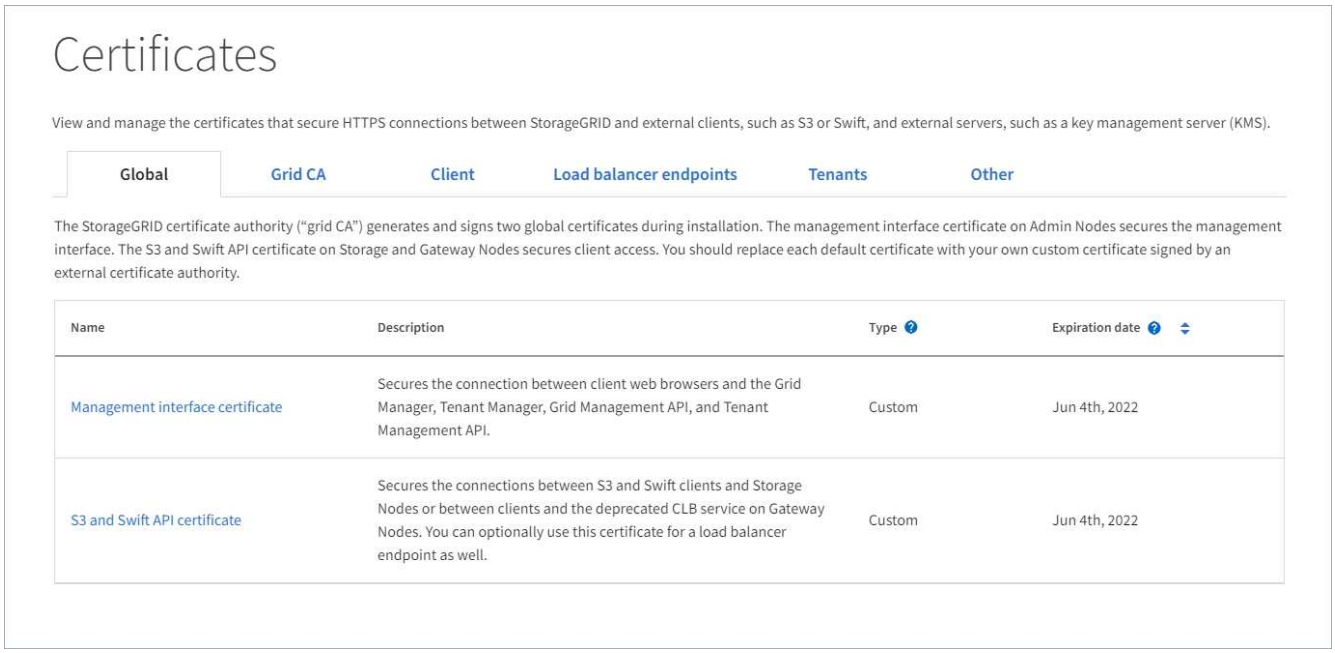
伺服器和用戶端憑證類型的變種會以多種方式實作。在設定系統之前、您應該StorageGRID 準備好特定的支援功能組態所需的所有憑證。

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》。

設定安全性設定

管理 TLS 和 SSH 原則

TLS 和 SSH 原則決定使用哪些通訊協定和加密程式來建立與用戶端應用程式的安全 TLS 連線、以及安全的 SSH 連線至內部 StorageGRID 服務。

安全性原則控制 TLS 和 SSH 如何加密移動中的資料。一般而言、請使用現代化相容性（預設）原則、除非您的系統需要符合一般準則、或您需要使用其他密碼。

某些 StorageGRID 服務尚未更新、無法在這些原則中使用密碼。

開始之前

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

選取安全性原則

步驟

1. 選擇 * 組態 * > * 安全性 * > * 安全性設定 * 。

   「 *TLS 與 SSH 原則 * 」標籤會顯示可用的原則。目前作用中的原則會在原則方塊上以綠色核取記號表示。

2. 檢閱方塊以瞭解可用的原則。

原則	說明
現代化相容性（預設）	如果您需要增強式加密、而且沒有特殊要求、請使用預設原則。此原則與大多數 TLS 和 SSH 用戶端相容。

原則	說明
舊版相容性	如果您需要舊版用戶端的其他相容性選項、請使用此原則。此原則中的其他選項可能會使其比現代相容性原則更不安全。
一般準則	如果您需要通用準則認證、請使用此原則。
FIPS 嚴格	如果您需要 Common Criteria 認證、而且需要使用 NetApp Cryptographic Security Module 3.0.0 進行外部用戶端連線、以連接負載平衡器端點、 Tenant Manager 和 Grid Manager 、請使用此原則。使用此原則可能會降低效能。
自訂	如果您需要套用自己的密碼、請建立自訂原則。

3. 若要查看每個原則的密碼、通訊協定和演算法的詳細資料、請選取 * 檢視詳細資料 * 。
4. 若要變更目前的原則、請選取 * 使用原則 * 。

   原則方塊上的 * 目前原則 * 旁會出現綠色核取記號。

建立自訂安全性原則

如果您需要套用自己的密碼、可以建立自訂原則。

步驟

1. 從最類似您要建立之自訂原則的原則方塊中、選取 * 檢視詳細資料 * 。
2. 選取 * 複製到剪貼簿 * 、然後選取 * 取消 * 。

3. 從 * 自訂原則 * 方塊中、選取 * 設定與使用 * 。
4. 貼上您複製的 JSON 、然後進行任何必要的變更。
5. 選取 * 使用原則 * 。

「自訂原則」方塊的 * 目前原則 * 旁會出現綠色核取記號。

6. 您也可以選擇 * 編輯組態 * 來對新的自訂原則進行更多變更。

暫時恢復為預設的安全性原則

如果您設定了自訂安全性原則、如果設定的 TLS 原則與不相容、則可能無法登入 Grid Manager "已設定的伺服器憑證"。

您可以暫時還原為預設的安全性原則。

步驟

1. 登入管理節點：
   a. 輸入下列命令： `ssh admin@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 `#`。

2. 執行下列命令：

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

3. 從網頁瀏覽器存取同一個管理節點上的Grid Manager。
4. 請依照中的步驟進行 選取安全性原則 重新設定原則。

設定網路和物件安全性

您可以設定網路和物件安全性來加密儲存的物件、防止某些 S3 和 Swift 要求、或允許用戶端連線至儲存節點使用 HTTP 而非 HTTPS 。

儲存的物件加密

儲存的物件加密可在透過 S3 擷取時、加密所有物件資料。根據預設、儲存的物件不會加密、但您可以選擇使用 AES - 128 或 AES - 256 加密演算法來加密物件。啟用此設定時、所有新擷取的物件都會加密、但不會對現有的儲存物件進行任何變更。如果停用加密、目前加密的物件仍會保持加密狀態、但新擷取的物件不會加密。

「儲存的物件加密」設定僅適用於未透過貯體層級或物件層級加密進行加密的 S3 物件。

如需 StorageGRID 加密方法的詳細資訊、請參閱 "檢閱StorageGRID 功能加密方法"。

防止用戶端修改

防止用戶端修改是全系統的設定。當選擇 * 防止用戶端修改 * 選項時、會拒絕下列要求。

S3 REST API

- 刪除時段要求
- 任何修改現有物件資料、使用者定義中繼資料或S3物件標記的要求

Swift REST API

- 刪除Container要求
- 要求修改任何現有物件。例如、下列作業會遭拒：「放置覆寫」、「刪除」、「中繼資料更新」等。

啟用 **HTTP** 以進行儲存節點連線

根據預設、用戶端應用程式會使用 HTTPS 網路傳輸協定來直接連線至儲存節點。您可以選擇性地為這些連線啟用HTTP、例如在測試非正式作業網格時。

只有當 S3 和 Swift 用戶端需要直接與儲存節點建立 HTTP 連線時、才可使用 HTTP 進行儲存節點連線。您不需要將此選項用於僅使用 HTTPS 連線的用戶端或連線至負載平衡器服務的用戶端（因為您可以 "設定每個負載平衡器端點" 使用 HTTP 或 HTTPS ）。

請參閱 "摘要：用於用戶端連線的IP位址和連接埠" 瞭解使用 HTTP 或 HTTPS 連線至儲存節點時、 S3 和 Swift 用戶端使用的連接埠。

選取選項

開始之前

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

步驟

1. 選擇 * 組態 * > * 安全性 * > * 安全性設定 * 。
2. 選取 * 網路和物件 * 索引標籤。
3. 對於儲存的物件加密、如果您不想加密儲存的物件、請使用 * 無 * （預設）設定、或選取 * AES-128* 或 * AES-256* 來加密儲存的物件。
4. 如果您想要防止 S3 和 Swift 用戶端提出特定要求、請選擇性地選取 * 防止用戶端修改 * 。

   如果您變更此設定、則需要約一分鐘的時間才能套用新設定。系統會快取設定的值、以利效能與擴充。

5. 如果用戶端直接連線至儲存節點、且您想使用 HTTP 連線、則可選擇 * 啟用儲存節點連線的 HTTP * 。

   啟用正式作業網格的HTTP時請務必小心、因為要求會以未加密的方式傳送。

6. 選擇*保存*。

變更瀏覽器閒置逾時

您可以控制Grid Manager和Tenant Manager使用者是否在超過一定時間內處於非作用中狀

態時登出。

開始之前

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

關於這項工作

瀏覽器閒置逾時預設為 15 分鐘。如果使用者的瀏覽器在這段時間內未啟用、則使用者會登出。

視需要、您可以設定 * 在 * 之後登出非使用中的使用者選項、以增加或縮短逾時時間。

瀏覽器閒置逾時也由下列項目控制：

- 另有一個不可設定StorageGRID 的獨立式計時功能、可用於系統安全性。根據預設、每個使用者的驗證權杖會在使用者登入後16小時過期。當使用者的驗證過期時、該使用者會自動登出、即使瀏覽器閒置逾時已停用、或瀏覽器逾時的值尚未達到。若要續約權杖、使用者必須重新登入。
- 假設 StorageGRID 已啟用單一登入（ SSO ）、則身分識別提供者的逾時設定。

  如果啟用 SSO 且使用者的瀏覽器逾時、使用者必須重新輸入其 SSO 認證、才能再次存取 StorageGRID 。請參閱 "設定單一登入"。

步驟

1. 選擇 * 組態 * > * 安全性 * > * 安全性設定 * 。
2. 選擇 * 瀏覽器閒置逾時 * 標籤。
3. 在 * 在 * 之後登出非使用中的使用者 * 欄位中、指定介於 60 秒到 7 天之間的瀏覽器逾時期間。

   您可以指定瀏覽器的逾時期間、以秒、分鐘、小時或天為單位。

4. 選擇*保存*。如果瀏覽器在指定的時間內處於非使用中狀態、則使用者會登出 Grid Manager 或 Tenant Manager 。

   新設定不會影響目前登入的使用者。使用者必須重新登入或重新整理瀏覽器、新的逾時設定才會生效。

設定金鑰管理伺服器

設定金鑰管理伺服器：總覽

您可以設定一或多個外部金鑰管理伺服器（KMS）、以保護特殊設定的應用裝置節點上的資料。

什麼是金鑰管理伺服器（**KMS**）？

金鑰管理伺服器（KMS）是一種外部的第三方系統StorageGRID 、可透過StorageGRID 金鑰管理互通性傳輸協定（KMIP）、為相關聯的站台上的應用裝置節點提供加密金鑰。

您可以使用一或多個金鑰管理伺服器、來管理StorageGRID 安裝期間啟用*節點加密*設定的任何節點的節點加密金鑰。即使從資料中心移除應用裝置、將關鍵管理伺服器與這些應用裝置節點搭配使用、也能保護資料。應用裝

