設定金鑰管理伺服器
StorageGRID 11.7

NetApp
April 12, 2024

目錄

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。

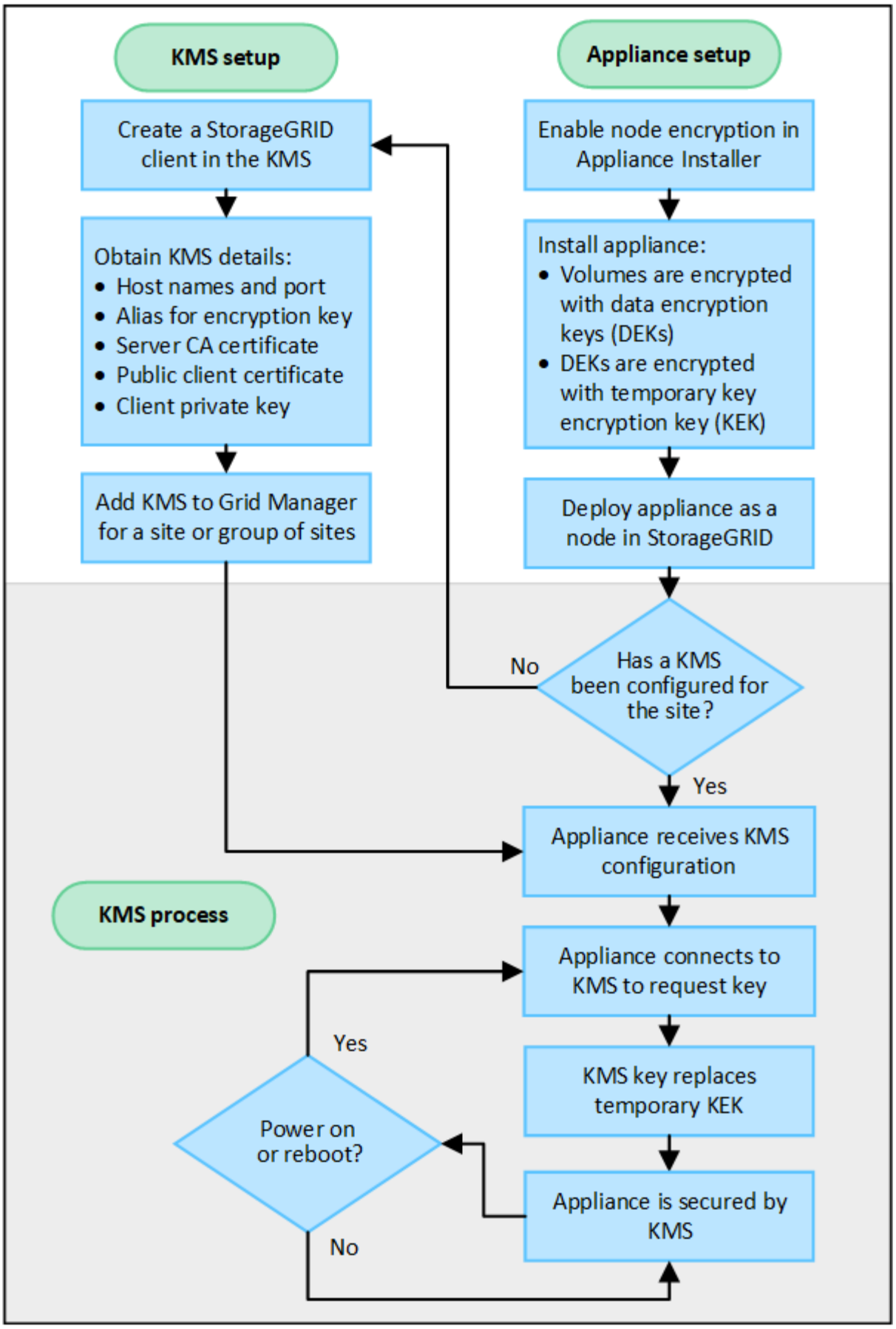
您可以使用一或多個金鑰管理伺服器、來管理StorageGRID 安裝期間啟用*節點加密*設定的任何節點的節點加密金鑰。即使從資料中心移除應用裝置、將關鍵管理伺服器與這些應用裝置節點搭配使用、也能保護資料。應用裝置磁碟區加密後、除非節點可以與 KMS 通訊、否則您無法存取應用裝置上的任何資料。

