



設定金鑰管理伺服器 StorageGRID 11.5

NetApp
April 11, 2024

目錄

| | |
|--------------------------------|----|
| 設定金鑰管理伺服器 | 1 |
| 什麼是金鑰管理伺服器 (KMS) ? | 1 |
| 檢閱StorageGRID 功能加密方法 | 1 |
| KMS與應用裝置組態總覽 | 3 |
| 使用金鑰管理伺服器的考量與要求 | 6 |
| 變更網站KMS的考量事項 | 9 |
| 在StorageGRID KMS中設定以用戶端身份執行的功能 | 11 |
| 新增金鑰管理伺服器 (KMS) | 12 |
| 檢視KMS詳細資料 | 20 |
| 檢視加密節點 | 21 |
| 編輯金鑰管理伺服器 (KMS) | 23 |
| 移除金鑰管理伺服器 (KMS) | 26 |

設定金鑰管理伺服器

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。設備磁碟區加密之後、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。

檢閱StorageGRID 功能加密方法

提供許多加密資料的選項。StorageGRID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） | 您可以為StorageGRID 該站台設定金鑰管理伺服器（組態>*系統設定*>*金鑰管理伺服器*）、並為該應用裝置啟用節點加密。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。可搭配StorageGRID 部分不含資料的儲存設備和服務設備使用。 |

| 加密選項 | 運作方式 | 適用於 |
|------------------------------|--|--|
| 在《支援資料保護系統》中提升安全性SANtricity | 如果儲存應用裝置已啟用磁碟機安全功能、您可以使用SANtricity「支援系統管理程式」來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。 | 具有完整磁碟加密 (FDE) 磁碟機或聯邦資訊處理標準 (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。無法與部分儲存設備或任何服務應用裝置搭配使用。 "SG6000儲存設備" "SG5700儲存設備" "SG5600儲存設備" |
| 儲存的物件加密網格選項 | 您可以在Grid Manager中啟用*儲存的物件加密*選項 (組態>*系統設定*>*網格選項*)。啟用時、任何未在儲存區層級或物件層級加密的新物件、都會在擷取期間加密。 | 新擷取的S3和Swift物件資料。現有的儲存物件不會加密。物件中繼資料和其他敏感資料不會加密。 "設定儲存的物件加密" |
| 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。任何未在物件層級加密的新物件、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。現有的儲存區物件不會加密。物件中繼資料和其他敏感資料不會加密。 "使用S3" |
| 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S3" |
| 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。 <ul style="list-style-type: none"> • 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S3" |

| 加密選項 | 運作方式 | 適用於 |
|-----------------------|--|--|
| 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：