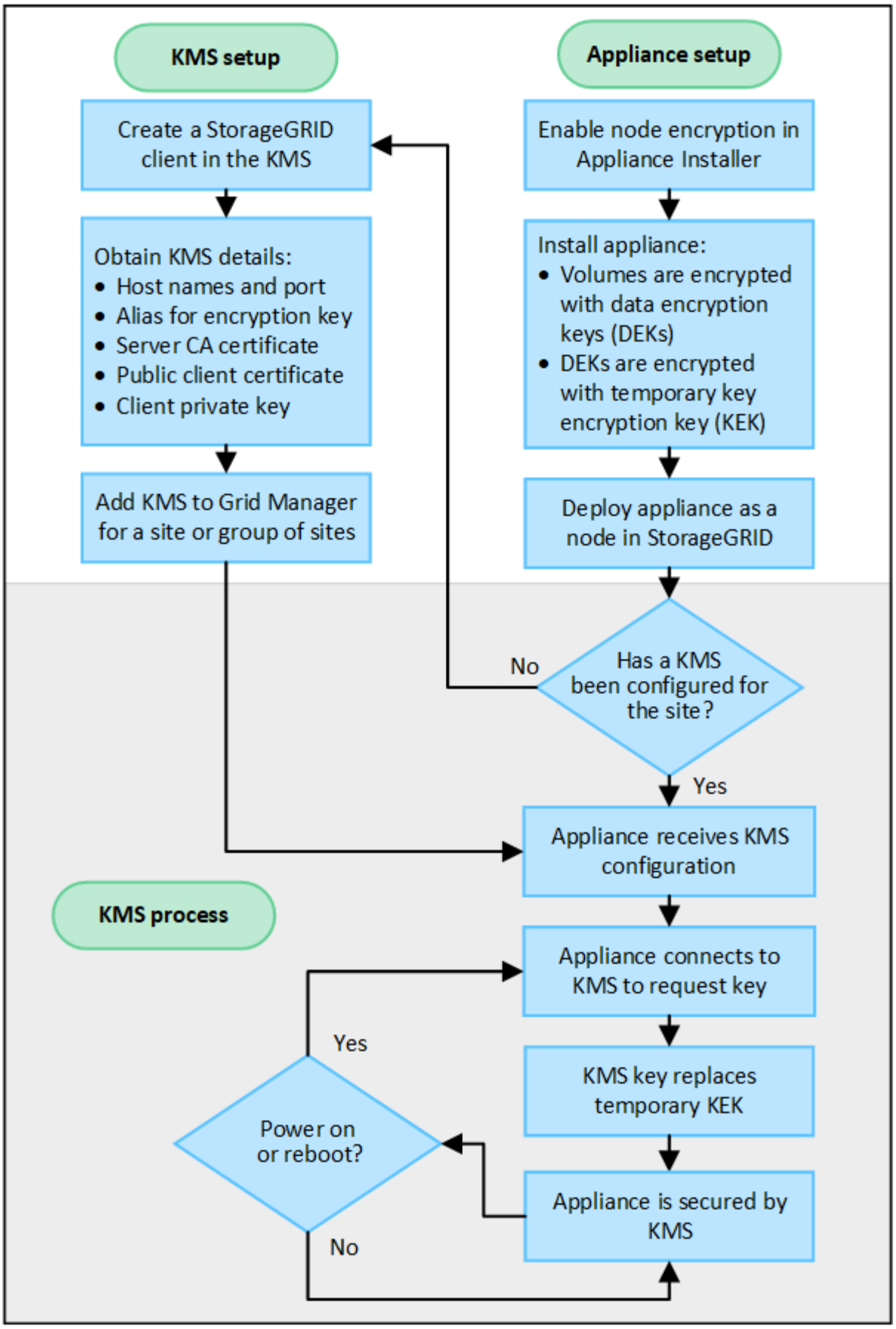
置磁碟區加密後、除非節點可以與 KMS 通訊、否則您無法存取應用裝置上的任何資料。

> 不建立或管理用於加密和解密應用裝置節點的外部金鑰。StorageGRID如果您打算使用外部金鑰管理伺服器來保護StorageGRID 這些資料、您必須瞭解如何設定該伺服器、而且必須瞭解如何管理加密金鑰。執行關鍵管理工作的範圍超出這些指示的範圍。如果您需要協助、請參閱金鑰管理伺服器的文件、或聯絡技術支援部門。

KMS與應用裝置組態總覽

在使用金鑰管理伺服器（KMS）來保護StorageGRID 應用裝置節點上的各項資料之前、您必須先完成兩項組態工作：設定一或多個KMS伺服器、以及為應用裝置節點啟用節點加密。完成這兩項組態工作之後、就會自動執行金鑰管理程序。

流程圖顯示使用KMS保護StorageGRID 應用裝置節點上的資訊安全的高階步驟。



流程圖會顯示KMS設定與應用裝置設定並行執行、不過您可以根據需求、在新應用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**）

設定金鑰管理伺服器包括下列高層級步驟。

步驟	請參閱
存取KMS軟體、並在StorageGRID 每個KMS或KMS叢集上新增一個用戶端以供使用。	"在StorageGRID KMS中設定以用戶端身份執行的功能"
在StorageGRID KMS取得有關該客戶端的必要資訊。	"在StorageGRID KMS中設定以用戶端身份執行的功能"
將KMS新增至Grid Manager、指派給單一站台或預設站台群組、上傳必要的憑證、並儲存KMS組態。	"新增金鑰管理伺服器（KMS）"

設定產品

設定KMS使用的應用裝置節點包括下列高層級步驟。

1. 在設備安裝的硬體組態階段、請使用StorageGRID 「支援服務」功能的「應用程式安裝程式」來啟用應用裝置的「節點加密」設定。

   將應用裝置新增至網格後、您無法啟用 * 節點加密 * 設定、也無法將外部金鑰管理用於未啟用節點加密的應用裝置。

2. 執行StorageGRID 《程式安裝程式：在安裝期間、會將隨機資料加密金鑰（DEek）指派給每個應用裝置磁碟區、如下所示：
   - DEK用於加密每個Volume上的資料。這些金鑰是使用應用裝置作業系統中的 Linux 統一金鑰設定（ LUKS ）磁碟加密來產生、無法變更。
   - 每個個別的「DEK」都是使用主要金鑰加密金鑰（KEK）進行加密。初始KEK是加密DEK的暫用金鑰、直到應用裝置連線至KMS為止。
3. 將應用裝置節點新增StorageGRID 至

請參閱 "啟用節點加密" 以取得詳細資料。

金鑰管理加密程序（自動執行）

金鑰管理加密包括下列自動執行的高層級步驟。

1. 當您在網格中安裝已啟用節點加密的應用裝置時StorageGRID 、即可判斷包含新節點的站台是否存在KMS組態。
   - 如果站台已設定KMS、則裝置會接收KMS組態。
   - 如果尚未為站台設定KMS、則在您為站台設定KMS、且裝置收到KMS組態之前、應用裝置上的資料會繼續由暫用KEK加密。
2. 應用裝置使用KMS組態連線至KMS、並要求加密金鑰。

3. KMS會傳送加密金鑰給應用裝置。來自KMS的新金鑰取代了暫用KEK、現在用於加密和解密應用裝置磁碟區的DEK。

> 加密應用裝置節點連線至設定的KMS之前存在的任何資料、都會以暫用金鑰加密。不過、除非KMS加密金鑰取代暫用金鑰、否則應用裝置磁碟區不應被視為受到保護、以免從資料中心移除。

4. 如果裝置電源已開啟或重新開機、則會重新連線至KMS以要求金鑰。儲存在揮發性記憶體中的金鑰、無法在停電或重新開機的情況下繼續運作。

使用金鑰管理伺服器的考量與要求

在設定外部金鑰管理伺服器（KMS）之前、您必須先瞭解考量事項與需求。

KMIP需求為何？

支援KMIP 1.4版。StorageGRID

"關鍵管理互通性傳輸協定規格1.4版"

應用裝置節點與設定的KMS之間的通訊使用安全的TLS連線。支援下列TLS v1.2加密算法的KMIP：StorageGRID

- TLS_ECDHE_RSA_with _AES-256_GCM_SHA384
- TLS_ECDHE_ECDSa_with _AES-256_GCM_SHA384

您必須確保使用節點加密的每個應用裝置節點、都能透過網路存取您為站台設定的KMS或KMS叢集。

網路防火牆設定必須允許每個應用裝置節點透過金鑰管理互通性傳輸協定（KMIP）通訊所使用的連接埠進行通訊。預設KMIP連接埠為5696。

支援哪些應用裝置？

您可以使用金鑰管理伺服器（KMS）來管理StorageGRID 網格中任何啟用「節點加密」設定的項目之加密金鑰。此設定只能在安裝應用StorageGRID 程式的硬體組態階段、使用《支援環境》安裝程式來啟用。

> 將應用裝置新增至網格後、您無法啟用節點加密、也無法將外部金鑰管理用於未啟用節點加密的應用裝置。

您可以使用已設定的 KMS for StorageGRID 應用裝置和應用裝置節點。

您無法將已設定的 KMS 用於軟體型（非應用裝置）節點、包括下列項目：

- 部署為虛擬機器（VM）的節點
- 部署在Linux主機上Container引擎內的節點

部署在這些其他平台上的節點、可以在StorageGRID 資料存放區或磁碟層級使用非功能加密。

何時應該設定金鑰管理伺服器？

對於新安裝、您通常應該先在Grid Manager中設定一或多個金鑰管理伺服器、然後再建立租戶。此順序可確保節點在儲存任何物件資料之前受到保護。

您可以在安裝應用裝置節點之前或之後、在Grid Manager中設定金鑰管理伺服器。

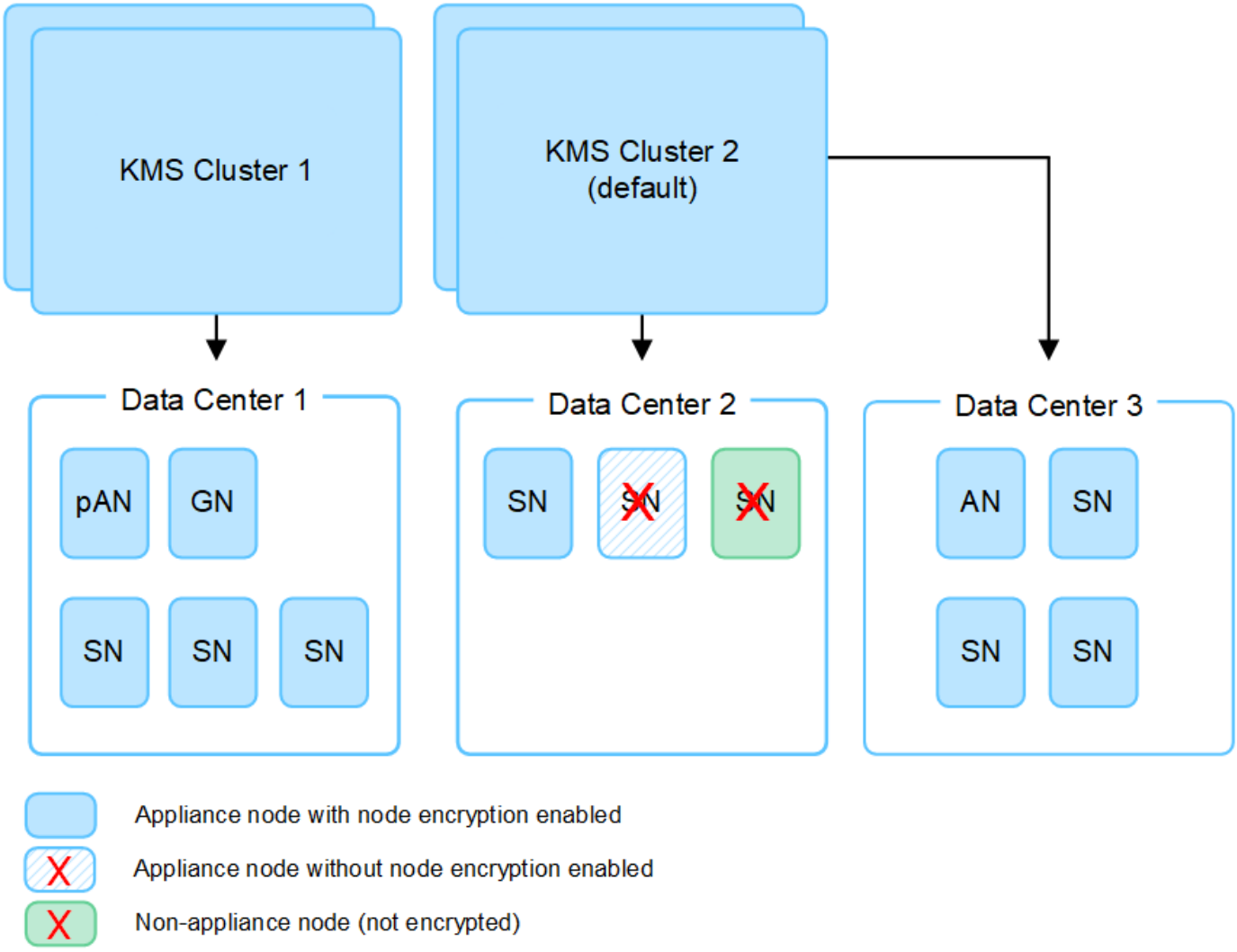
我需要多少個關鍵管理伺服器？

您可以設定一或多個外部金鑰管理伺服器、為StorageGRID 您的作業系統中的應用裝置節點提供加密金鑰。每個KMS都會在StorageGRID 單一站台或一組站台上、提供單一的加密金鑰給各個不完整的應用裝置節點。