> 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。

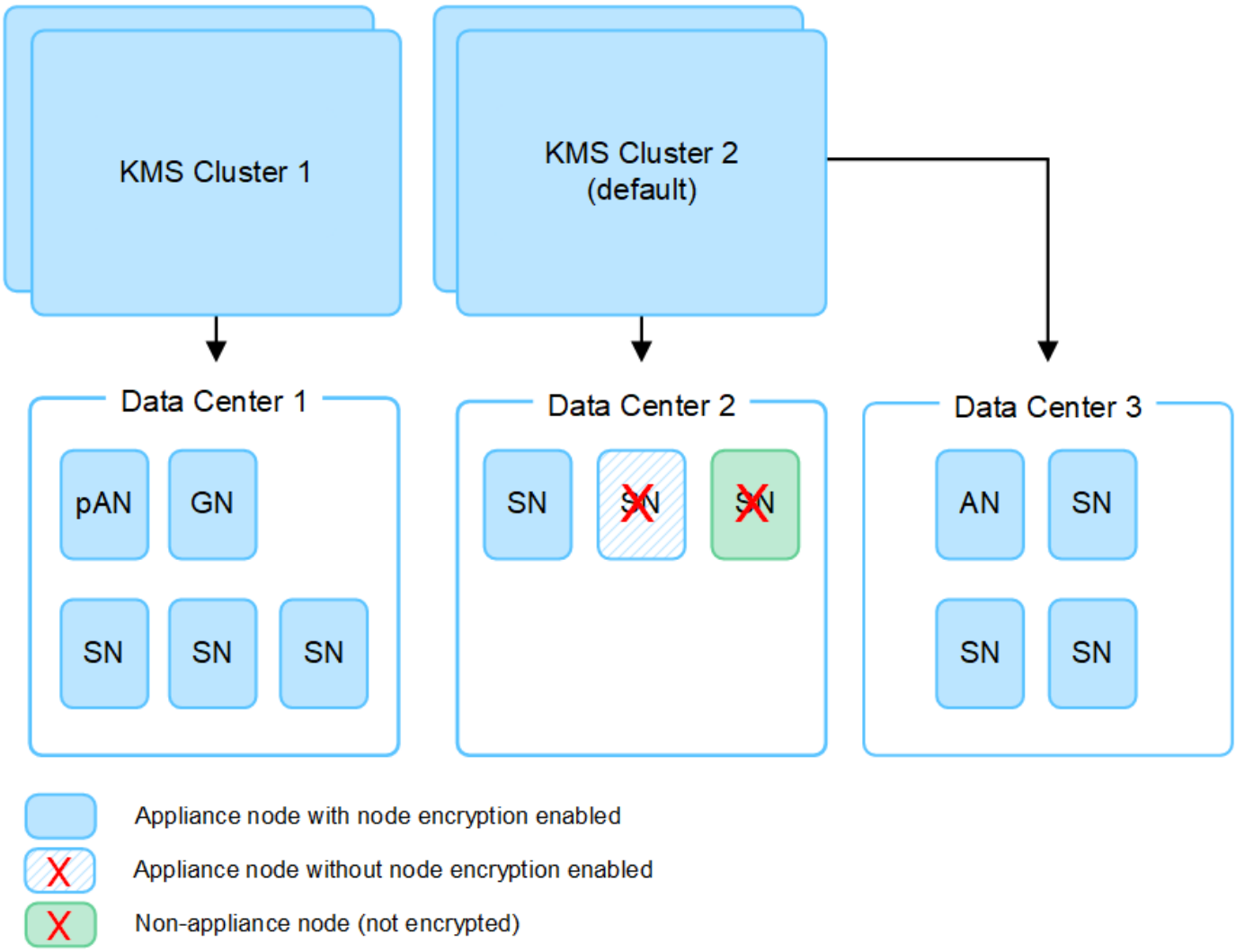
我需要多少個關鍵管理伺服器？

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。

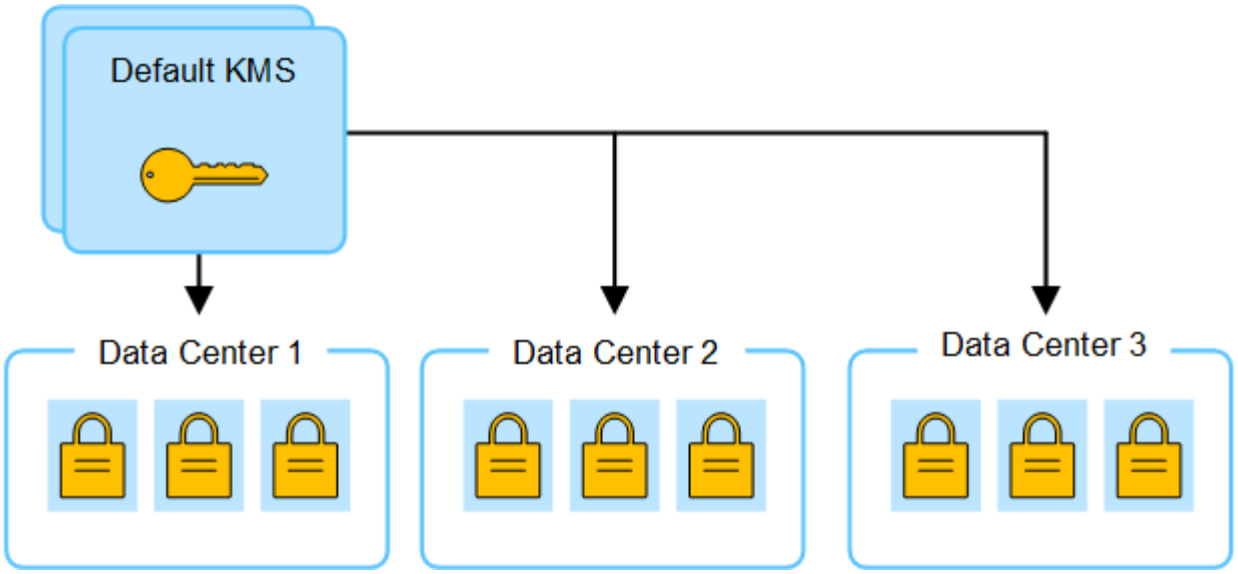
變更網站KMS的考量事項