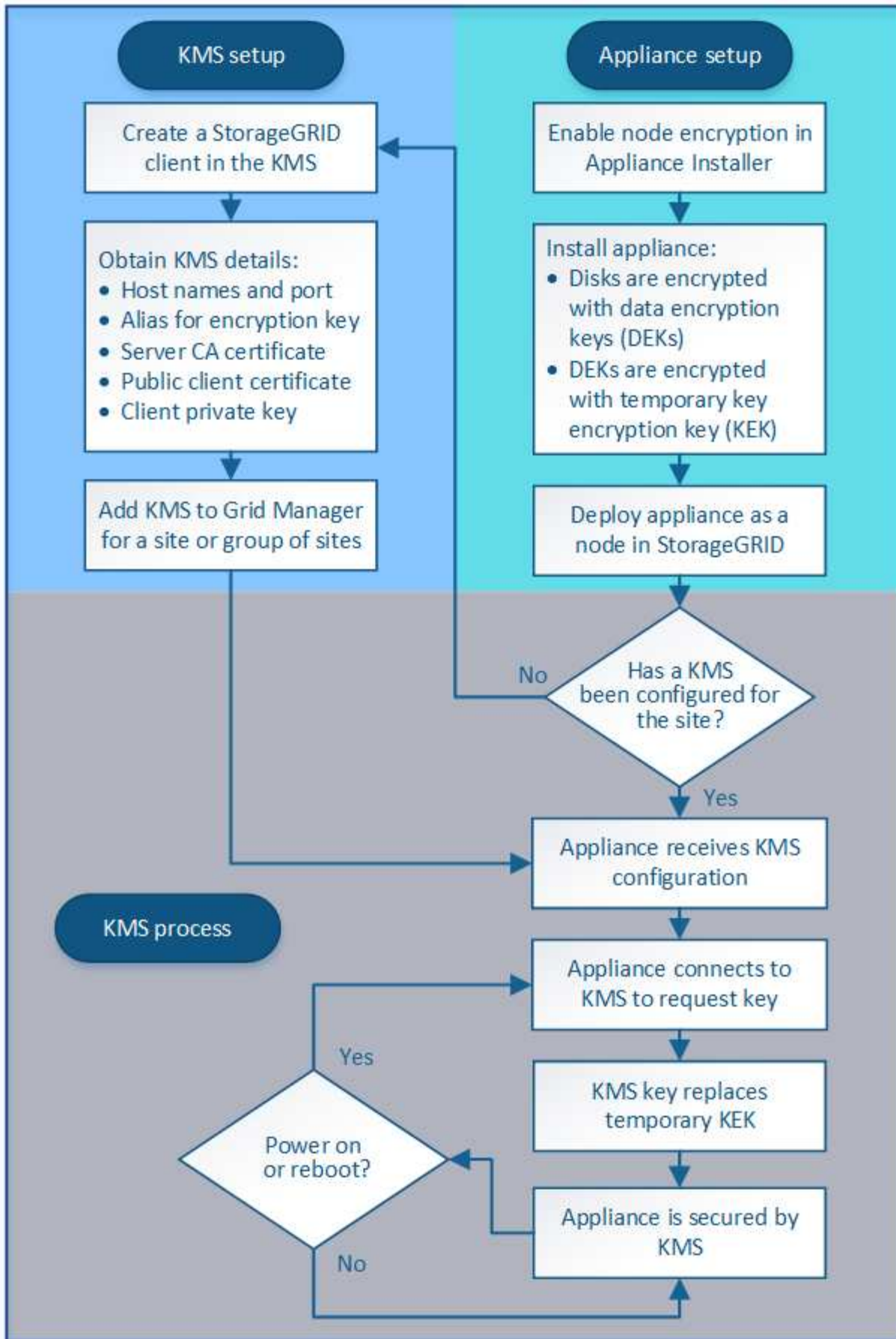
- 您可以使用KMS來保護應用裝置節點、也可以使用SANtricity 支援系統管理程式中的磁碟機安全功能、在同一個應用裝置中的自我加密磁碟機上「雙重加密」資料。
- 您可以使用KMS來保護應用裝置節點上的資料安全、也可以使用「儲存的物件加密」網格選項、在擷取所有物件時加密所有物件。

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。

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 Unified Key Setup (LUKS) 磁碟加密產生、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

如需詳細資料、請參閱下列內容：

- "[SG100 機；SG1000服務應用裝置](#)"
- "[SG6000儲存設備](#)"
- "[SG5700儲存設備](#)"
- "[SG5600儲存設備](#)"

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、無法在電力中斷或重新開機後繼續運作。

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。

您可以將設定的KMS用於下列StorageGRID 的不含技術的應用程式和應用裝置節點：

| 應用裝置 | 節點類型 |
|--------------|-----------|
| SG1000服務應用裝置 | 管理節點或閘道節點 |
| SG100服務應用裝置 | 管理節點或閘道節點 |
| SG6000儲存應用裝置 | 儲存節點 |
| SG5700儲存應用裝置 | 儲存節點 |
| SG5600儲存應用裝置 | 儲存節點 |