支援使用KMS叢集。StorageGRID每個KMS叢集都包含多個複寫的金鑰管理伺服器、這些伺服器共用組態設定和加密金鑰。建議使用KMS叢集進行金鑰管理、因為它能改善高可用度組態的容錯移轉功能。

舉例來說、假設StorageGRID 您的一套系統有三個資料中心站台。您可以設定一個KMS叢集、為資料中心1的所有應用裝置節點提供金鑰、並設定第二個KMS叢集、為所有其他站台的所有應用裝置節點提供金鑰。新增第二個KMS叢集時、您可以為資料中心2和資料中心3設定預設KMS。

請注意、您無法將 KMS 用於非應用裝置節點、或用於安裝期間未啟用 * 節點加密 * 設定的任何應用裝置節點。



當金鑰旋轉時會發生什麼事？

最佳安全做法是定期旋轉每個設定KMS所使用的加密金鑰。

旋轉加密金鑰時、請使用KMS軟體、從上次使用的金鑰版本轉換成相同金鑰的新版本。請勿旋轉至完全不同的金鑰。

> 切勿嘗試在Grid Manager中變更KMS的金鑰名稱（別名）來旋轉金鑰。而是更新KMS軟體中的金鑰版本來旋轉金鑰。對新金鑰使用與先前金鑰相同的金鑰別名。如果您變更設定KMS的金鑰別名、StorageGRID 則可能無法解密您的資料。

當新的金鑰版本可用時：

- 它會自動發佈至站台或與KMS相關之站台的加密應用裝置節點。發佈應在鑰匙轉動後一個小時內完成。
- 如果在發佈新金鑰版本時、加密的應用裝置節點已離線、節點會在重新開機時立即收到新金鑰。
- 如果由於任何原因而無法使用新的金鑰版本來加密應用裝置磁碟區、則會針對應用裝置節點觸發 * KMS 加密金鑰旋轉失敗 * 警示。您可能需要聯絡技術支援部門、以協助解決此警示。

我可以在設備節點加密後重複使用嗎？

如果您需要將加密的應用裝置安裝到另一個StorageGRID 版本、則必須先取消委任網格節點、才能將物件資料移到另一個節點。然後、您可以使用 StorageGRID 應用裝置安裝程式來執行 "清除 KMS 組態"。清除KMS組態會停用「節點加密」設定、並移除應用裝置節點與StorageGRID 本網站KMS組態之間的關聯。

> 由於無法存取KMS加密金鑰、因此無法再存取設備上的任何資料、而且會永久鎖定。

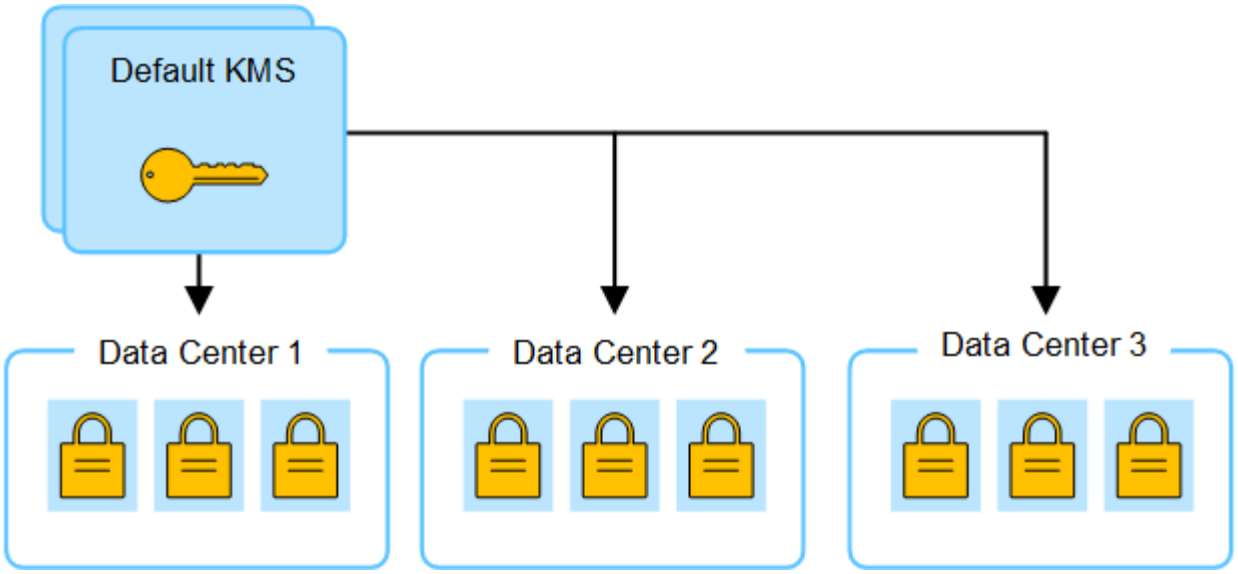
變更網站**KMS**的考量事項

每個金鑰管理伺服器（KMS）或KMS叢集都會為單一站台或一組站台的所有應用裝置節點提供加密金鑰。如果您需要變更站台使用的KMS、可能需要將加密金鑰從一個KMS複製到另一個KMS。

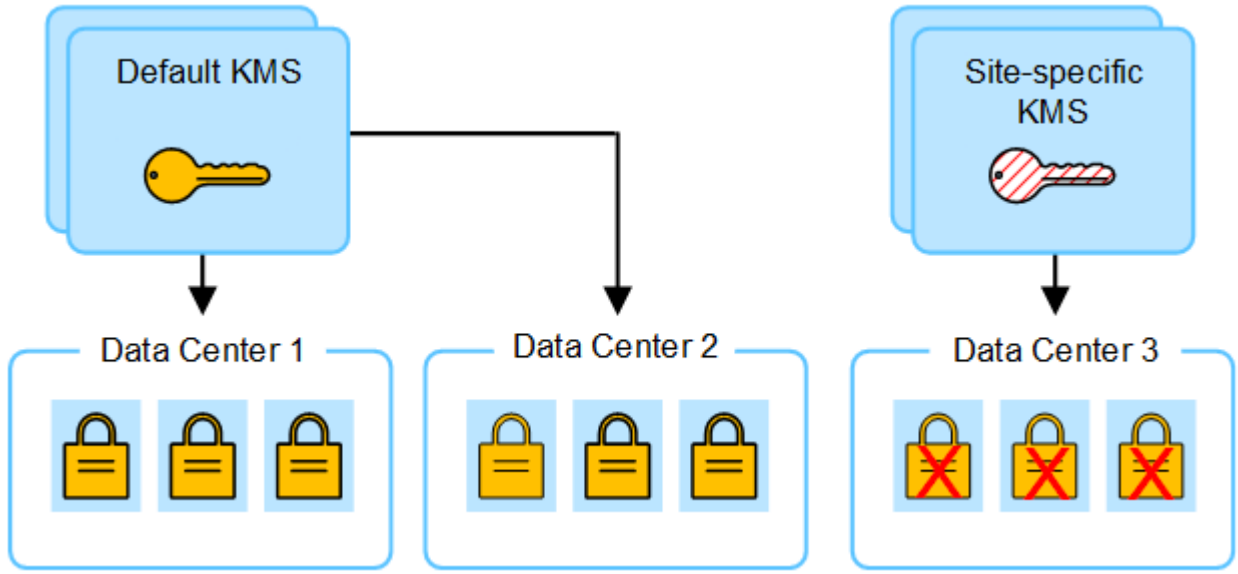
如果您變更站台使用的KMS、則必須確保該站台先前加密的應用裝置節點可以使用儲存在新KMS上的金鑰來解密。在某些情況下、您可能需要將目前版本的加密金鑰從原始KMS複製到新的KMS。您必須確保KMS擁有正確的金鑰、以便在站台上解密加密的應用裝置節點。

例如：

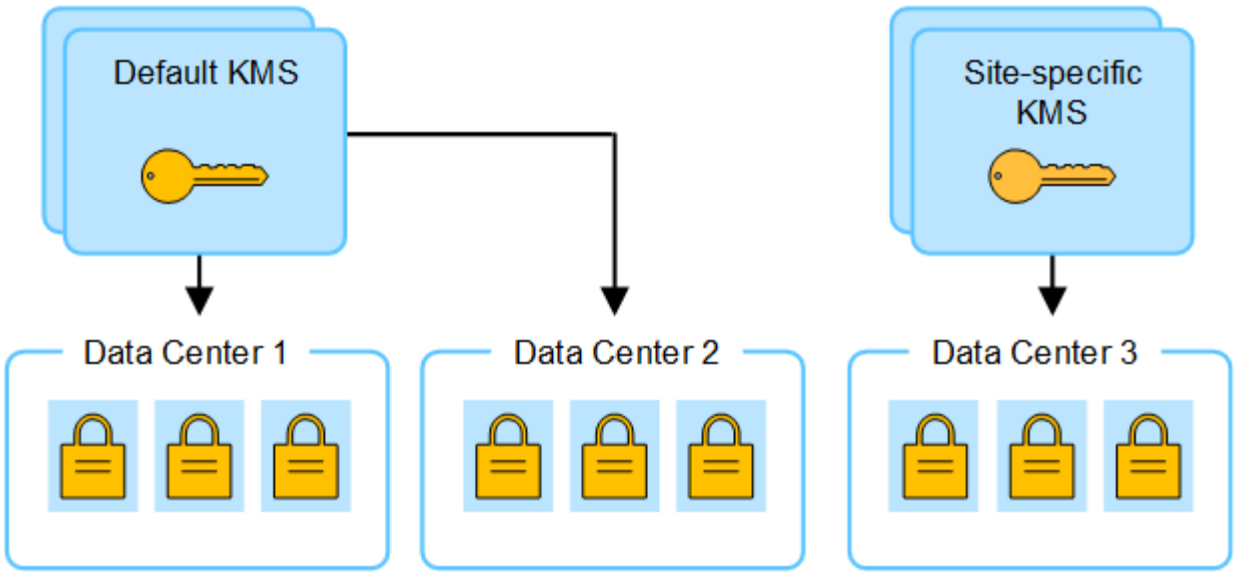
1. 您一開始會設定預設 KMS 、以套用至所有沒有專屬 KMS 的網站。
2. 儲存KMS時、所有啟用「節點加密」設定的應用裝置節點都會連線至KMS、並要求加密金鑰。此金鑰用於加密所有站台的應用裝置節點。此相同金鑰也必須用於解密這些應用裝置。



3. 您決定為單一站台新增站台專屬的KMS（圖中的資料中心3）。不過、由於應用裝置節點已加密、因此當您嘗試儲存站台特定KMS的組態時、就會發生驗證錯誤。發生此錯誤的原因是站台特定的KMS沒有正確的金鑰來解密該站台的節點。



4. 若要解決此問題、請將目前版本的加密金鑰從預設KMS複製到新的KMS。（技術上、您可以將原始金鑰複製到具有相同別名的新金鑰。原始金鑰會成為新金鑰的先前版本。） 站台專屬的KMS現在擁有正確的金鑰、可在Data Center 3解密應用裝置節點、以便儲存在StorageGRID 原地。



變更站台使用**KMS**的使用案例

下表摘要列出變更站台KMS的最常見案例所需步驟。

變更站台**KMS**的使用案例	必要步驟
您有一或多個站台專屬的KMS項目、您想要使用其中一個做為預設KMS。	編輯站台專屬的KMS。在*管理金鑰*欄位中、選取*不受其他KMS管理的站台（預設KMS）*。網站專屬KMS現在將做為預設KMS使用。它將套用至任何沒有專屬 KMS 的網站。 "編輯金鑰管理伺服器（KMS）"
您有預設的KMS、而且您在擴充中新增了一個網站。您不想在新網站上使用預設的 KMS 。	1. 如果新站台的應用裝置節點已在預設KMS中加密、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Grid Manager新增KMS並選取網站。 "新增金鑰管理伺服器（KMS）"
您想讓站台的KMS使用不同的伺服器。	1. 如果站台上的應用裝置節點已由現有的KMS加密、請使用KMS軟體將目前版本的加密金鑰從現有的KMS複製到新的KMS。 2. 使用Grid Manager編輯現有的KMS組態、然後輸入新的主機名稱或IP位址。 "新增金鑰管理伺服器（KMS）"