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。

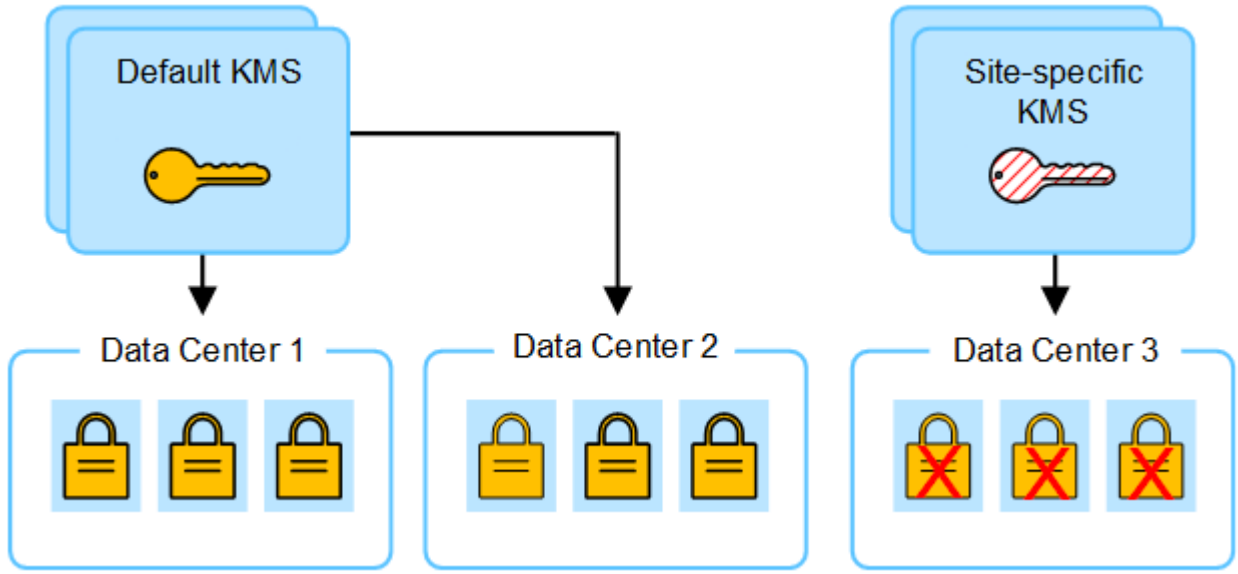
如果您變更站台使用的KMS、則必須確保該站台先前加密的應用裝置節點可以使用儲存在新KMS上的金鑰來解密。在某些情況下、您可能需要將目前版本的加密金鑰從原始KMS複製到新的KMS。您必須確保KMS擁有正確的金鑰、以便在站台上解密加密的應用裝置節點。