您無法將設定的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Docker容器內的節點

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。

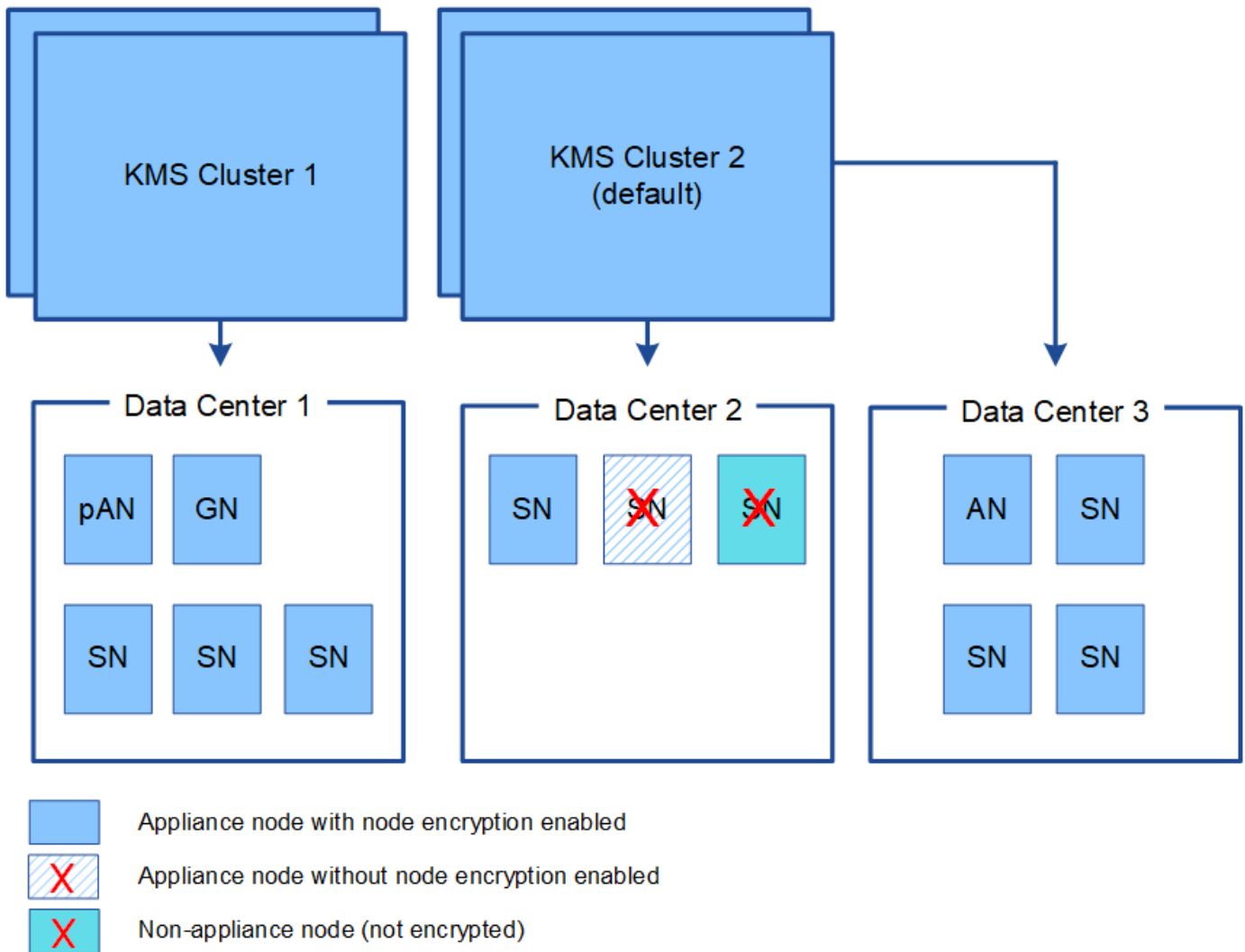
我需要多少個關鍵管理伺服器？

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、您無法在非應用裝置節點或安裝期間未啟用*節點加密*設定的任何應用裝置節點上使用KMS。



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按鍵。



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。
- 如果新的金鑰版本因故無法加密應用裝置磁碟區、則會觸發應用裝置節點的* KMS加密金鑰旋轉失敗*警告。您可能需要聯絡技術支援部門、以協助解決此警告。

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 《不知道如何使用產品安裝程式來清除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。

"SG100 機；SG1000服務應用裝置"

"SG6000儲存設備"

"SG5700儲存設備"

"SG5600儲存設備"

