配置金鑰管理伺服器

StorageGRID software

NetApp
May 29, 2026

目錄

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)"。

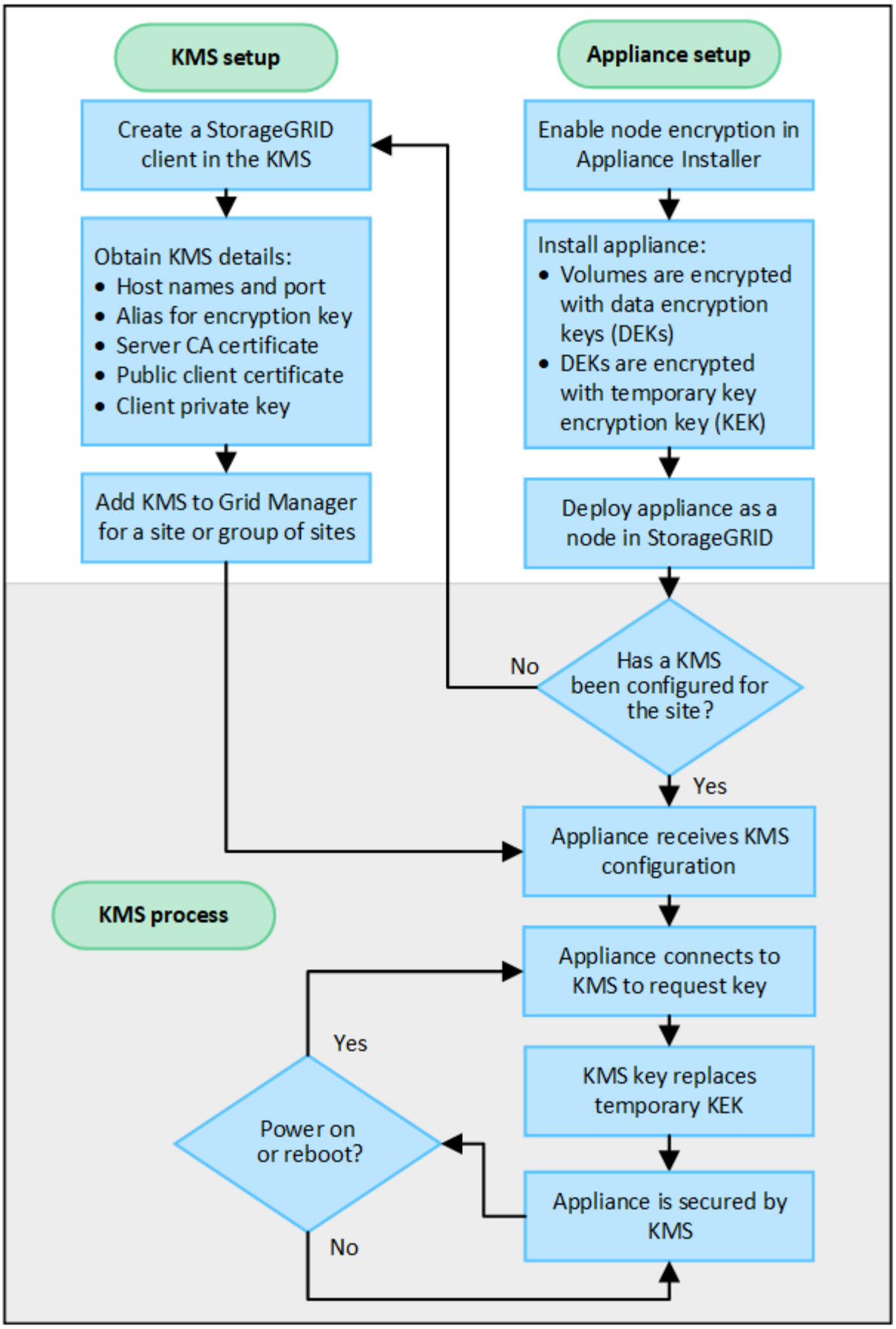
您可以使用一個或多個金鑰管理伺服器來管理在安裝期間啟用了「節點加密」設定的任何StorageGRID裝置節點的節點加密金鑰。透過將這些設備節點與金鑰管理伺服器結合使用，即使設備從資料中心移除，您也可以保護資料。裝置磁碟區加密後，除非節點可以與 KMS 通信，否則您無法存取裝置上的任何資料。