例如：

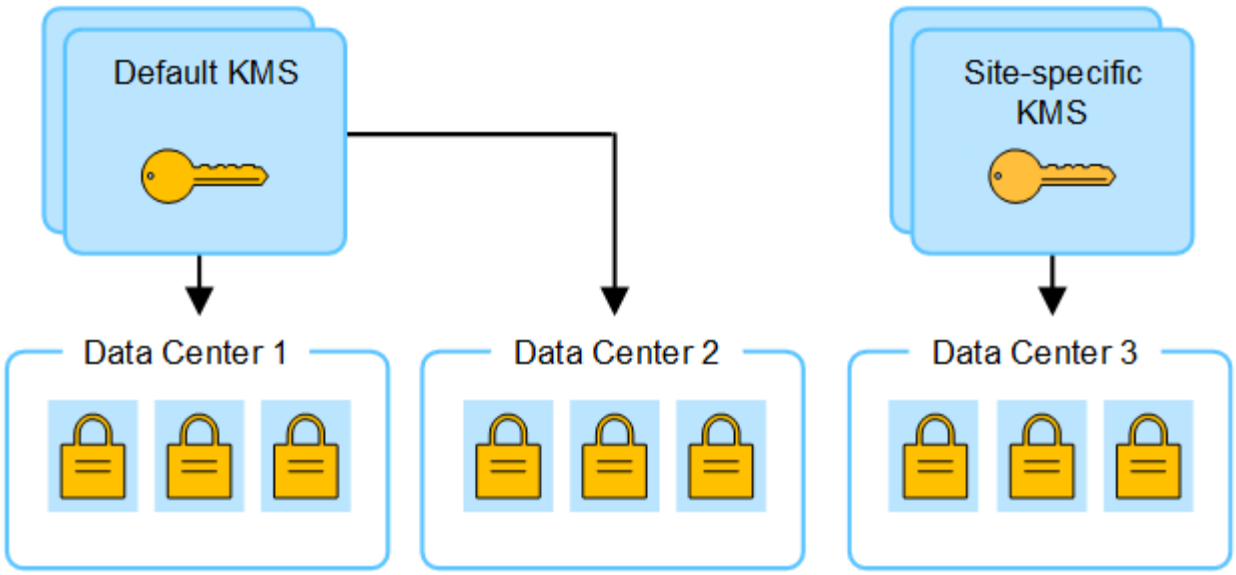
1. 您一開始會設定預設 KMS 、以套用至所有沒有專屬 KMS 的網站。
2. 儲存KMS時、所有啟用「節點加密」設定的應用裝置節點都會連線至KMS、並要求加密金鑰。此金鑰用於加密所有站台的應用裝置節點。此相同金鑰也必須用於解密這些應用裝置。