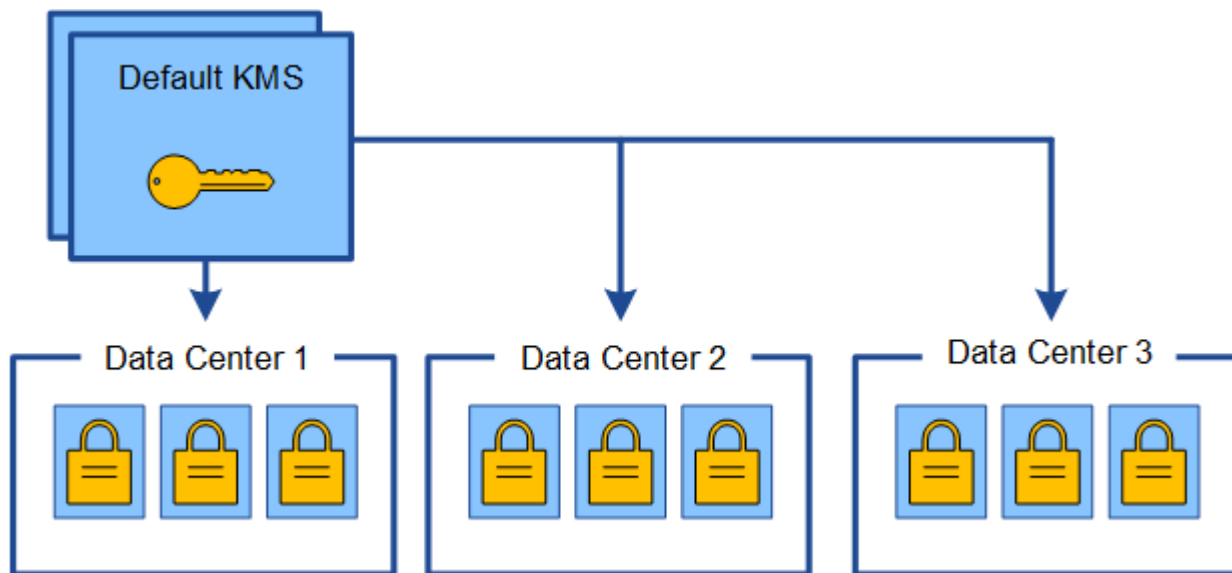
變更網站KMS的考量事項

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。

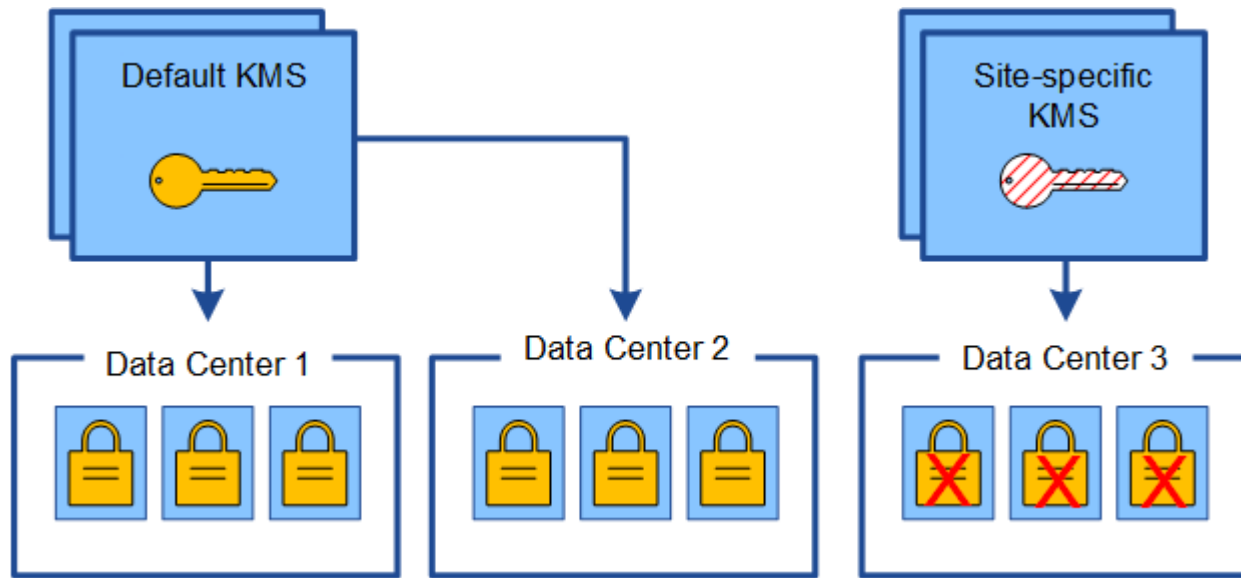
例如：

1. 您一開始會設定適用於所有沒有專屬KMS的站台的預設KMS。
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。