> 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。

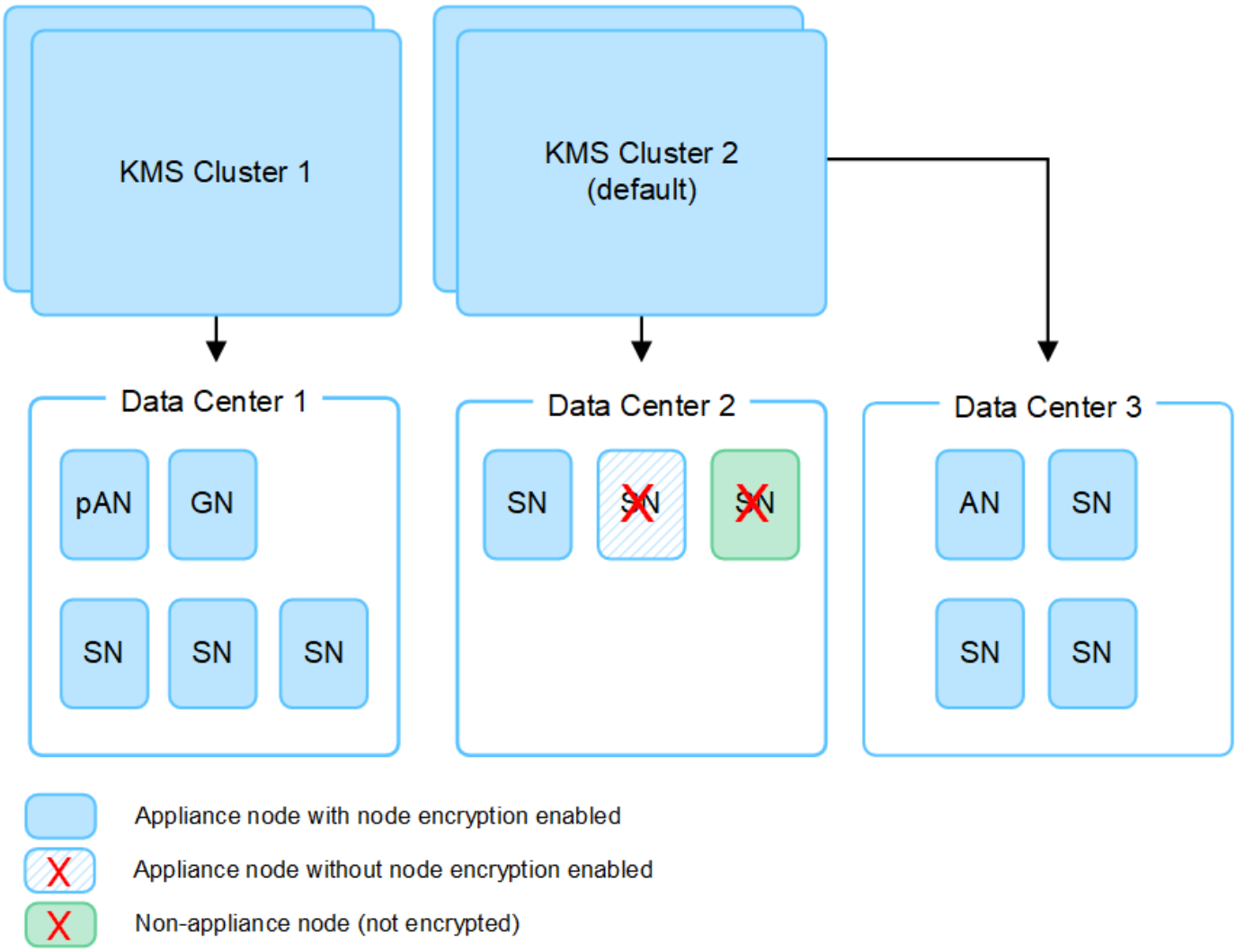
我需要多少個金鑰管理伺服器？

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。

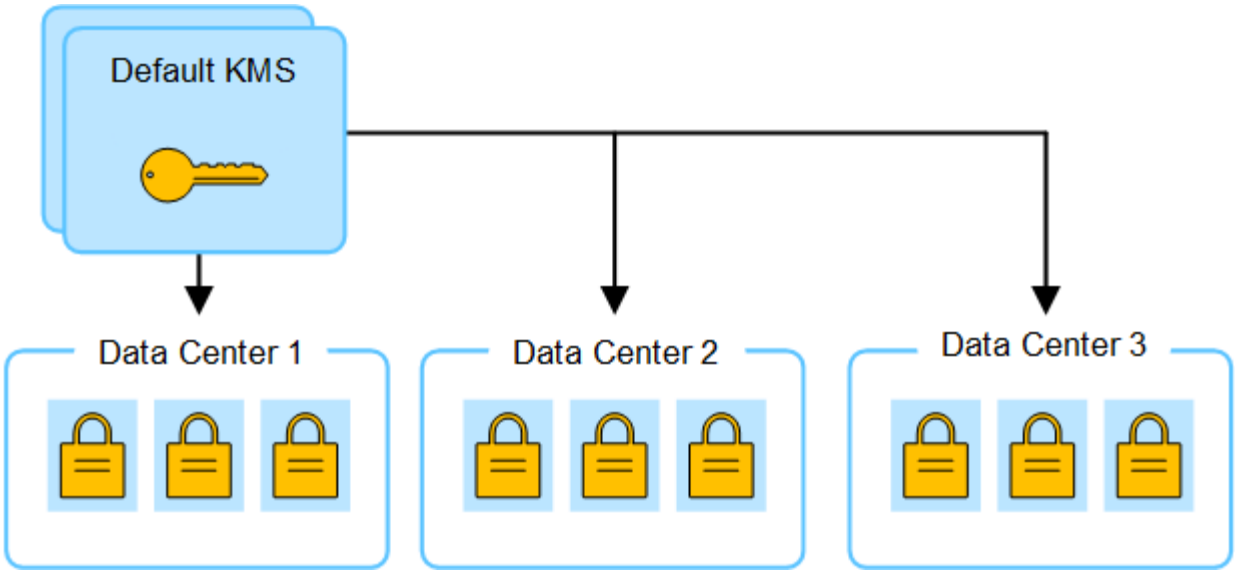
更改站點 **KMS** 的注意事項