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。

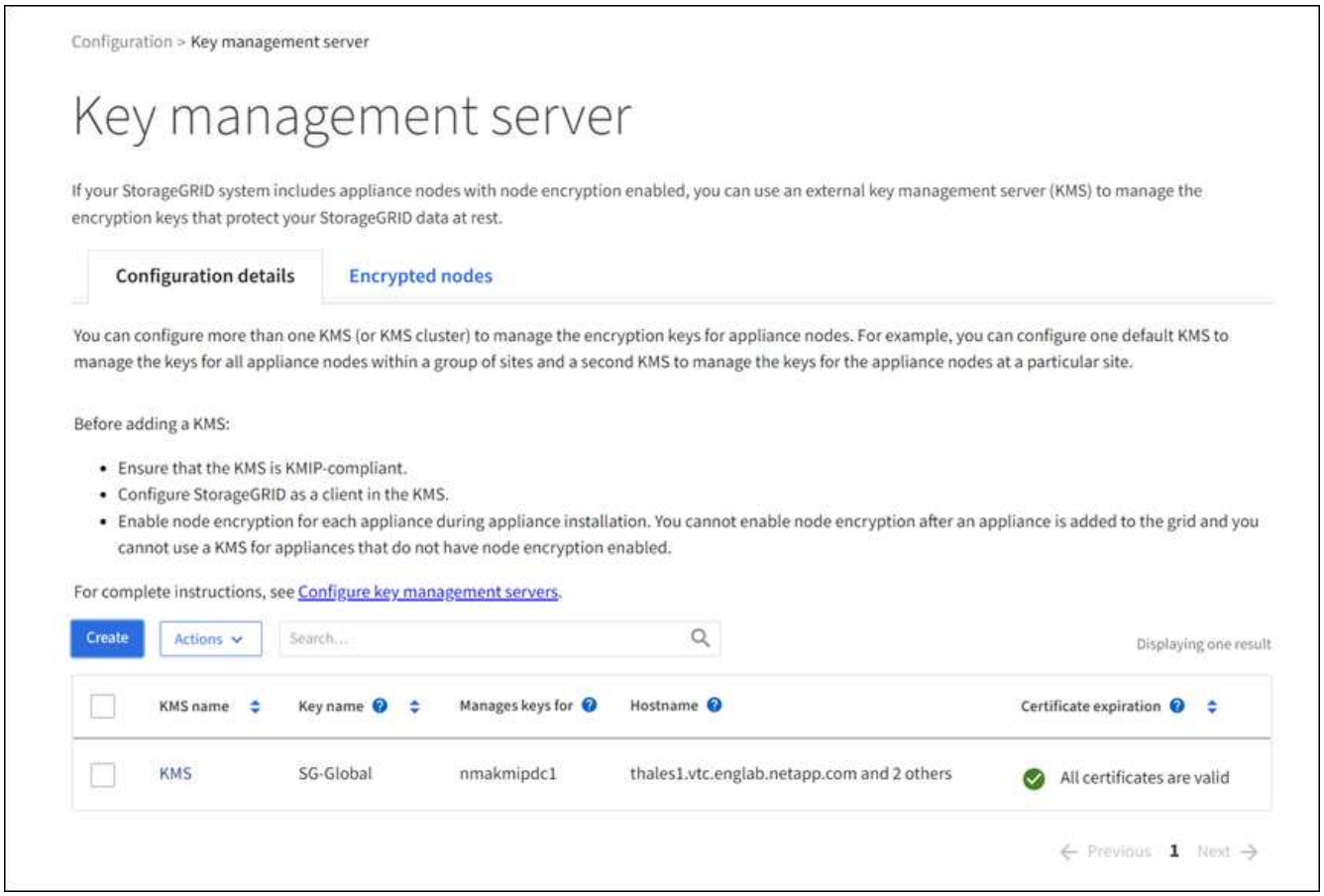
步驟 1 ： KMS 詳細資料

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

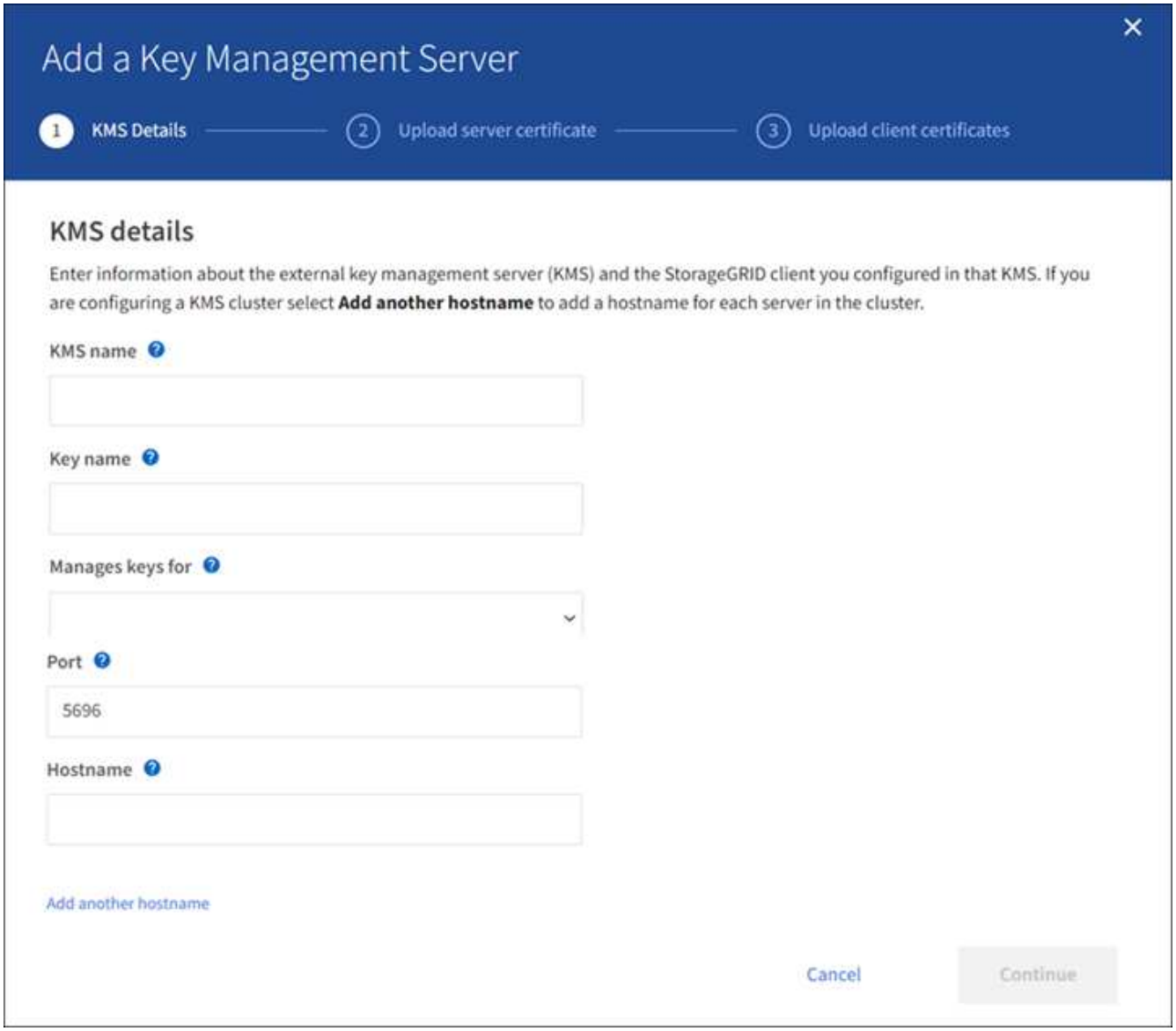
1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   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。