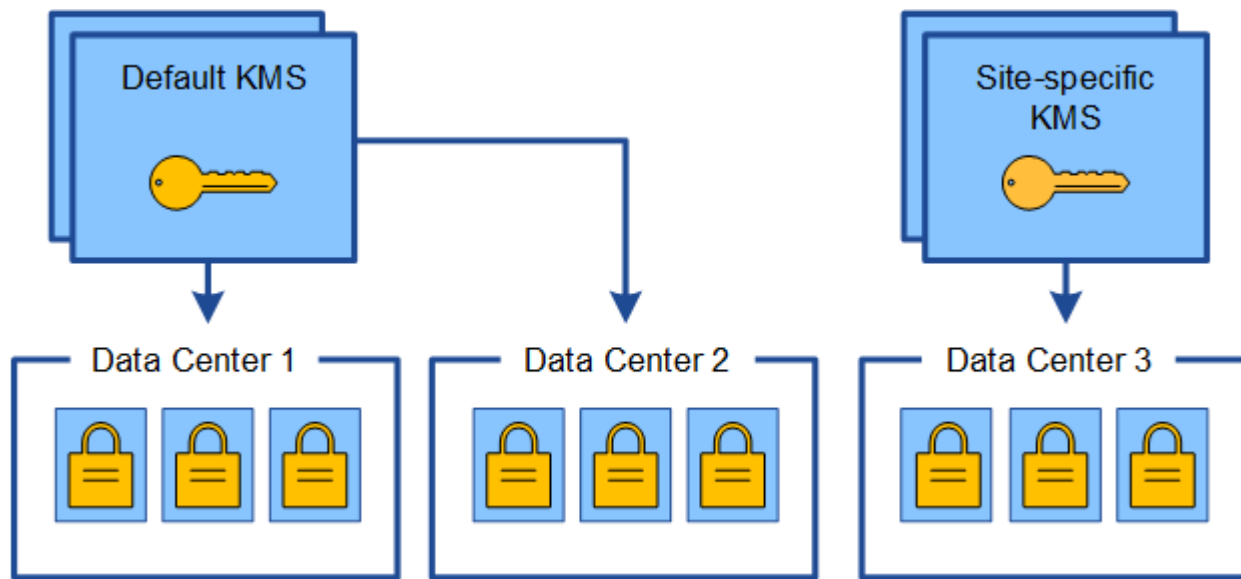


3. 您決定為單一站台新增站台專屬的KMS（圖中的資料中心3）。不過、由於應用裝置節點已加密、因此當您

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。 | <p>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。此套用至任何沒有專屬KMS的站台。</p> <p>"編輯金鑰管理伺服器 (KMS) "</p> |
| 您有預設的KMS、而且您在擴充中新增了一個網站。您不想將預設KMS用於新網站。 | <ol style="list-style-type: none"> 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。 <p>"新增金鑰管理伺服器 (KMS) "</p> |
| 您想讓站台的KMS使用不同的伺服器。 | <ol style="list-style-type: none"> 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。 <p>"新增金鑰管理伺服器 (KMS) "</p> |

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 CSpherTrust Manager k170v、2.0、2.1及2.2版。如果您對使用不同的關鍵管理伺服器StorageGRID 搭配使用方面有任何疑問、請聯絡技術支援部門。

["Thales CiperTrust經理"](#)

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。

您需要的產品

- 您必須已檢閱 ["使用金鑰管理伺服器的考量與要求"](#)。
- 您必須擁有 ["設定StorageGRID 成KMS中的用戶端"](#)，而且您必須擁有每個KMS或KMS叢集所需的資訊
- 您必須具有「根存取」權限。
- 您必須使用支援的瀏覽器登入Grid Manager。

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。

["變更網站KMS的考量事項"](#)

步驟

1. ["步驟1：輸入KMS詳細資料"](#)
2. ["步驟2：上傳伺服器憑證"](#)
3. ["步驟3：上傳用戶端憑證"](#)

