



配置密钥管理服务 StorageGRID 11.7

NetApp
April 12, 2024

目录

- 配置密钥管理服务器 1
 - 配置密钥管理服务器：概述 1
 - KMS 和设备配置概述 1
 - 使用密钥管理服务器的注意事项和要求 4
 - 更改站点的 KMS 的注意事项 6
 - 在 KMS 中将 StorageGRID 配置为客户端 8
 - 添加密钥管理服务器（KMS） 9
 - 查看 KMS 详细信息 16
 - 查看加密节点 17
 - 编辑密钥管理服务器（KMS） 18
 - 删除密钥管理服务器（KMS） 20

配置密钥管理服务

配置密钥管理服务：概述

您可以配置一个或多个外部密钥管理服务（KMS）来保护专门配置的设备节点上的数据。

什么是密钥管理服务（KMS）？

密钥管理服务（Key Management Server，KMS）是一种外部第三方系统，可使用密钥管理互操作性协议（Key Management Interoperability Protocol，KMIP）为关联 StorageGRID 站点上的 StorageGRID 设备节点提供加密密钥。

您可以使用一个或多个密钥管理服务来管理安装期间启用了 * 节点加密 * 设置的任何 StorageGRID 设备节点的节点加密密钥。通过将密钥管理与这些设备节点结合使用，您可以保护数据，即使设备已从数据中心中删除也是如此。对设备卷进行加密后、您将无法访问设备上的任何数据、除非此节点可以与KMS进行通信。