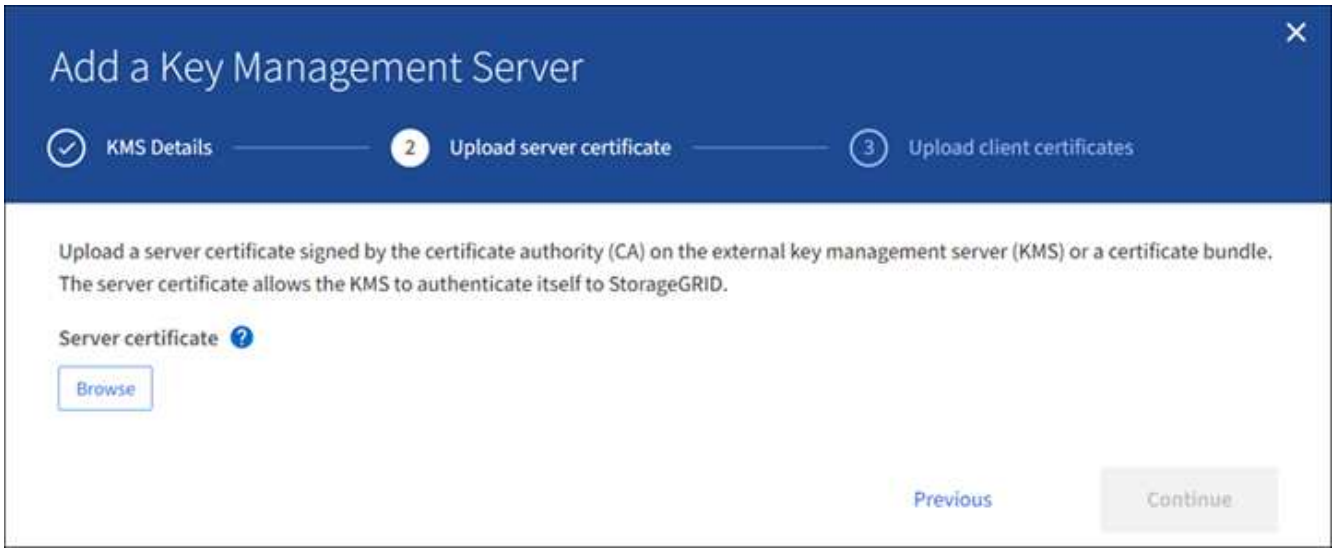
4. 如果您要設定 KMS 叢集、請選取 * 新增其他主機名稱 * 、為叢集中的每部伺服器新增主機名稱。
5. 選擇*繼續*。