在**StorageGRID KMS**中設定以用戶端身份執行的功能

您必須先為StorageGRID 每個外部金鑰管理伺服器或KMS叢集設定用作用戶端的功能、才能將KMS新增StorageGRID 至原地。

關於這項工作

這些指示適用於 Thales CipherTrust Manager 。如需支援版本的清單、請使用 "NetApp互通性對照表工具IMT（不含）"。

步驟

1. 在KMS軟體中、為StorageGRID 您打算使用的每個KMS或KMS叢集建立一個完善的用戶端。

   每個KMS都會在StorageGRID 單一站台或一組站台上、管理一個用於「不完整」應用裝置節點的加密金鑰。

2. 從KMS軟體為每個KMS或KMS叢集建立AES加密金鑰。

   加密金鑰必須為 2 、 048 位元以上、而且必須可匯出。

3. 記錄每個KMS或KMS叢集的下列資訊。

   當您將KMS新增StorageGRID 至原地時、您需要這些資訊。

   - 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。

     KMS中必須已存在加密金鑰。不建立或管理KMS金鑰。StorageGRID

4. 對於每個KMS或KMS叢集、請取得由憑證授權單位（CA）簽署的伺服器憑證、或是包含每個以憑證鏈順序串聯的、以PEE編碼之CA憑證檔案的憑證套件。

   伺服器憑證可讓外部KMS驗證自己StorageGRID 以供驗證。

   - 憑證必須使用隱私增強型郵件（ PEF ） Base - 64 編碼的 X · 509 格式。
   - 每個伺服器憑證中的「Subject Alternative Name（SAN）（主體替代名稱（SAN））」欄位必須包含StorageGRID 完整網域名稱（FQDN）或要連線的IP位址。

     在StorageGRID 進行KMS設定時、您必須在*主機名稱*欄位中輸入相同的FQDN或IP位址。

   - 伺服器憑證必須符合KMS KMIP介面所使用的憑證、後者通常使用連接埠5696。

5. 取得由StorageGRID 外部KMS核發的公有用戶端憑證、以及用戶端憑證的私密金鑰。

   用戶端憑證StorageGRID 可讓支援驗證本身到KMS。

新增金鑰管理伺服器（**KMS**）

您可以使用StorageGRID 「驗鑰管理伺服器」精靈來新增每個KMS或KMS叢集。

開始之前

- 您已檢閱 "使用金鑰管理伺服器的考量與要求"。
- 您有 "設定StorageGRID 成KMS中的用戶端"，而且您擁有每個KMS或KMS叢集所需的資訊。

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

關於這項工作

如有可能、請先設定任何站台專屬的金鑰管理伺服器、再設定適用於其他KMS未管理之所有站台的預設KMS。如果您先建立預設KMS、則網格中的所有節點加密應用裝置都會以預設KMS加密。如果您想要稍後建立站台專屬的KMS、必須先將目前版本的加密金鑰從預設的KMS複製到新的KMS。請參閱 "變更網站KMS的考量事項" 以取得詳細資料。

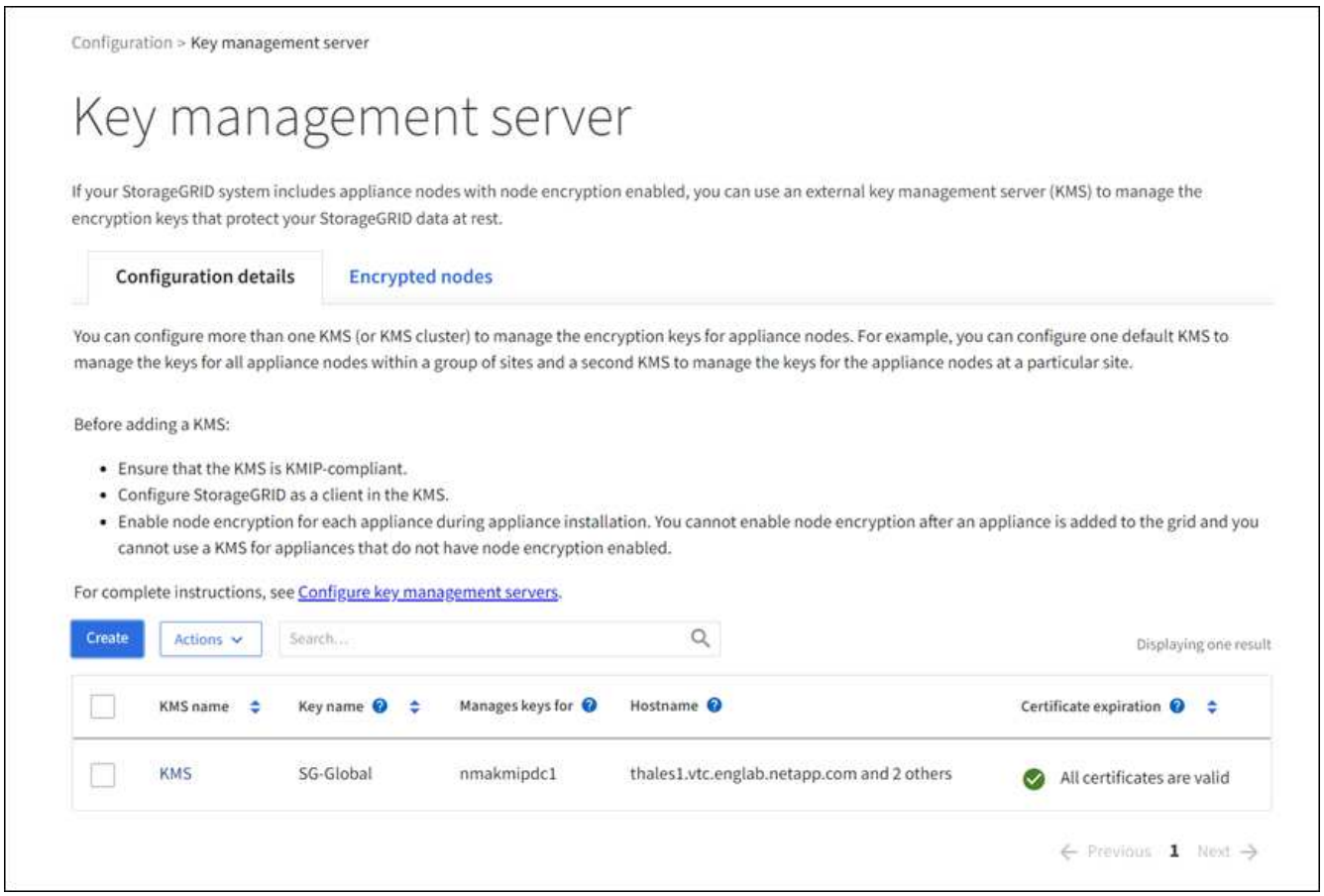
步驟 **1** ： **KMS** 詳細資料

在新增金鑰管理伺服器精靈的步驟 1 （ KMS 詳細資料）中、您會提供 KMS 或 KMS 叢集的詳細資料。

步驟

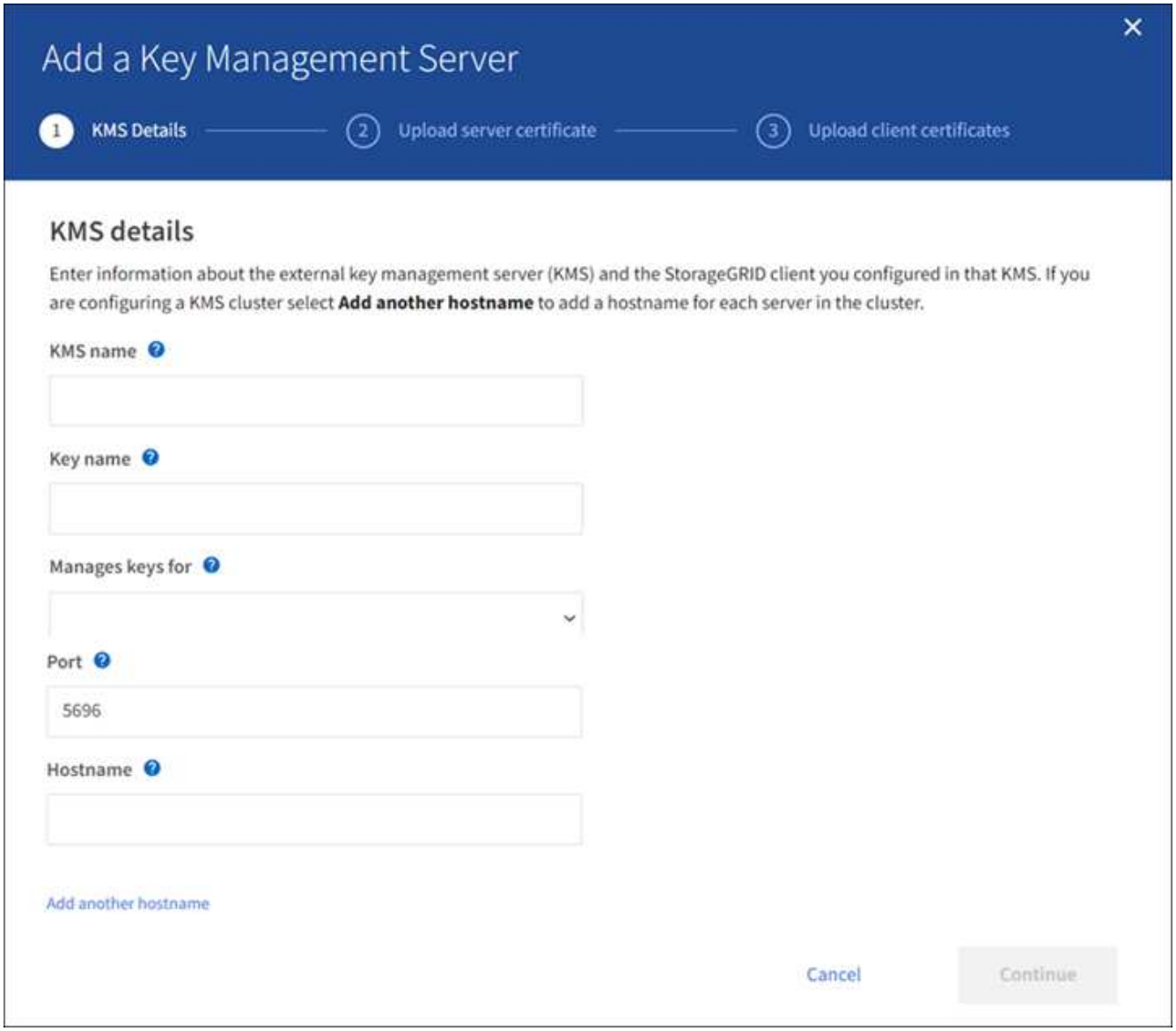
1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   此時會出現金鑰管理伺服器頁面、並選取組態詳細資料索引標籤。



2. 選擇* Create （建立）。

   隨即顯示新增金鑰管理伺服器精靈的步驟 1 （ KMS 詳細資料）。



3. 針對您StorageGRID 在該KMS中設定的KMS和整套用戶端、輸入下列資訊。

欄位	說明
KMS 名稱	可協助您識別此KMS的描述性名稱。必須介於1到64個字元之間。
金鑰名稱	KMS中適用於該客戶端的確切金鑰別名StorageGRID 。必須介於1到255個字元之間。

欄位	說明
管理的金鑰	將與此KMS相關聯的網站。StorageGRID如有可能、您應該先設定任何站台專屬的金鑰管理伺服器、再設定適用於其他KMS未管理之所有站台的預設KMS。 • 如果此KMS將管理特定站台應用裝置節點的加密金鑰、請選取站台。 • 選取 * 不受其他 KMS 管理的網站（預設 KMS ） * 來設定預設 KMS 、以套用至任何沒有專用 KMS 的網站、以及您在後續擴充中新增的任何網站。 *附註：*如果您選取先前已由預設KMS加密的網站、但未將目前版本的原始加密金鑰提供給新的KMS、則儲存KMS組態時會發生驗證錯誤。
連接埠	KMS伺服器用於金鑰管理互通性傳輸協定（KMIP）通訊的連接埠。預設為5696、即KMIP標準連接埠。
主機名稱	KMS的完整網域名稱或IP位址。 • 注意： * 伺服器憑證的主體替代名稱（ SAN ）欄位必須包含您在此輸入的 FQDN 或 IP 位址。否則StorageGRID 、無法將無法連接至KMS或KMS叢集中的所有伺服器。