步驟1：輸入KMS詳細資料

在「新增金鑰管理伺服器」精靈的步驟1（輸入KMS詳細資料）中、您將提供有關KMS或KMS叢集的詳細資料。

步驟

1. 選擇*組態*系統設定*金鑰管理伺服器*。

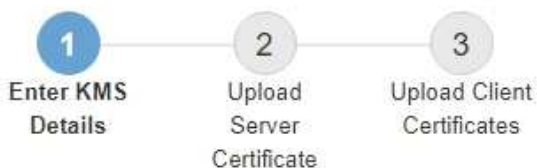
此時會出現「金鑰管理伺服器」頁面、並選取「組態詳細資料」索引標籤。

The screenshot shows the 'Key Management Server' configuration page. At the top, there's a title 'Key Management Server' and a descriptive paragraph: 'If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.' Below this, there are two tabs: 'Configuration Details' (selected) and 'Encrypted Nodes'. A paragraph explains that you can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. Below this, it says 'Before adding a KMS:' followed by a bulleted list of instructions: 'Ensure that the KMS is KMIP-compliant.', 'Configure StorageGRID as a client in the KMS.', and 'Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.' Below the list, it says 'For complete instructions, see [administering StorageGRID](#).' At the bottom, there's a table with columns: 'KMS Display Name', 'Key Name', 'Manages keys for', 'Hostname', and 'Certificate Status'. Above the table are buttons for '+ Create', 'Edit', and 'Remove'. Below the table, it says 'No key management servers have been configured. Select Create.'

2. 選擇* Create（建立）。

此時會出現「Add a Key Management Server（新增金鑰管理伺服器）」精靈的步驟1（輸入KMS詳細資料）。

Add a Key Management Server



Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name

Key Name

Manages keys for

Port

Hostname +

Cancel

Next

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 |
|--------|---|
| 公里顯示名稱 | 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。 |
| 管理的金鑰 | <p>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。</p> <ul style="list-style-type: none">• 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管理的站台（預設KMS）*來設定預設KMS、以套用至任何沒有專屬KMS的站台、以及您在後續擴充中新增的任何站台。 <p>*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。</p> |

| 欄位 | 說明 |
|------|---|
| 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。 *附註：*伺服器憑證的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。 |

- 如果您使用KMS叢集、請選取加號 **+** 為叢集中的每個伺服器新增主機名稱。
- 選擇*下一步*。

此時會出現「Add a Key Management Server (新增金鑰管理伺服器)」精靈的步驟2 (上傳伺服器憑證)。

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、您會上傳KMS的伺服器憑證 (或憑證套件組合)。伺服器憑證可讓外部KMS驗證自己StorageGRID 以供驗證。

步驟

- 從*步驟2 (上傳伺服器憑證)* 瀏覽至儲存的伺服器憑證或憑證套裝組合位置。

Add a Key Management Server

1
 Enter KMS
Details

2
 Upload
Server
Certificate

3
 Upload Client
Certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate 🔍 Browse

Cancel
Back
Next

2. 上傳憑證檔案。

隨即顯示伺服器憑證中繼資料。

Add a Key Management Server

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate k170vCA.pem

Server Certificate Metadata

| | |
|--------------------|---|
| Server DN: | /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA |
| Serial Number: | 71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E |
| Issue DN: | /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA |
| Issued On: | 2020-10-15T21:12:45.000Z |
| Expires On: | 2030-10-13T21:12:45.000Z |
| SHA-1 Fingerprint: | EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79 |



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*下一步*。

出現「Add a Key Management Server（新增金鑰管理伺服器）」精靈的步驟3（上傳用戶端憑證）。

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、您會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。

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate 

Client Certificate Private Key 

Cancel

Back

Save

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。

此時會顯示用戶端憑證和用戶端憑證私密金鑰的中繼資料。

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate k170vClientCert.pem

```
Server DN: /CN=admin/UID=  
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB  
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA  
Issued On: 2020-10-15T23:31:49.000Z  
Expires On: 2022-10-15T23:31:49.000Z  
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69
```

Client Certificate Private Key k170vClientKey.pem

Cancel

Back

Save

5. 選擇*保存*。

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. 如果在選擇*保存*時出現錯誤訊息、請檢閱訊息詳細資料、然後選擇*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*。

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ⓘ k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ⓘ k170vClientKey.pem

Select **Force Save** to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Cancel

Back

Force Save

Save



選取*強制儲存*會儲存KMS組態、但不會測試每個應用裝置與該KMS之間的外部連線。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 *。

⚠ Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

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*系統設定*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。