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。

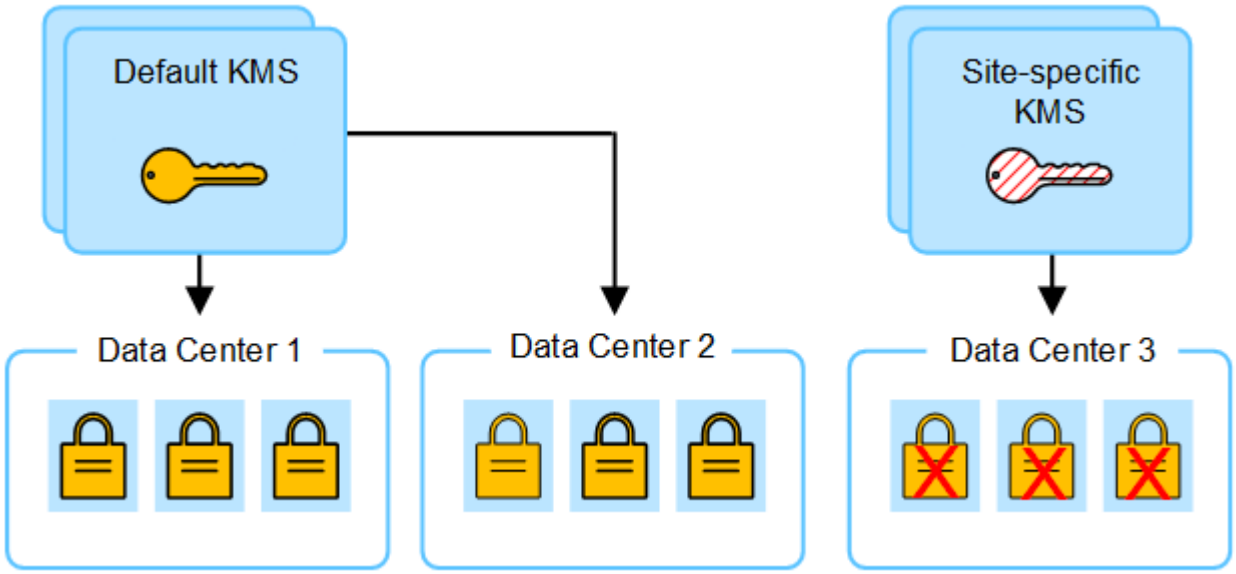
如果您變更網站所使用的 KMS，則必須確保該網站上先前加密的裝置節點可以使用儲存在新 KMS 上的金鑰解密。在某些情況下，您可能需要將目前版本的加密金鑰從原始 KMS 複製到新的 KMS。您必須確保 KMS 具有正確的金鑰來解密網站上的加密裝置節點。