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。

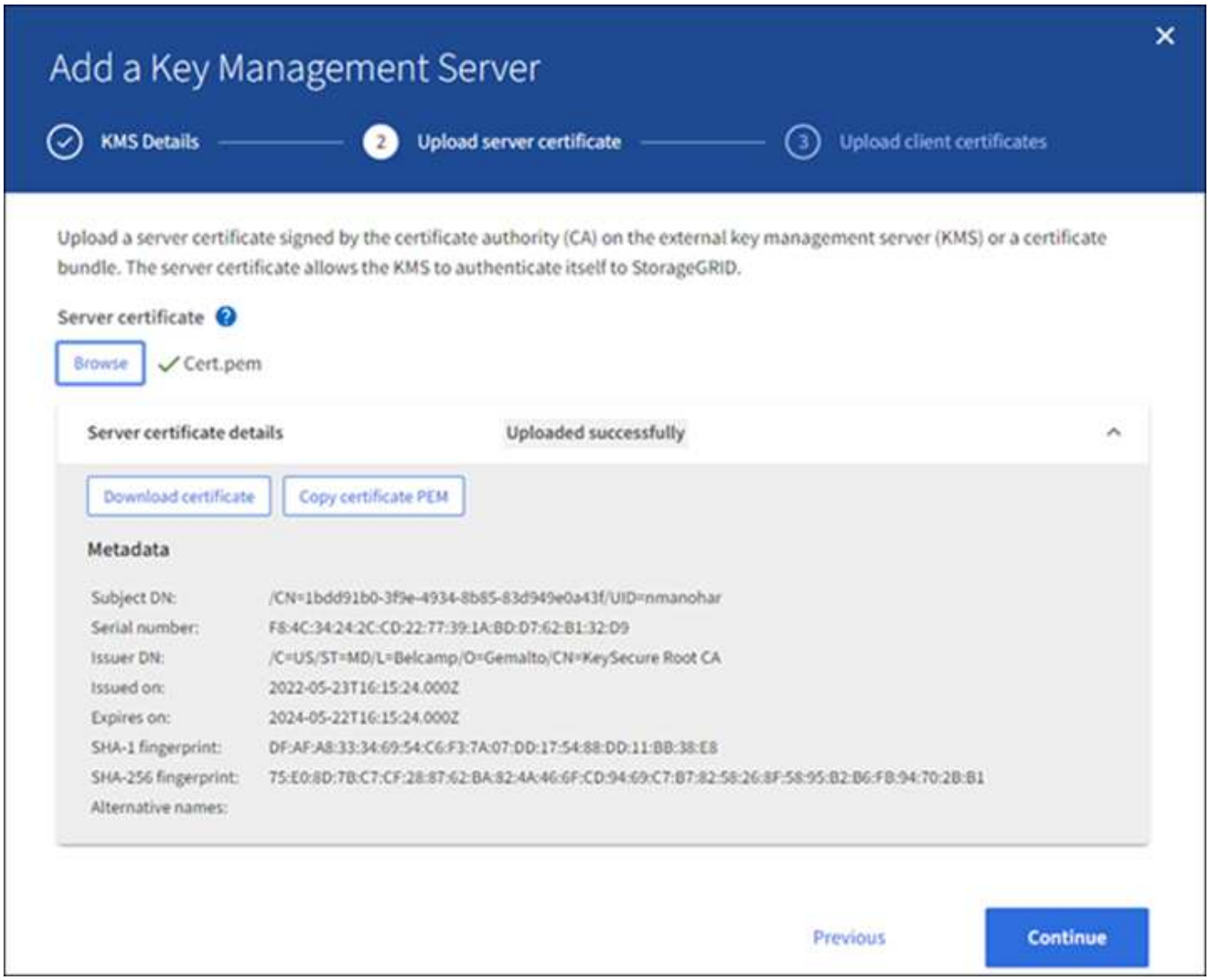
步驟

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。

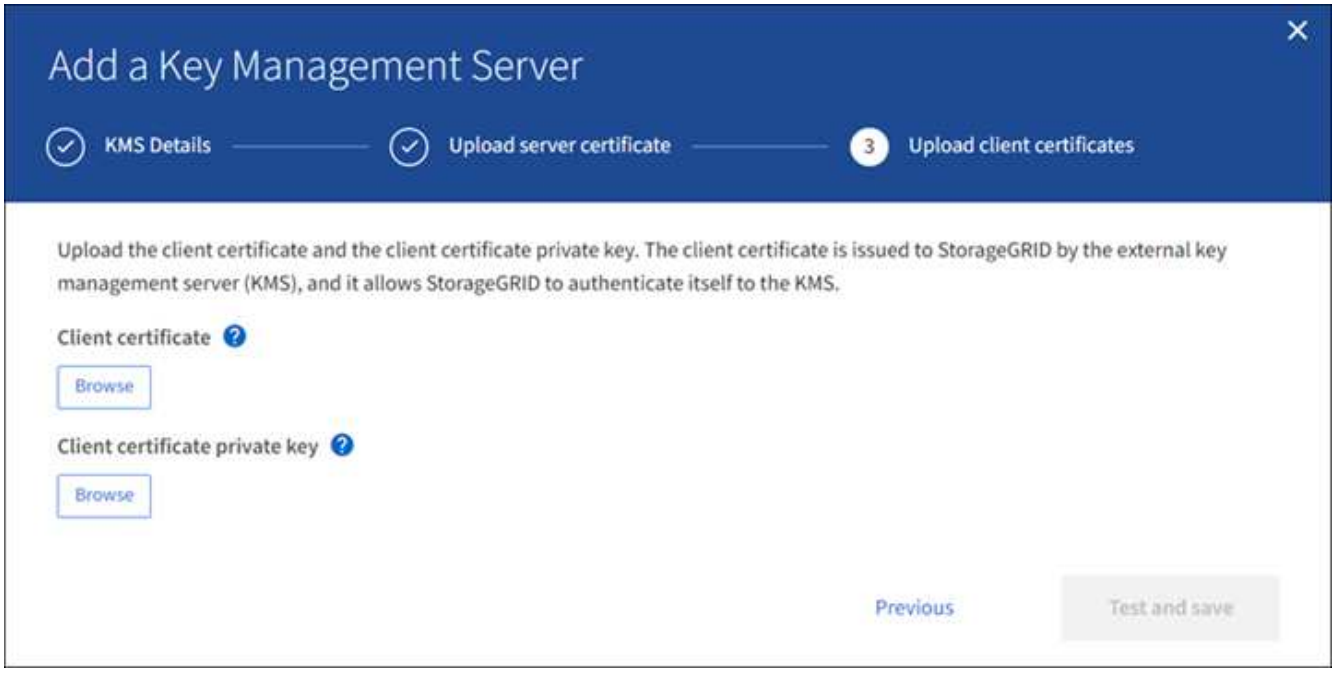
3. 選擇*繼續*。