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

| + Create Edit Remove | | | | |
|----------------------------|----------|--|--------------|------------------------------|
| KMS Display Name | Key Name | Manages keys for | Hostname | Certificate Status |
| Default KMS | test | Sites not managed by another KMS (default KMS) | 10.96.99.164 | ✓ All certificates are valid |

2. 檢閱表格中每個KMS的資訊。

| 欄位 | 說明 |
|--------|--|
| 公里顯示名稱 | 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)。 |

| 欄位 | 說明 |
|------|--|
| 主機名稱 | <p>KMS的完整網域名稱或IP位址。</p> <p>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。</p> <p>例如： 10.10.10.10 and 10.10.10.11 或 10.10.10.10 and 2 others °</p> <p>若要檢視叢集中的所有主機名稱、請選取KMS、然後選取*編輯*。</p> |
| 憑證狀態 | <p>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。</p> <p>附註： StorageGRID 更新憑證狀態可能需要30分鐘的時間。您必須重新整理網頁瀏覽器、才能查看目前值。</p> |

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



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、才能查看實際狀態。

4. 如果「憑證狀態」欄指出某個憑證已過期或即將到期、請盡快解決此問題。

請參閱監控StorageGRID 與疑難排解的指示、瞭解有關* KMS CA憑證過期*、* KMS用戶端憑證過期*和* KMS伺服器憑證過期*警示的建議行動。



您必須盡快解決任何憑證問題、才能維持資料存取。

相關資訊

["監控安培；疑難排解"](#)

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*系統設定*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。

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

| + Create | Edit | Remove | | | |
|--------------------------|----------------------|--|--------------|------------------------------|--|
| KMS Display Name | Key Name | Manages keys for | Hostname | Certificate Status | |
| Default KMS | test | Sites not managed by another KMS (default KMS) | 10.96.99.164 | ✓ All certificates are valid | |

2. 從頁面頂端選取*加密節點*索引標籤。

Key Management Server

If your StorageGRID system includes appliance nodes with Full Disk Encryption (FDE) enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

「加密節點」索引標籤會列出StorageGRID 啟用*節點加密*設定的支援系統中的應用裝置節點。

Configuration Details

Encrypted Nodes

Review the KMS status for all appliance nodes that have node encryption enabled. Address any issues immediately to ensure your data is fully protected. If no KMS exists for a site, select Configuration Details and add a KMS.

Nodes with Encryption Enabled

| Node Name | Node Type | Site | KMS Display Name | Key UID | Status |
|--------------------|--------------|---------------|------------------|-------------|--|
| SGA-010-096-104-67 | Storage Node | Data Center 1 | Default KMS | 41b0...5c57 | ✓ Connected to KMS (2021-03-12 10:59:32 MST) |

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。 |
| 網站 | 安裝節點的站台名稱。StorageGRID |

| 欄位 | 說明 |
|--------|---|
| 公里顯示名稱 | 用於節點的KMS描述性名稱。 如果未列出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。若要檢視完整的金鑰UID、請將游標暫留在儲存格上。 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KMS請參閱監控和疑難排解StorageGRID 說明中的建議警示動作。



您必須立即解決任何問題、確保資料受到完整保護。

相關資訊

["監控安培；疑難排解"](#)

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。

您需要的產品

- 您必須已檢閱 ["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、則必須已檢閱 ["變更網站KMS的考量事項"](#)。
- 您必須具有「根存取」權限。
- 您必須使用支援的瀏覽器登入Grid Manager。

步驟

1. 選擇*組態*系統設定*金鑰管理伺服器*。

「金鑰管理伺服器」頁面隨即出現、並顯示所有已設定的金鑰管理伺服器。

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details **Encrypted Nodes**

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

| + Create Edit Remove | | | | |
|--|----------------------------|--|----------------------------|--------------------------------------|
| KMS Display Name ? | Key Name ? | Manages keys for ? | Hostname ? | Certificate Status ? |
| Default KMS | test | Sites not managed by another KMS (default KMS) | 10.96.99.164 | ✓ All certificates are valid |