例如：

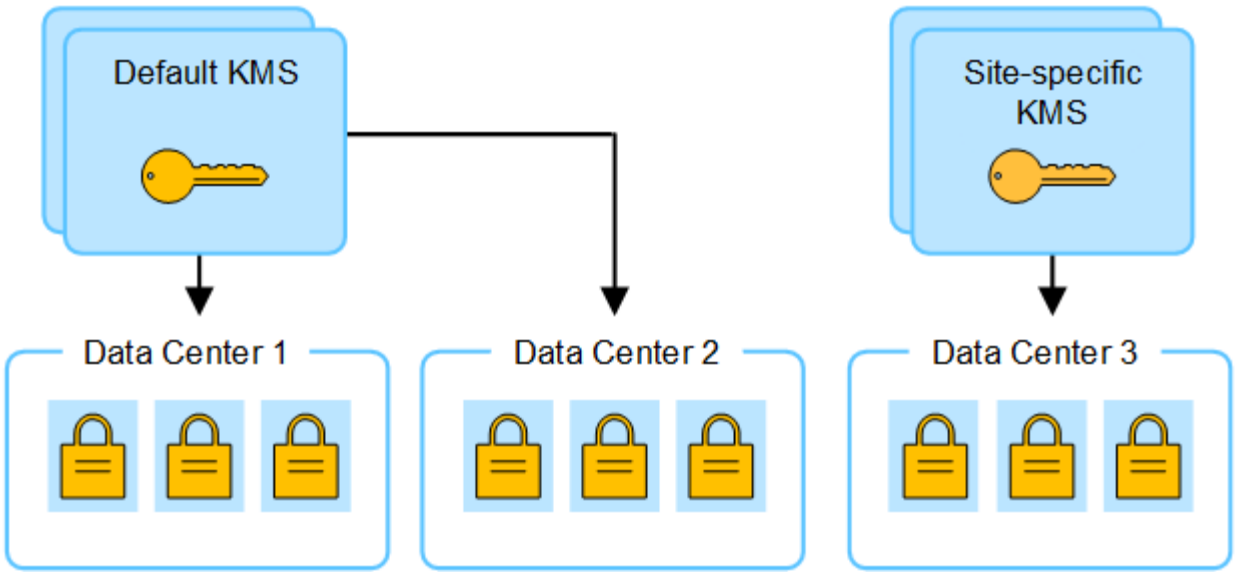
1. 您最初配置一個適用於所有沒有專用 KMS 的網站的預設 KMS。
2. 儲存 KMS 後，所有啟用了 節點加密 設定的裝置節點都會連接到 KMS 並要求加密金鑰。此金鑰用於加密所有網站的設備節點。也必須使用相同的金鑰來解密這些裝置。



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。