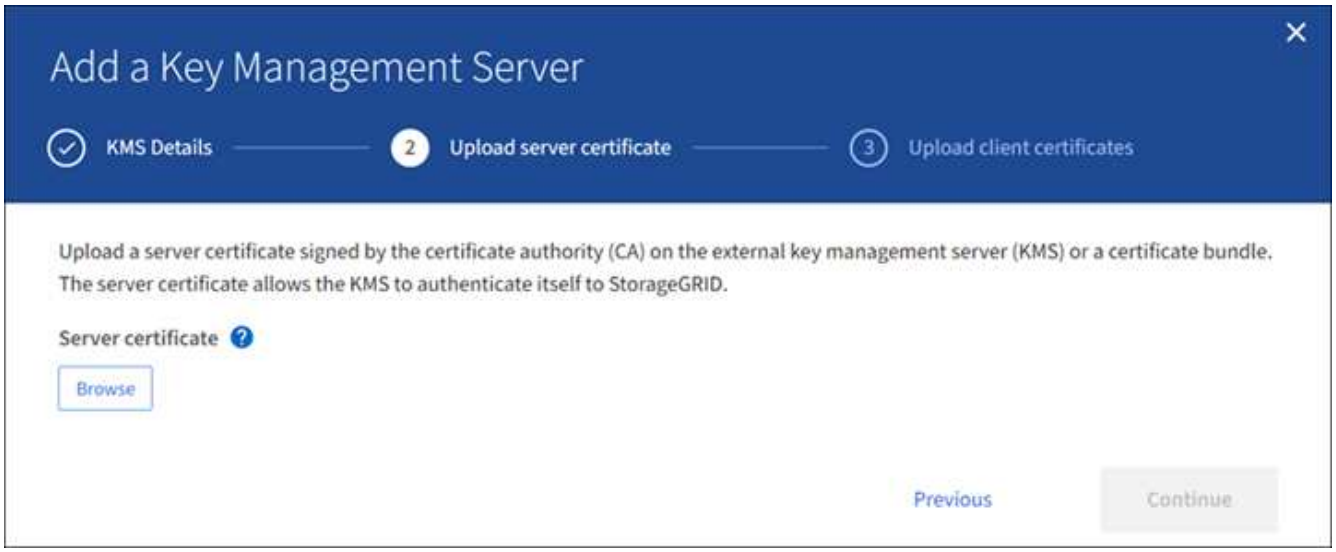
4. 如果您要設定 KMS 叢集、請選取 * 新增其他主機名稱 * 、為叢集中的每部伺服器新增主機名稱。
5. 選擇*繼續*。

步驟 **2** ：上傳伺服器憑證

在新增金鑰管理伺服器精靈的步驟 2 （上傳伺服器憑證）中、您可以上傳 KMS 的伺服器憑證（或憑證套件）。伺服器憑證可讓外部KMS驗證自己StorageGRID 以供驗證。

