



添加密钥管理服务器(KMS)

StorageGRID 11.5

NetApp
April 11, 2024

目录

添加密钥管理服务器(KMS)	1
第 1 步：输入 KMS 详细信息	1
第 2 步：上传服务器证书	3
第 3 步：上传客户端证书	5

添加密钥管理服务器(KMS)

您可以使用 StorageGRID 密钥管理服务器向导添加每个 KMS 或 KMS 集群。

您需要的内容

- 您必须已查看 ["使用密钥管理服务器的注意事项和要求"](#)。
- 您必须拥有 ["已在 KMS 中将 StorageGRID 配置为客户端"](#)和必须具有每个KMS或KMS集群的所需信息
- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

关于此任务

如果可能，请先配置任何站点特定的密钥管理服务器，然后再配置一个默认 KMS ，以便对所有不受另一个 KMS 管理的站点进行适用场景 。如果首先创建默认 KMS ，则网格中所有节点加密的设备都将使用默认 KMS 进行加密。如果要稍后创建站点专用的 KMS ，则必须先将当前版本的加密密钥从默认 KMS 复制到新的 KMS 。

["更改站点的 KMS 的注意事项"](#)

步骤

1. ["第 1 步：输入 KMS 详细信息"](#)
2. ["第 2 步：上传服务器证书"](#)
3. ["第 3 步：上传客户端证书"](#)

第 1 步：输入 KMS 详细信息

在添加密钥管理服务器向导的步骤 1 （输入 KMS 详细信息）中，您可以提供有关 KMS 或 KMS 集群的详细信息。

步骤

1. 选择*配置系统设置密钥管理服务器*。

此时将显示密钥管理服务器页面，并选中配置详细信息选项卡。

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. 选择 * 创建 *。

此时将显示添加密钥管理服务器向导的第 1 步（输入 KMS 详细信息）。

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. 为 KMS 和您在该 KMS 中配置的 StorageGRID 客户端输入以下信息。

字段	Description
Kms 显示名称	一个描述性名称，可帮助您标识此 KMS。必须介于 1 到 64 个字符之间。

字段	Description
密钥名称	StorageGRID 客户端在 KMS 中的确切密钥别名。必须介于 1 到 255 个字符之间。
管理的密钥	<p>将与此 KMS 关联的 StorageGRID 站点。如果可能，您应先配置任何站点特定的密钥管理服务器，然后再配置一个默认 KMS，以便对不受另一个 KMS 管理的所有站点进行适用场景。</p> <ul style="list-style-type: none"> • 如果此 KMS 将管理特定站点上设备节点的加密密钥，请选择一个站点。 • 选择 * 不受其他 KMS 管理的站点（默认 KMS）* 可配置一个默认 KMS，该 KMS 将应用于没有专用 KMS 的任何站点以及您在后续扩展中添加的任何站点。 <ul style="list-style-type: none"> ◦ 注意：* 如果您选择的站点先前已被默认 KMS 加密，但未向新 KMS 提供当前版本的原始加密密钥，则保存 KMS 配置时将发生验证错误。
Port	KMS 服务器用于密钥管理互操作性协议（Key Management Interoperability Protocol，KMIP）通信的端口。默认为 5696，即 KMIP 标准端口。
主机名	<p>KMS 的完全限定域名或 IP 地址。</p> <ul style="list-style-type: none"> • 注：* 服务器证书的 SAN 字段必须包含您在此处输入的 FQDN 或 IP 地址。否则，StorageGRID 将无法连接到 KMS 或 KMS 集群中的所有服务器。

4. 如果您使用的是 KMS 集群，请选择加号 **+** 为集群中的每个服务器添加主机名。

5. 选择 * 下一步 *。

此时将显示添加密钥管理服务器向导的第2步(上传服务器证书)。

第 2 步：上传服务器证书

在添加密钥管理服务器向导的第 2 步（上传服务器证书）中，您可以上传 KMS 的服务器证书（或证书包）。通过服务器证书，外部 KMS 可以向 StorageGRID 进行身份验证。

步骤

1. 从 * 步骤 2（上传服务器证书）* 中，浏览到保存的服务器证书或证书包的位置。

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 

2. 上传证书文件。

此时将显示服务器证书元数据。

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



如果您上传的是证书捆绑包，则每个证书的元数据将显示在其自己的选项卡上。

3. 选择 * 下一步 *。

此时将显示添加密钥管理服务器向导的第3步(上传客户端证书)。

第 3 步：上传客户端证书

在添加密钥管理服务器向导的第 3 步（上传客户端证书）中，您可以上传客户端证书和客户端证书专用密钥。客户端证书允许 StorageGRID 向 KMS 进行身份验证。

步骤

1. 从 * 步骤 3（上传客户端证书）* 中，浏览到客户端证书的位置。

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. 上传客户端证书文件。

此时将显示客户端证书元数据。

3. 浏览到客户端证书的专用密钥位置。


4. 上传私钥文件。

此时将显示客户端证书和客户端证书专用密钥的元数据。

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. 选择 * 保存 *。

测试密钥管理服务器与设备节点之间的连接。如果所有连接均有效，并且在 KMS 上找到正确的密钥，则新的密钥管理服务器将添加到密钥管理服务器页面上的表中。



添加 KMS 后，密钥管理服务器页面上的证书状态将立即显示为未知。StorageGRID 可能需要长达 30 分钟才能获取每个证书的实际状态。您必须刷新 Web 浏览器才能查看当前状态。

6. 如果选择 * 保存 * 时显示错误消息，请查看消息详细信息，然后选择 * 确定 *。

例如，如果连接测试失败，您可能会收到 422： Unprocessable Entity 错误。

7. 如果需要保存当前配置而不测试外部连接，请选择 * 强制保存 *。

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



选择 * 强制保存 * 可保存 KMS 配置，但不会测试每个设备与该 KMS 的外部连接。如果具有此配置的问题描述，则可能无法重新启动受影响站点上已启用节点加密的设备节点。在问题解决之前，您可能无法访问数据。

- 查看确认警告，如果确实要强制保存配置，请选择 * 确定 *。

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

已保存 KMS 配置，但未测试与 KMS 的连接。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。