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

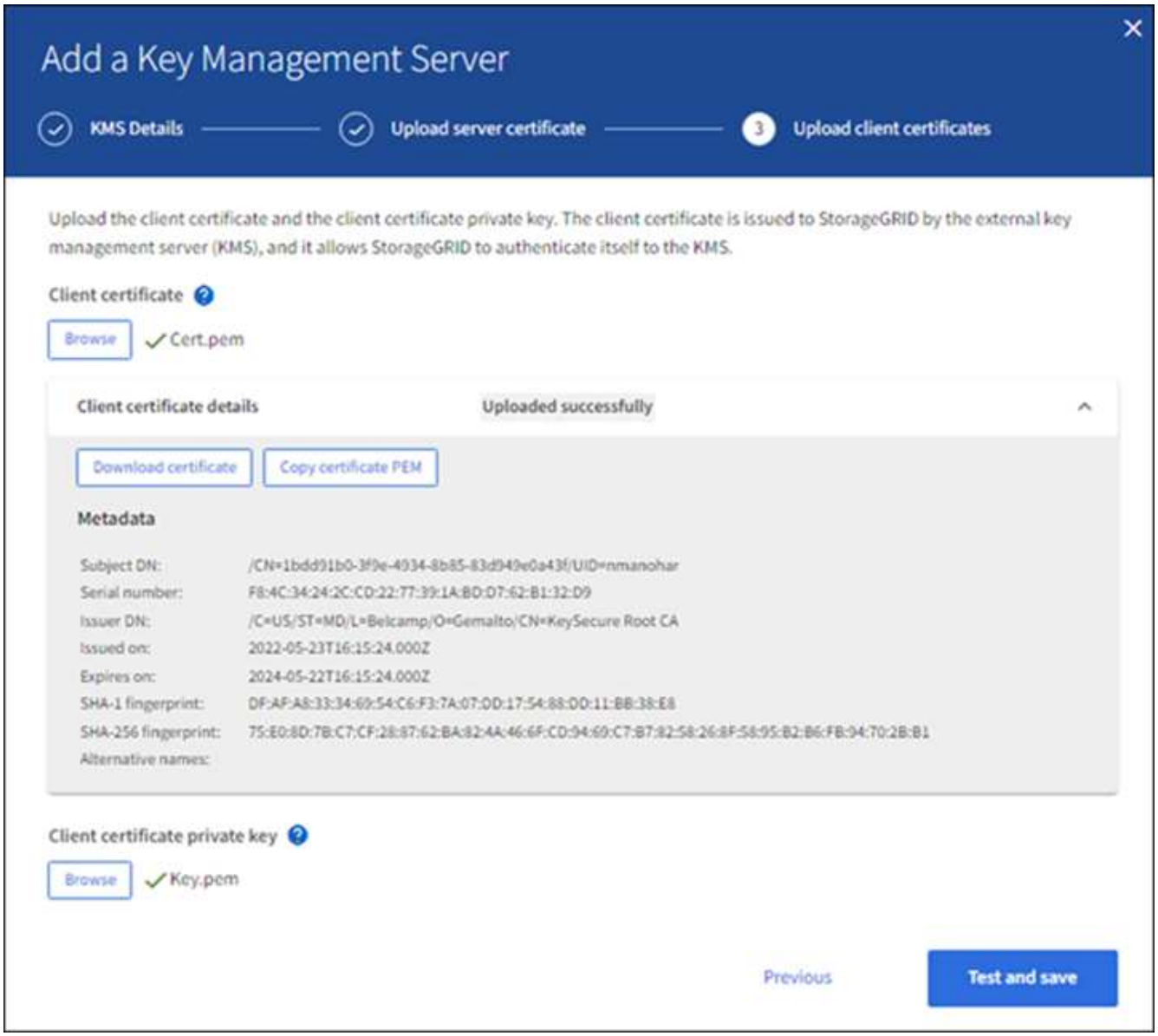
1. 從 * 步驟 3 （上傳用戶端憑證） * 、瀏覽至用戶端憑證的位置。



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。

版權資訊

商標資訊