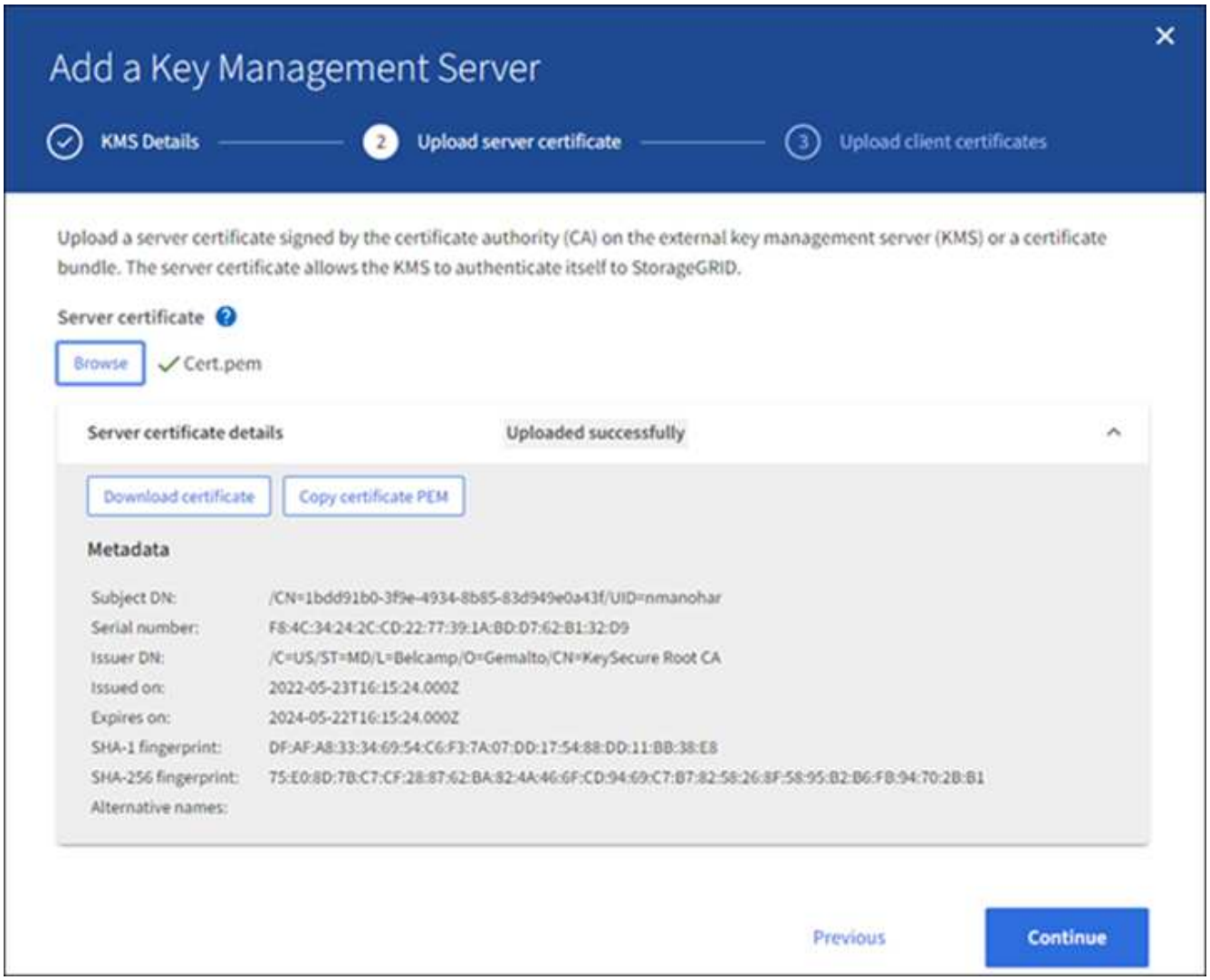
步驟

1. 從 * 步驟 2 （上傳伺服器憑證） * 中、瀏覽至儲存伺服器憑證或憑證套件的位置。



2. 上傳憑證檔案。

隨即顯示伺服器憑證中繼資料。



如果您上傳了憑證套件組合、每個憑證的中繼資料都會顯示在其各自的索引標籤上。

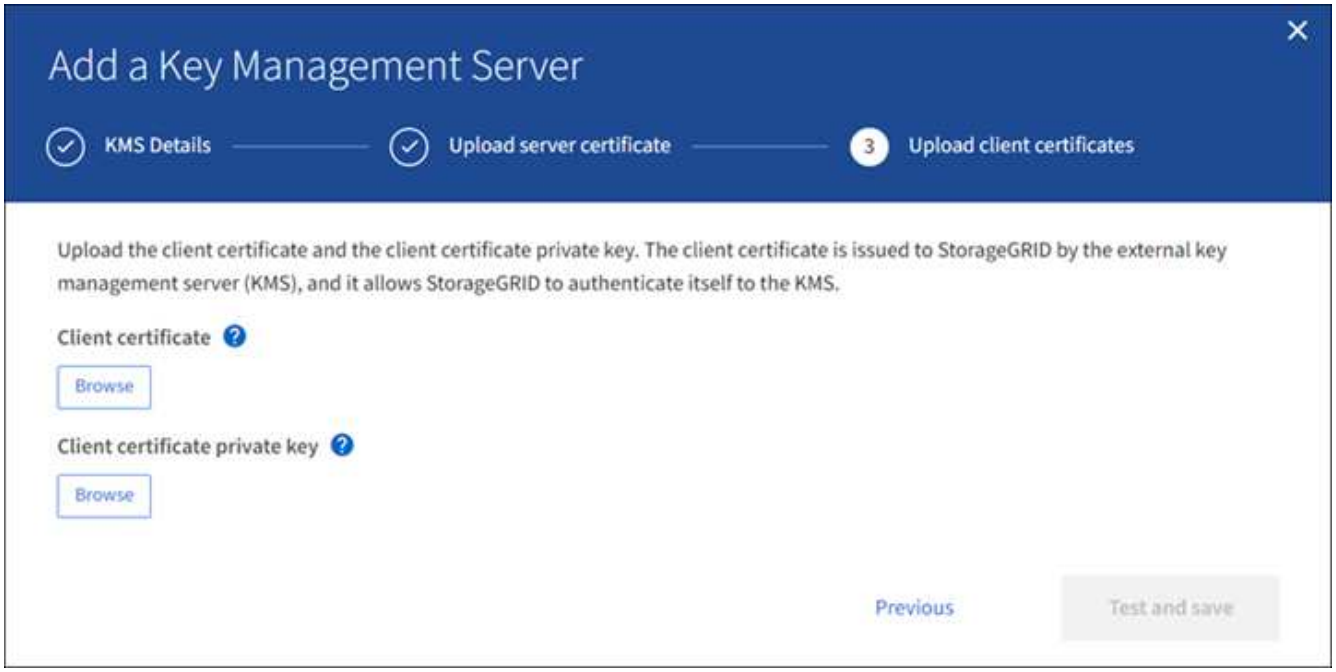
3. 選擇*繼續*。

步驟 **3** ：上傳用戶端憑證

在新增金鑰管理伺服器精靈的步驟 3 （上傳用戶端憑證）中、您可以上傳用戶端憑證和用戶端憑證私密金鑰。用戶端憑證StorageGRID 可讓支援驗證本身到KMS。

步驟

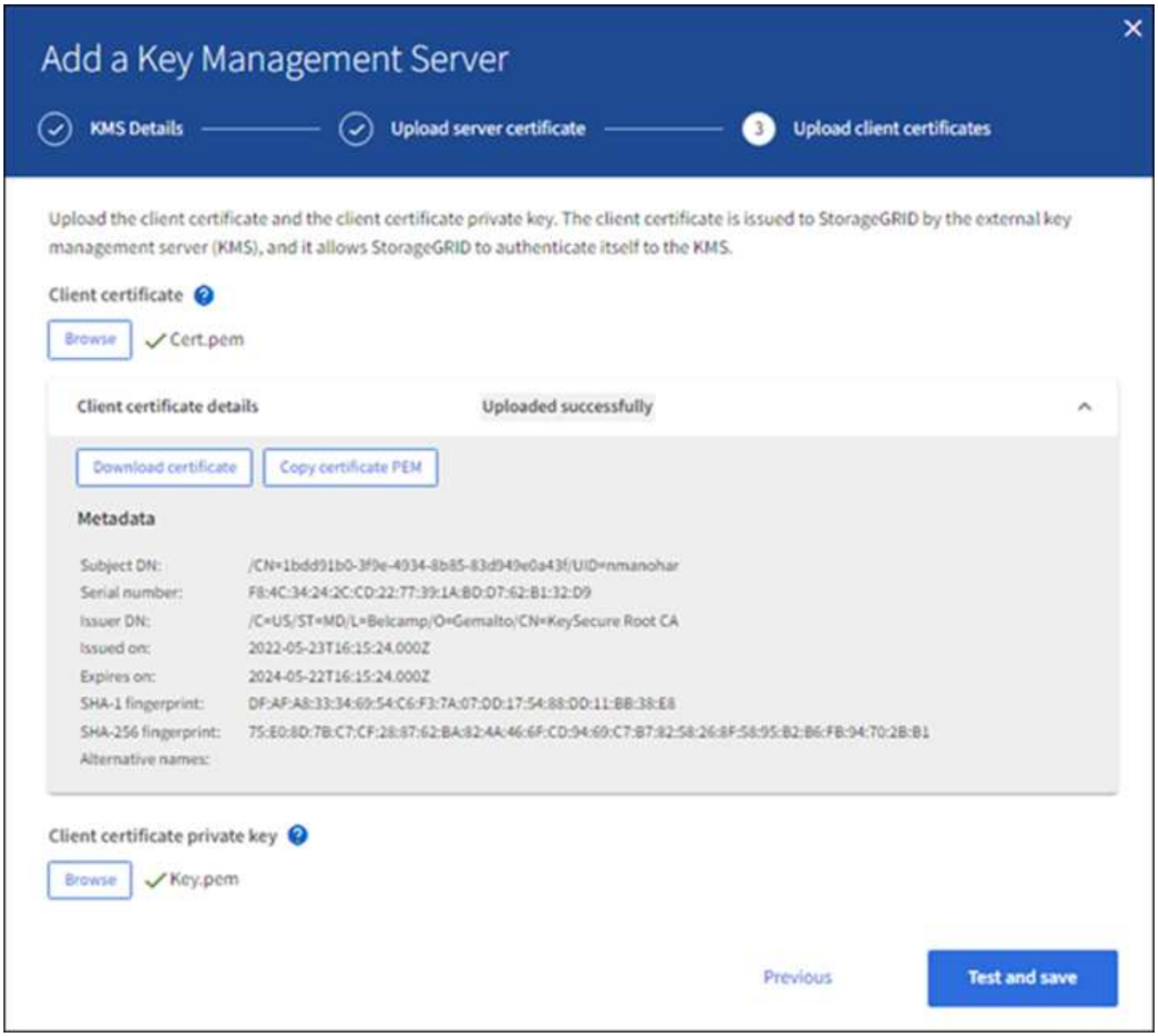
1. 從 * 步驟 3 （上傳用戶端憑證） * 、瀏覽至用戶端憑證的位置。



2. 上傳用戶端憑證檔案。

   此時會出現用戶端憑證中繼資料。

3. 瀏覽至用戶端憑證的私密金鑰位置。
4. 上傳私密金鑰檔案。



5. 選擇 * 測試並儲存 * 。

   測試金鑰管理伺服器與應用裝置節點之間的連線。如果所有連線都有效、且KMS上找到正確的金鑰、新的金鑰管理伺服器就會新增至金鑰管理伺服器頁面的表格。

   新增KMS之後、「金鑰管理伺服器」頁面上的憑證狀態會立即顯示為「未知」。可能需要StorageGRID 30分鐘才能取得每個憑證的實際狀態。您必須重新整理網頁瀏覽器、才能查看目前狀態。

6. 如果您選取 * 測試並儲存 * 時出現錯誤訊息、請檢閱訊息詳細資料、然後選取 * 確定 * 。

   例如、如果連線測試失敗、您可能會收到「無法處理的實體」錯誤。

7. 如果您需要儲存目前的組態而不測試外部連線、請選取 * 強制儲存 * 。

選取 * 強制儲存 * 會儲存 KMS 組態、但不會測試從每個應用裝置到該 KMS 的外部連線。如果組態發生問題、您可能無法重新啟動受影響站台已啟用節點加密的應用裝置節點。在問題解決之前、您可能無法存取資料。

8. 檢閱確認警告、如果您確定要強制儲存組態、請選取* OK *。

   系統會儲存KMS組態、但不會測試與KMS的連線。

檢視**KMS**詳細資料

您可以檢視StorageGRID 有關您的作業系統中每個金鑰管理伺服器（KMS）的資訊、包括伺服器和用戶端憑證的目前狀態。

步驟

1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   此時會出現金鑰管理伺服器頁面。組態詳細資料索引標籤會顯示任何已設定的金鑰管理伺服器。

2. 檢閱表格中每個KMS的資訊。

欄位	說明
KMS 名稱	KMS的描述性名稱。
金鑰名稱	KMS中的核心用戶端別名StorageGRID 。
管理的金鑰	與KMS相關的站台。StorageGRID 此欄位會顯示特定StorageGRID 的站台名稱、或*不由其他KMS管理的站台名稱（預設KMS）。*
主機名稱	KMS的完整網域名稱或IP位址。 如果有兩個金鑰管理伺服器的叢集、則會列出兩個伺服器的完整網域名稱或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的完整網域名稱或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 `10.10.10.10 and 2 others`。 若要檢視叢集中的所有主機名稱、請開啟 KMS 、然後選取 * 編輯 * 或 * 動作 * > * 編輯 * 。

欄位	說明
憑證過期	伺服器憑證、選用CA憑證和用戶端憑證的目前狀態：有效、過期、即將到期或不明。 • 注意： * 取得憑證過期更新可能需要 30 分鐘的 StorageGRID 時間。您必須重新整理網頁瀏覽器、才能查看目前值。

3. 如果「憑證過期」為「未知」、請等待長達 30 分鐘、然後重新整理您的網頁瀏覽器。

> 在您新增 KMS 之後、「金鑰管理伺服器」頁面上的憑證到期日會立即顯示為「未知」。可能需要StorageGRID 30分鐘才能取得每個憑證的實際狀態。您必須重新整理網頁瀏覽器、才能查看實際狀態。

4. 如果「憑證過期」欄顯示憑證已過期或即將過期、請盡快解決此問題。

   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 * 警示時、請記下每個警示的說明、然後執行建議的動作。

> 您必須盡快解決任何憑證問題、才能維持資料存取。

5. 若要檢視此 KMS 的憑證詳細資料、請從表格中選取 KMS 名稱。
6. 在 KMS 摘要頁面上、檢閱伺服器憑證和用戶端憑證的中繼資料和憑證 PEM 。視需要選取 * 編輯憑證 * 以新憑證取代憑證。

檢視加密節點

您可以在StorageGRID 啟用「節點加密」設定的支援功能系統中、檢視應用裝置節點的相關資訊。

步驟

1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   此時會出現「金鑰管理伺服器」頁面。「組態詳細資料」索引標籤會顯示任何已設定的金鑰管理伺服器。

2. 從頁面頂端、選取 * 加密節點 * 索引標籤。

   加密節點索引標籤會列出 StorageGRID 系統中已啟用 * 節點加密 * 設定的應用裝置節點。

3. 檢閱表格中每個應用裝置節點的資訊。

欄位	說明
節點名稱	應用裝置節點的名稱。
節點類型	節點類型：儲存設備、管理或閘道。

欄位	說明
網站	安裝節點的站台名稱。StorageGRID
KMS 名稱	用於節點的KMS描述性名稱。 如果沒有列出 KMS 、請選取組態詳細資料索引標籤以新增 KMS 。 "新增金鑰管理伺服器（KMS）"
金鑰UID	加密金鑰的唯一ID、用於加密及解密應用裝置節點上的資料。若要檢視整個金鑰 UID 、請將游標放在儲存格上方。 破折號（-）表示金鑰唯一碼未知、可能是因為應用裝置節點與KMS之間的連線問題。
狀態	KMS與應用裝置節點之間的連線狀態。如果節點已連線、時間戳記每30分鐘更新一次。變更KMS組態之後、連線狀態可能需要幾分鐘的時間才能更新。 *注意：*您必須重新整理網頁瀏覽器、才能看到新的值。

4. 如果「狀態」欄指出KMS問題、請立即解決問題。

   在一般KMS作業期間、狀態將*連線至KMS *。如果節點與網格中斷連線、則會顯示節點連線狀態（管理性關閉或未知）。

   其他狀態訊息則對應StorageGRID 於名稱相同的Ses姓名：

   - 無法載入kms組態
   - KMS連線錯誤
   - 找不到kms加密金鑰名稱
   - KMS加密金鑰旋轉失敗
   - KMS金鑰無法解密應用裝置磁碟區
   - 未設定公里

   執行這些警示的建議動作。

   您必須立即解決任何問題、確保資料受到完整保護。

編輯金鑰管理伺服器（KMS）

您可能需要編輯金鑰管理伺服器的組態、例如、如果憑證即將過期。

開始之前

- 您已檢閱 "使用金鑰管理伺服器的考量與要求"。

- 如果您打算更新選取的KMS網站、則表示您已檢閱 "變更網站KMS的考量事項"。
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有root存取權限。

步驟

1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   此時會出現「金鑰管理伺服器」頁面、並顯示所有已設定的金鑰管理伺服器。

2. 選取您要編輯的 KMS 、然後選取 * 動作 * > * 編輯 * 。

   您也可以在表格中選取 KMS 名稱、然後在 KMS 詳細資料頁面上選取 * 編輯 * 來編輯 KMS 。

3. 您也可以在「編輯金鑰管理伺服器」精靈的 * 步驟 1 （ KMS 詳細資料） * 中更新詳細資料。

欄位	說明
KMS 名稱	可協助您識別此KMS的描述性名稱。必須介於1到64個字元之間。
金鑰名稱	KMS中適用於該客戶端的確切金鑰別名StorageGRID 。必須介於1到255個字元之間。 在極少數情況下、您只需要編輯金鑰名稱即可。例如、如果在KMS中重新命名別名、或是先前金鑰的所有版本都已複製到新別名的版本歷程記錄、則必須編輯金鑰名稱。 切勿嘗試變更KMS的金鑰名稱（別名）來旋轉金鑰。而是更新KMS軟體中的金鑰版本來旋轉金鑰。若要從KMS存取先前使用過的所有金鑰版本（以及未來的任何金鑰版本）、必須使用相同的金鑰別名。StorageGRID如果您變更設定KMS的金鑰別名、StorageGRID 則可能無法解密您的資料。 "使用金鑰管理伺服器的考量與要求"
管理的金鑰	如果您正在編輯網站專屬的 KMS 、但尚未有預設的 KMS 、請選擇性地選取 * 「不是由其他 KMS 管理的網站」（預設 KMS ） * 。此選項會將網站專屬的 KMS 轉換成預設的 KMS 、適用於所有沒有專屬 KMS 的網站、以及新增至擴充中的任何網站。 • 注意： * 如果您正在編輯網站專屬的 KMS 、則無法選取其他網站。如果您正在編輯預設 KMS 、則無法選取特定網站。
連接埠	KMS伺服器用於金鑰管理互通性傳輸協定（KMIP）通訊的連接埠。預設為5696、即KMIP標準連接埠。

欄位	說明
主機名稱	KMS的完整網域名稱或IP位址。 • 注意： * 伺服器憑證的主體替代名稱（ SAN ）欄位必須包含您在此輸入的 FQDN 或 IP 位址。否則StorageGRID 、無法將無法連接至KMS或KMS叢集中的所有伺服器。

4. 如果您要設定 KMS 叢集、請選取 * 新增其他主機名稱 * 、為叢集中的每部伺服器新增主機名稱。
5. 選擇*繼續*。

   此時將顯示 Edit a Key Management Server （編輯金鑰管理伺服器）精靈的步驟 2 （上傳伺服器憑證）。
6. 如果您需要更換伺服器憑證、請選取*瀏覽*並上傳新檔案。
7. 選擇*繼續*。

   此時將顯示 Edit a Key Management Server （編輯金鑰管理伺服器）精靈的步驟 3 （上傳用戶端憑證）。
8. 如果您需要更換用戶端憑證和用戶端憑證私密金鑰、請選取*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與受影響站台上所有節點加密應用裝置節點之間的連線。如果所有節點連線均有效、且KMS上找到正確的金鑰、則金鑰管理伺服器會新增至金鑰管理伺服器頁面的表格。
10. 如果出現錯誤訊息、請檢閱訊息詳細資料、然後選取*確定*。

    例如、如果您為此KMS選取的站台已由其他KMS管理、或連線測試失敗、您可能會收到「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的組態、請選取 * 強制儲存 * 。

    > 選取 * 強制儲存 * 會儲存 KMS 組態、但不會測試從每個應用裝置到該 KMS 的外部連線。如果組態發生問題、您可能無法重新啟動受影響站台已啟用節點加密的應用裝置節點。在問題解決之前、您可能無法存取資料。

    系統會儲存KMS組態。
12. 檢閱確認警告、如果您確定要強制儲存組態、請選取* OK *。

    系統會儲存KMS組態、但不會測試與KMS的連線。

移除金鑰管理伺服器（**KMS**）

在某些情況下、您可能會想要移除金鑰管理伺服器。例如、如果您已停用站台、可能會想要移除站台專屬的KMS。

開始之前

- 您已檢閱 "使用金鑰管理伺服器的考量與要求"。

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

關於這項工作

在下列情況下、您可以移除KMS：

- 如果站台已停用、或站台中沒有啟用節點加密的應用裝置節點、您可以移除站台專屬的KMS。
- 如果每個已啟用節點加密功能的應用裝置節點已存在站台專屬KMS、您可以移除預設KMS。