2. 選取您要編輯的KMS、然後選取*編輯*。
3. 您也可以更新編輯金鑰管理伺服器精靈*步驟1（輸入KMS詳細資料）*中的詳細資料。

| 欄位 | 說明 |
|--------|--|
| 公里顯示名稱 | 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 | <p>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。</p> <p>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。</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> 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。</p> <p>"使用金鑰管理伺服器的考量與要求"</p> </div> |

| 欄位 | 說明 |
|-------|--|
| 管理的金鑰 | <p>如果您正在編輯網站專屬的KMS、但尚未擁有預設的KMS、請選擇*不受其他KMS管理的網站（預設KMS）*。此選項會將站台專屬的KMS轉換成預設KMS、適用於所有沒有專屬KMS的站台、以及任何新增至擴充中的站台。</p> <p>*注意：*如果您正在編輯站台專屬的KMS、則無法選取其他站台。如果您正在編輯預設KMS、則無法選取特定網站。</p> |
| 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 | <p>KMS的完整網域名稱或IP位址。</p> <p>*附註：*伺服器憑證的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。</p> |

4. 如果您要設定KMS叢集、請選取加號 **+** 為叢集中的每個伺服器新增主機名稱。

5. 選擇*下一步*。

此時會出現「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*下一步*。

此時會出現「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*保存*。

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。

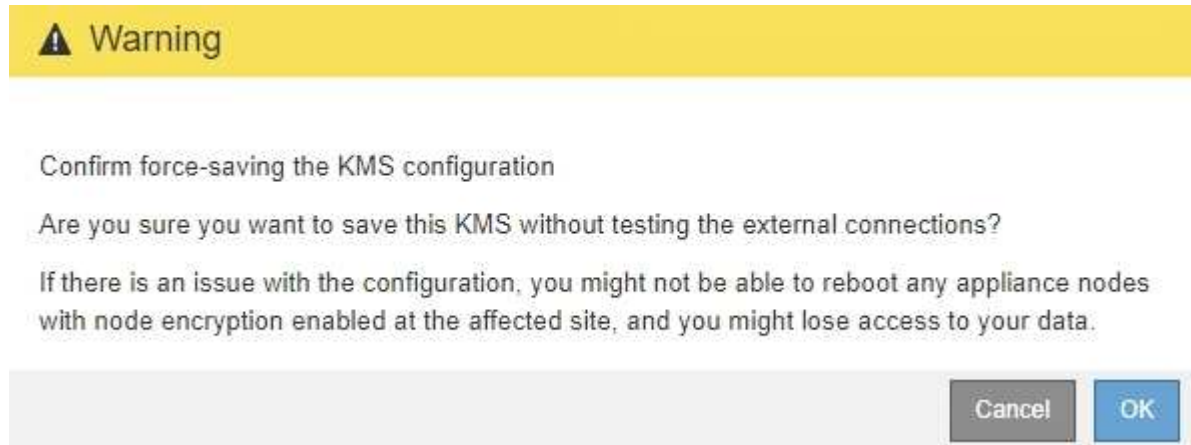
11. 如果您需要在解決連線錯誤之前儲存目前的組態、請選取*強制儲存*。



選取*強制儲存*會儲存KMS組態、但不會測試每個應用裝置與該KMS之間的外部連線。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。

您需要的產品

- 您必須已檢閱 "[使用金鑰管理伺服器的考量與要求](#)"。
- 您必須具有「根存取」權限。
- 您必須使用支援的瀏覽器登入Grid Manager。

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*系統設定*金鑰管理伺服器*。

「金鑰管理伺服器」頁面隨即出現、並顯示所有已設定的金鑰管理伺服器。

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

| + Create Edit Remove | | | | |
|--------------------------|----------|--|--------------|------------------------------|
| KMS Display Name | Key Name | Manages keys for | Hostname | Certificate Status |
| Default KMS | test | Sites not managed by another KMS (default KMS) | 10.96.99.164 | ✓ All certificates are valid |

2. 選取您要移除之KMS的選項按鈕、然後選取*移除*。
3. 檢閱警告對話方塊中的考量事項。

Warning

Delete KMS Configuration

You can only remove a KMS in these cases:

- You are removing a site-specific KMS for a site that has no appliance nodes with node encryption enabled.
- You are removing the default KMS, but a site-specific KMS already exists for each site with node encryption.

Are you sure you want to delete the Default KMS KMS configuration?

Cancel

OK

4. 選擇*確定*。

KMS組態隨即移除。

版權資訊

Copyright © 2024 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。