



新增金鑰管理伺服器 (KMS)

StorageGRID 11.5

NetApp
April 11, 2024

目錄

新增金鑰管理伺服器 (KMS)	1
步驟1：輸入KMS詳細資料	1
步驟2：上傳伺服器憑證	3
步驟3：上傳用戶端憑證	5

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。

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
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

1 Enter KMS Details 2 Upload Server Certificate 3 Upload Client Certificates

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	<input type="text"/>
Key Name	<input type="text"/>
Manages keys for	-- Choose One --
Port	5696
Hostname	<input type="text"/>

+

[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	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。 <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>
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。 <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。

5. 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

1. 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



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 

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
```

Cancel

Back

Next



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。

- 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。

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。