步驟

1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   此時會出現「金鑰管理伺服器」頁面、並顯示所有已設定的金鑰管理伺服器。

2. 選取您要移除的 KMS 、然後選取 * 動作 * > * 移除 * 。

   您也可以選取表格中的 KMS 名稱、然後從 KMS 詳細資料頁面中選取 * 移除 * 來移除 KMS 。

3. 請確認下列各項正確無誤：
   - 您正在移除網站專屬 KMS 、此網站沒有啟用節點加密的應用裝置節點。
   - 您正在移除預設的 KMS 、但每個具有節點加密的站台都已存在特定站台的 KMS 。
4. 選擇*是*。

   KMS組態隨即移除。

管理Proxy設定

設定儲存Proxy設定

如果您使用的是平台服務或雲端儲存資源池、可以在儲存節點和外部S3端點之間設定不透明的Proxy。例如、您可能需要不透明的Proxy、才能將平台服務訊息傳送至外部端點、例如網際網路上的端點。

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"。

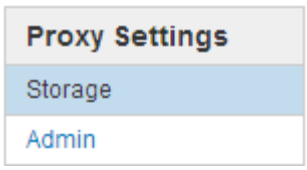
關於這項工作

您可以設定單一儲存Proxy的設定。

步驟

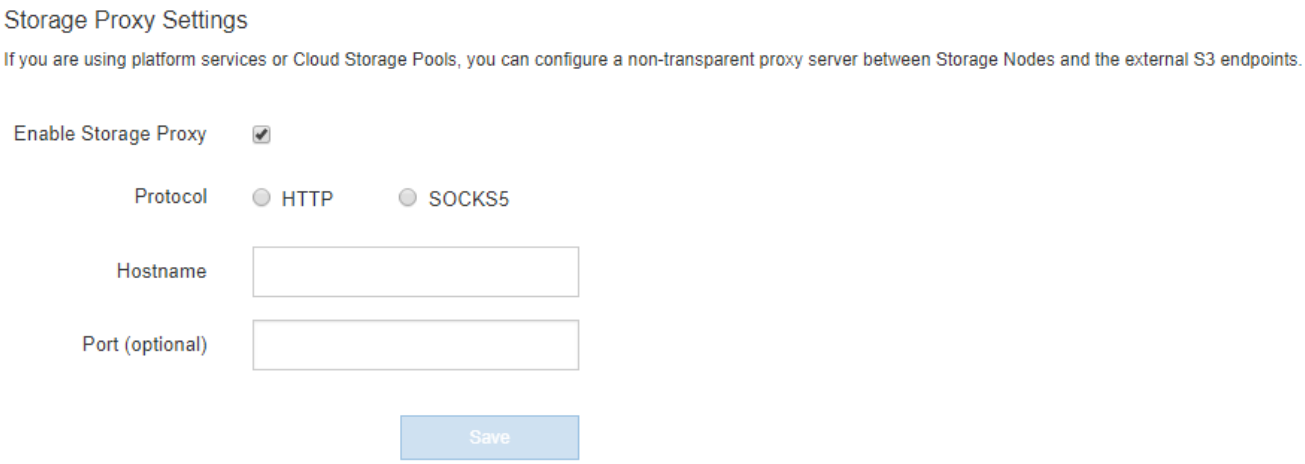
1. 選擇*組態*>*安全性*>* Proxy設定*。

   此時會出現「儲存Proxy設定」頁面。預設會在側邊列功能表中選取* Storage *。



2. 選中 **Enable Storage Proxy** 複選框。

   此時會顯示用於設定儲存Proxy的欄位。



3. 選取不透明儲存Proxy的傳輸協定。
4. 輸入Proxy伺服器的主機名稱或IP位址。
5. 或者、輸入用來連線至Proxy伺服器的連接埠。

   如果您使用傳輸協定的預設連接埠：HTTP為80、SOCKS5為1080、則可將此欄位留白。

6. 選擇*保存*。

   儲存Proxy之後、即可設定及測試平台服務或雲端儲存資源池的新端點。

   Proxy變更可能需要10分鐘才能生效。

7. 檢查Proxy伺服器的設定、確保StorageGRID 不會封鎖來自下列項目的平台服務相關訊息。

完成後

如果您需要停用儲存 Proxy 、請清除 * 啟用儲存 Proxy * 核取方塊、然後選取 * 儲存 * 。

相關資訊

- "平台服務的網路和連接埠"
- "使用ILM管理物件"

設定管理**Proxy**設定

如果您使用AutoSupport HTTP或HTTPS傳送不實訊息（請參閱 "設定AutoSupport 功能"）、您可以在管理節點和技術支援AutoSupport （例如、）之間設定不透明的Proxy伺服

器。

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

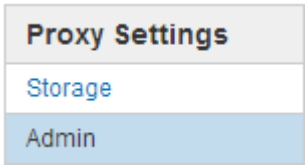
您可以設定單一管理Proxy的設定。

步驟

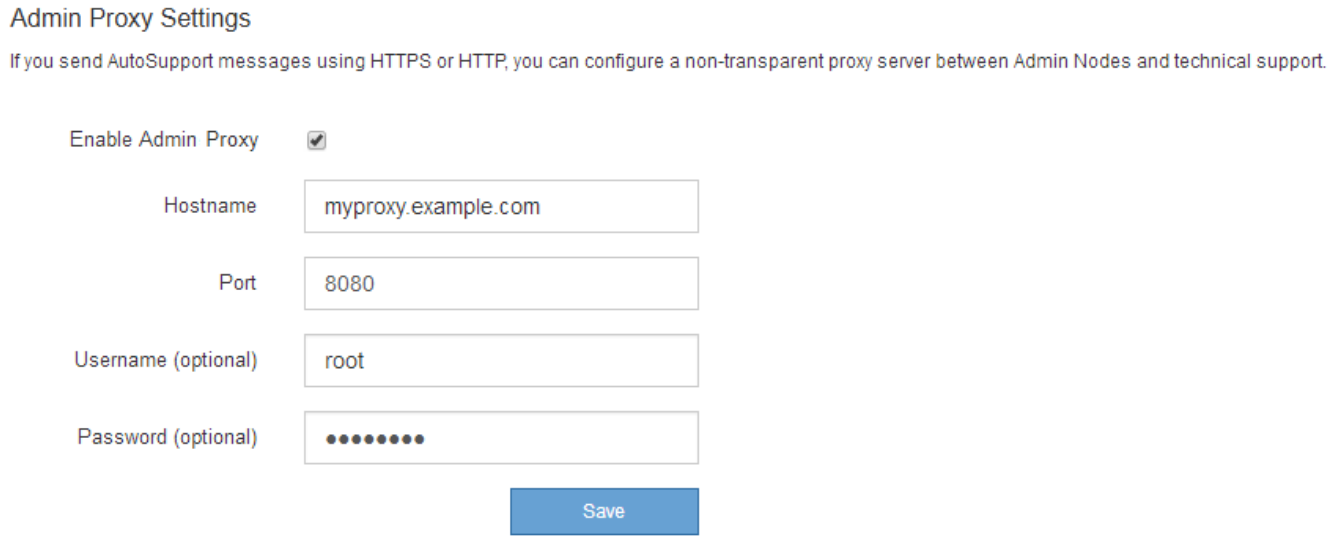
1. 選擇*組態*>*安全性*>* Proxy設定*。

   此時會出現「管理Proxy設定」頁面。預設會在側邊列功能表中選取* Storage *。

2. 從側欄功能表中、選取*管理*。



3. 選中 **Enable Admin Proxy** 複選框。



4. 輸入Proxy伺服器的主機名稱或IP位址。
5. 輸入用來連線至Proxy伺服器的連接埠。
6. 或者、輸入Proxy使用者名稱。

   如果您的Proxy伺服器不需要使用者名稱、請將此欄位留白。

7. 或者、輸入Proxy密碼。

   如果您的Proxy伺服器不需要密碼、請將此欄位留白。

8. 選擇*保存*。

   儲存管理Proxy之後、系統會設定管理節點與技術支援之間的Proxy伺服器。

   Proxy變更可能需要10分鐘才能生效。

9. 如果需要禁用代理，請清除 **Enable Admin Proxy** 複選框，然後選擇 **Save** 。

控制防火牆

控制外部防火牆的存取

您可以在外部防火牆開啟或關閉特定連接埠。

您可以StorageGRID 在外部防火牆開啟或關閉特定連接埠、以控制對使用者介面和API的存取。例如、除了使用其他方法來控制系統存取之外、您可能還想要防止租戶連線到防火牆的Grid Manager。

如果您想要設定 StorageGRID 內部防火牆、請參閱 "設定內部防火牆"。

連接埠	說明	如果連接埠已開啟...
443..	管理節點的預設HTTPS連接埠	Web瀏覽器和管理API用戶端可存取Grid Manager、Grid Management API、租戶管理程式和租戶管理API。 *附註：*連接埠443也用於部分內部流量。
8443.	管理節點上的受限網格管理器連接埠	• Web瀏覽器和管理API用戶端可使用HTTPS存取Grid Manager和Grid Management API。 • Web 瀏覽器和管理 API 用戶端無法存取租戶管理員或租戶管理 API 。 • 系統將拒絕內部內容的要求。
9443	管理節點上的受限租戶管理程式連接埠	• Web瀏覽器和管理API用戶端可使用HTTPS存取租戶管理程式和租戶管理API。 • Web 瀏覽器和管理 API 用戶端無法存取 Grid Manager 或 Grid Management API 。 • 系統將拒絕內部內容的要求。

單一登入（SSO）無法在受限網格管理器或租戶管理器連接埠上使用。如果您想要使用者透過單一登入進行驗證、則必須使用預設的HTTPS連接埠（443）。

相關資訊

- "登入Grid Manager"
- "建立租戶帳戶"

- "外部通訊"

管理內部防火牆控制

StorageGRID 在每個節點上都包含內部防火牆、可讓您控制對節點的網路存取、藉此增強網格的安全性。使用防火牆可防止網路存取所有連接埠、但您的特定網格部署所需的連接埠除外。您在「防火牆控制」頁面上所做的組態變更會部署到每個節點。

使用「防火牆控制」頁面上的三個索引標籤、自訂您網格所需的存取權限。

- * 貴賓位址清單 * ：使用此索引標籤可允許選取的存取已關閉的連接埠。您可以使用「管理外部存取」索引標籤、以 CIDR 表示法新增 IP 位址或子網路、以存取關閉的連接埠。
- * 管理外部存取 * ：使用此索引標籤關閉預設開啟的連接埠、或重新開啟先前關閉的連接埠。
- * 不受信任的用戶端網路 * ：使用此索引標籤指定節點是否信任來自用戶端網路的傳入流量。

  此索引標籤也提供選項、可指定設定不受信任用戶端網路時要開啟的其他連接埠。這些連接埠可讓您存取 Grid Manager 、 Tenant Manager 或兩者。

  此索引標籤上的設定會覆寫「管理外部存取」索引標籤中的設定。

  - 具有不受信任用戶端網路的節點只會接受在該節點上設定的負載平衡器端點連接埠（全域、節點介面和節點類型繫結端點）上的連線。
  - 在「不受信任的用戶端網路」標籤下開啟的其他連接埠會在所有不受信任的用戶端網路上開啟、即使沒有設定負載平衡器端點也一樣。
  - 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和所選的其他連接埠 _ 都是不受信任用戶端網路上唯一開放的連接埠 _ 。
  - 當信任時、所有在「管理外部存取」索引標籤下開啟的連接埠、以及在「用戶端網路」上開啟的任何負載平衡器端點都可以存取。

> 您在一個索引標籤上所做的設定可能會影響您在其他索引標籤上所做的存取變更。請務必檢查所有索引標籤上的設定、以確保您的網路運作方式符合預期。

若要設定內部防火牆控制、請參閱 "設定防火牆控制項"。

如需外部防火牆和網路安全性的詳細資訊、請參閱 "控制外部防火牆的存取"。

權限位址清單和管理外部存取索引標籤

「貴賓位址清單」標籤可讓您登錄一或多個 IP 位址、以存取已關閉的網格連接埠。「管理外部存取」索引標籤可讓您關閉外部存取、以存取選取的外部連接埠或所有開啟的外部連接埠（外部連接埠為非網格節點預設可存取的連接埠）。這兩個索引標籤通常可以一起使用、以自訂您需要的確切網路存取、以供網格使用。

> 預設情況下、特權 IP 位址沒有內部網格連接埠存取。

範例 1 ：使用跳躍主機來執行維護工作

假設您想要使用跨接主機（安全強化的主機）進行網路管理。您可以使用下列一般步驟：

1. 使用「貴賓位址清單」標籤新增跳躍主機的 IP 位址。
2. 使用「管理外部存取」索引標籤來封鎖所有連接埠。

> 在封鎖連接埠 443 和 8443 之前、請先新增權限 IP 位址。目前連線至封鎖連接埠的任何使用者（包括您）將無法存取 Grid Manager 、除非他們的 IP 位址已新增至「貴賓」位址清單。

儲存組態之後、除了跳躍主機之外、所有主機都會封鎖網格中管理節點上的所有外部連接埠。然後、您可以使用跳躍主機更安全地在網格上執行維護工作。

範例 2 ：限制存取 Grid Manager 和 Tenant Manager

假設基於安全考量、您想要限制對 Grid Manager 和 Tenant Manager 的存取。您可以使用下列一般步驟：

1. 使用「管理外部存取」索引標籤上的切換開關來封鎖連接埠 443 。
2. 使用「管理外部存取」索引標籤上的切換開關、即可存取連接埠 8443 。
3. 使用「管理外部存取」索引標籤上的切換開關、即可存取連接埠 9443 。

儲存組態後、主機將無法存取連接埠 443 、但仍可透過連接埠 8443 存取 Grid Manager 、並透過連接埠 9443 存取 Tenant Manager 。

範例 3 ：鎖定敏感連接埠

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 ）。您可以使用下列一般步驟：

1. 使用「貴賓」位址清單標籤、僅授予需要存取服務的主機存取權。
2. 使用「管理外部存取」索引標籤來封鎖所有連接埠。

> 在封鎖連接埠 443 和 8443 之前、請先新增權限 IP 位址。目前連線至封鎖連接埠的任何使用者（包括您）將無法存取 Grid Manager 、除非他們的 IP 位址已新增至「貴賓」位址清單。

儲存組態後、連接埠 22 和 SSH 服務將可用於權限位址清單上的主機。無論要求來自哪個介面、所有其他主機都將無法存取服務。

範例 4 ：停用對未使用服務的存取

在網路層級、您可以停用一些不想使用的服務。例如、如果您不提供 Swift 存取、請執行下列一般步驟：

1. 使用「管理外部存取」索引標籤上的切換開關來封鎖連接埠 18083 。
2. 使用「管理外部存取」索引標籤上的切換開關來封鎖連接埠 18085 。

儲存組態後、儲存節點不再允許 Swift 連線、但仍允許存取未封鎖連接埠上的其他服務。

不受信任的用戶端網路索引標籤

如果您使用的是用戶端網路、只能在明確設定的端點或您在此索引標籤上選取的其他連接埠上接受傳入用戶端流量、以協助保護 StorageGRID 免受惡意攻擊。

依預設、每個網格節點上的用戶端網路為_truste_。也就是說、根據預設、 StorageGRID 會信任所有網格節點的傳入連線 "可用的外部連接埠"。

您可以StorageGRID 指定每個節點上的用戶端網路為_不受信任_、藉此減少對您的作業系統進行惡意攻擊的威脅。如果節點的用戶端網路不受信任、則節點只接受明確設定為負載平衡器端點的連接埠傳入連線、以及使用「防火牆控制」頁面上的「不受信任的用戶端網路」索引標籤指定的任何其他連接埠。請參閱 "設定負載平衡器端點" 和 "設定防火牆控制項"。

範例**1**：閘道節點僅接受**HTTPS S3**要求

假設您希望閘道節點拒絕用戶端網路上除HTTPS S3要求以外的所有傳入流量。您可以執行下列一般步驟：

1. 從 "負載平衡器端點" 頁面中、在連接埠 443 上、透過 HTTPS 為 S3 設定負載平衡器端點。
2. 在「防火牆控制」頁面中、選取「不受信任」、以指定「閘道節點」上的「用戶端網路」不可信任。

儲存組態之後、除了連接埠443上的HTTPS S3要求和ICMP回應（ping）要求之外、閘道節點用戶端網路上的所有傳入流量都會捨棄。

範例**2**：儲存節點傳送**S3**平台服務要求

假設您想要從儲存節點啟用輸出 S3 平台服務流量、但想要防止任何傳入連線到用戶端網路上的該儲存節點。您可以執行以下一般步驟：

- 從「防火牆控制」頁面的「不受信任的用戶端網路」索引標籤、指出儲存節點上的用戶端網路不受信任。

儲存組態後、儲存節點將不再接受用戶端網路上的任何傳入流量、但仍會繼續允許傳出要求至設定的平台服務目的地。

範例 **3** ：將網格管理程式的存取限制在子網路上

假設您只想在特定子網路上允許 Grid Manager 存取。您可以執行下列步驟：

1. 將管理節點的用戶端網路連接至子網路。
2. 使用不受信任的用戶端網路索引標籤、將用戶端網路設定為不受信任。
3. 在索引標籤的 * 「在不受信任的用戶端網路上開啟的其他連接埠」區段中、新增連接埠 443 或 8443 。
4. 使用管理外部存取索引標籤來封鎖所有外部連接埠（無論是否為該子網路以外的主機設定了權限 IP 位址）。

儲存組態之後、只有指定子網路上的主機才能存取 Grid Manager 。所有其他主機都會遭到封鎖。

設定內部防火牆

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

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已檢閱中的資訊 "管理防火牆控制" 和 "網路準則"。
- 如果您希望管理節點或閘道節點僅接受明確設定的端點上的傳入流量、則表示您已定義負載平衡器端點。

變更用戶端網路的組態時、如果尚未設定負載平衡器端點、現有的用戶端連線可能會失敗。

關於這項工作

StorageGRID 在每個節點上都有內部防火牆、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」索引標籤來開啟或關閉預設在 Grid Network 、 Admin Network 和 Client Network 上開啟的連接埠。您也可以建立權限 IP 位址清單、以存取已關閉的網格連接埠。如果您使用的是用戶端網路、您可以指定節點是否信任來自用戶端網路的傳入流量、也可以設定用戶端網路上特定連接埠的存取。

將開放給網格外部 IP 位址的連接埠數量限制為只有絕對必要的連接埠數量、可增強網格的安全性。您可以使用三個防火牆控制索引標籤上的每個設定、確保只開啟所需的連接埠。

如需使用防火牆控制項的詳細資訊、包括範例、請參閱 "管理防火牆控制"。

如需外部防火牆和網路安全性的詳細資訊、請參閱 "控制外部防火牆的存取"。

存取防火牆控制

步驟

1. 選擇 * 組態 * > * 安全性 * > * 防火牆控制 * 。

   此頁面上的三個索引標籤如所述 "管理防火牆控制"。

2. 選取任何索引標籤以設定防火牆控制項。

   您可以依任何順序使用這些索引標籤。您在一個索引標籤上設定的組態不會限制您可以在其他索引標籤上執行的動作；不過、您在一個索引標籤上所做的組態變更可能會變更在其他索引標籤上設定的連接埠行為。

特殊權限位址清單

您可以使用「貴賓」位址清單標籤、將預設關閉或由「管理外部存取」標籤上的設定關閉的連接埠、授予主機存取權。

預設情況下、特權 IP 位址和子網路沒有內部網格存取。此外、即使在「管理外部存取」索引標籤中遭到封鎖、仍可存取負載平衡器端點和在「貴賓」位址清單索引標籤中開啟的其他連接埠。

「貴賓」位址清單標籤上的設定無法覆寫「不受信任的用戶端網路」標籤上的設定。

步驟

1. 在「貴賓位址清單」標籤上、輸入您要授予封閉連接埠存取權的位址或 IP 子網路。
2. 您也可以選擇 * 以 CIDR 表示法新增其他 IP 位址或子網路 * 來新增其他的特殊權限用戶端。

   將盡可能少的位址新增至權限清單。

3. （可選）選擇 * 允許特權 IP 地址訪問 StorageGRID 內部端口 * 。請參閱 "內部連接埠StorageGRID"。

   此選項會移除內部服務的某些保護。如果可能、請將其停用。

4. 選擇*保存*。

管理外部存取

在「管理外部存取」索引標籤中關閉連接埠時、除非您將 IP 位址新增至特殊權限位址清單、否則任何非網格 IP 位址都無法存取連接埠。您只能關閉預設開啟的連接埠、而且只能開啟已關閉的連接埠。

「管理外部存取」索引標籤上的設定無法覆寫「不受信任的用戶端網路」索引標籤上的設定。例如、如果節點不受信任、則即使在「管理外部存取」索引標籤上開啟連接埠 SSH/22 、用戶端網路上的連接埠 SSH/22 也會遭到封鎖。「不受信任的用戶端網路」標籤上的設定會覆寫用戶端網路上的關閉連接埠（例如 443 、 8443 、 9443 ）。

步驟

1. 選取 * 管理外部存取 * 。索引標籤會顯示一個表格、其中包含網格中節點的所有外部連接埠（預設為非網格節點可存取的連接埠）。
2. 使用下列選項設定您要開啟和關閉的連接埠：
   - 使用每個連接埠旁的切換開關來開啟或關閉選取的連接埠。
   - 選取 * 開啟所有顯示的連接埠 * 以開啟表格中列出的所有連接埠。
   - 選取 * 關閉所有顯示的連接埠 * 以關閉表格中列出的所有連接埠。

   如果您關閉 Grid Manager 連接埠 443 或 8443 、除非已將目前連線至封鎖連接埠的任何使用者（包括您）的 IP 位址新增至「貴賓」位址清單、否則他們將無法存取 Grid Manager 。

   使用表格右側的捲軸、確定您已檢視所有可用的連接埠。使用搜尋欄位、輸入連接埠編號、以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，如果您輸入 **2** ，則會顯示字串 "2" 做為其名稱一部分的所有連接埠。

3. 選擇*保存*

不受信任的用戶端網路

如果節點的用戶端網路不受信任、則節點只接受設定為負載平衡器端點的連接埠上的傳入流量、以及您在此索引標籤上選取的其他連接埠（選擇性）。您也可以使用此索引標籤來指定擴充中新增節點的預設設定。

如果尚未設定負載平衡器端點、現有的用戶端連線可能會失敗。

您在 * 不受信任的用戶端網路 * 標籤上所做的組態變更會覆寫 * 管理外部存取 * 標籤上的設定。

步驟

1. 選取 * 不受信任的用戶端網路 * 。
2. 在 Set New Node Default （設定新節點預設值）區段中、指定在擴充程序中將新節點新增至網格時的預設設定值。
   - * Trusted * （預設值）：當節點新增至擴充時、其 Client Network 會受到信任。
   - 不受信任：在擴充中新增節點時、其用戶端網路不受信任。

   視需要、您可以返回此索引標籤、變更特定新節點的設定。

此設定不會影響StorageGRID 到您的不完善系統中現有的節點。

3. 使用下列選項來選取節點、這些節點只能在明確設定的負載平衡器端點或其他選取的連接埠上允許用戶端連線：

   - 選取 * 不信任顯示的節點 * 、將表格中顯示的所有節點新增至「不受信任的用戶端網路」清單。
   - 選取 * 信任顯示的節點 * 、將表格中顯示的所有節點從「不受信任的用戶端網路」清單中移除。
   - 使用每個連接埠旁邊的切換、將所選節點的用戶端網路設為信任或不信任。

   例如、您可以選取 * 在顯示的節點上不信任 * 、將所有節點新增至「不信任的用戶端網路」清單、然後使用個別節點旁的切換、將該單一節點新增至「信任的用戶端網路」清單。

   使用表格右側的捲軸、確定您已檢視所有可用的節點。使用搜尋欄位輸入節點名稱、即可尋找任何節點的設定。您可以輸入部分名稱。例如、如果您輸入 * GW* 、則會顯示字串 "Gw" 做為其名稱一部分的所有節點。

4. 您也可以選擇在不受信任的用戶端網路上開啟的任何其他連接埠。這些連接埠可讓您存取 Grid Manager 、 Tenant Manager 或兩者。

   例如、您可能想要使用此選項、以確保可在用戶端網路上存取 Grid Manager 進行維護。

   這些附加連接埠會在用戶端網路上開啟、無論它們是否在「管理外部存取」標籤中關閉。

5. 選擇*保存*。

   新的防火牆設定會立即套用及強制執行。如果尚未設定負載平衡器端點、現有的用戶端連線可能會失敗。

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。