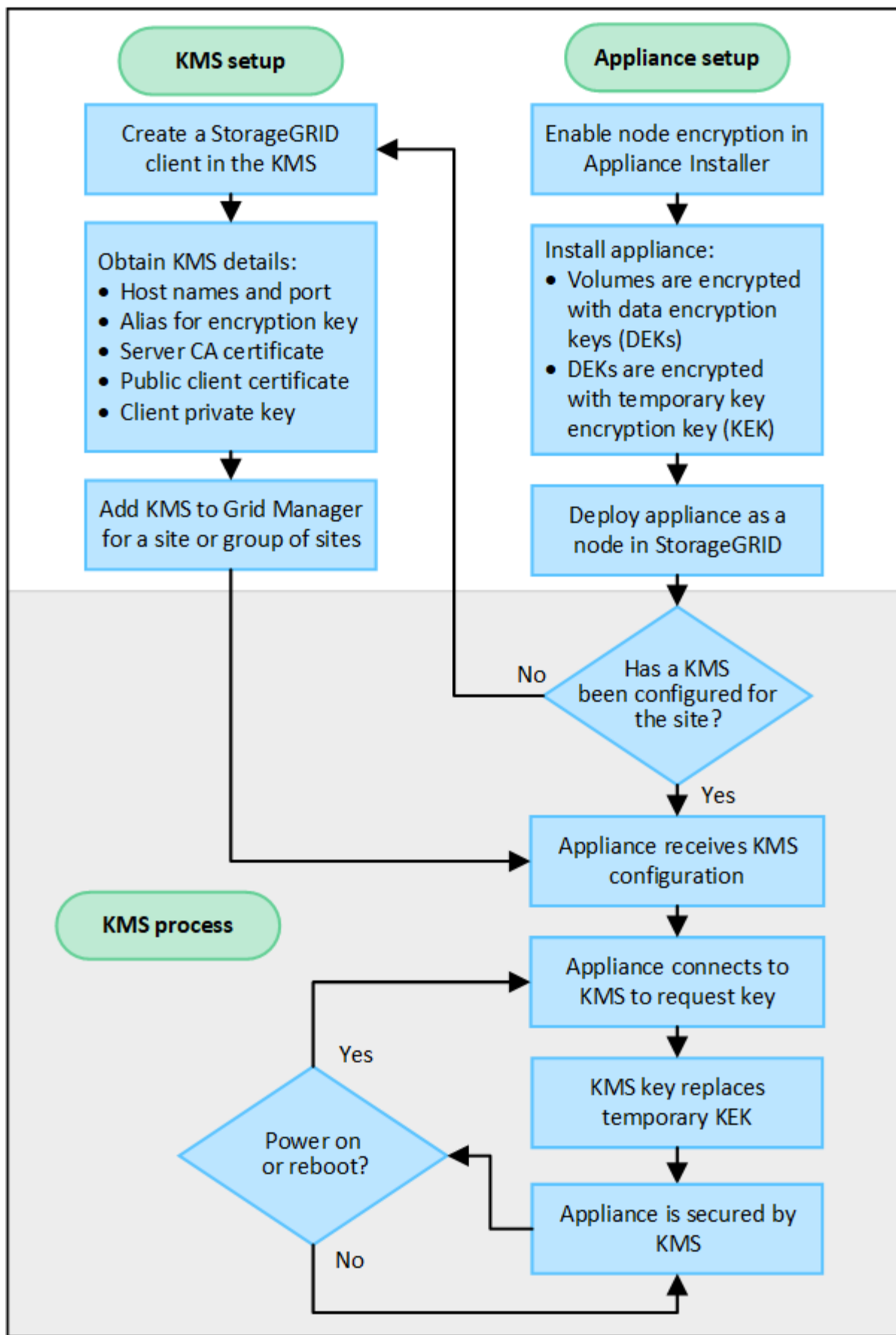


StorageGRID 不会创建或管理用于对设备节点进行加密和解密的外部密钥。如果您计划使用外部密钥管理服务来保护 StorageGRID 数据，则必须了解如何设置该服务器，并且必须了解如何管理加密密钥。执行密钥管理任务不在本说明的范围之内。如果需要帮助，请参见密钥管理服务器的文档或联系技术支持。

KMS 和设备配置概述

在使用密钥管理服务（KMS）保护设备节点上的 StorageGRID 数据之前，必须完成两项配置任务：设置一个或多个 KMS 服务器以及为设备节点启用节点加密。完成这两项配置任务后，密钥管理过程将自动进行。

此流程图显示了使用 KMS 在设备节点上保护 StorageGRID 数据的高级步骤。



流程图显示了 KMS 设置和设备设置并行进行；但是，您可以根据需要在为新设备节点启用节点加密之前或之后

设置密钥管理服务器。

设置密钥管理服务器（KMS）

设置密钥管理服务器包括以下高级步骤。

步骤	请参见
访问 KMS 软件，并向每个 KMS 或 KMS 集群添加一个 StorageGRID 客户端。	"在 KMS 中将 StorageGRID 配置为客户端"
在 KMS 上获取 StorageGRID 客户端所需的信息。	"在 KMS 中将 StorageGRID 配置为客户端"
将 KMS 添加到网格管理器中，将其分配到一个站点或一组默认站点，上传所需的证书并保存 KMS 配置。	"添加密钥管理服务器（KMS）"

设置设备

设置要使用 KMS 的设备节点包括以下高级步骤。

1. 在设备安装的硬件配置阶段，使用 StorageGRID 设备安装程序为设备启用 * 节点加密 * 设置。



将设备添加到网格后、您无法启用*节点加密*设置、并且无法对未启用节点加密的设备使用外部密钥管理。

2. 运行 StorageGRID 设备安装程序。在安装期间，系统会为每个设备卷分配一个随机数据加密密钥（DEK），如下所示：
 - 这些 DEKs 用于对每个卷上的数据进行加密。这些密钥是在设备操作系统中使用Linux统一密钥设置(LUKS)磁盘加密生成的、无法更改。
 - 每个 DEK 都通过主密钥加密密钥（KEK）进行加密。初始 KEK 是一个临时密钥，用于对密钥进行加密，直到设备可以连接到 KMS 为止。
3. 将设备节点添加到 StorageGRID 。

请参见 ["启用节点加密"](#) 了解详细信息。

密钥管理加密过程（自动发生）

密钥管理加密包括以下高级步骤，这些步骤会自动执行。

1. 在网格中安装启用了节点加密的设备时，StorageGRID 会确定包含新节点的站点是否存在 KMS 配置。
 - 如果已为站点配置 KMS，则设备将接收 KMS 配置。
 - 如果尚未为站点配置 KMS，则设备上的数据将继续由临时 KEK 加密，直到您为站点配置 KMS 且设备收到 KMS 配置为止。
2. 设备使用 KMS 配置连接到 KMS 并请求加密密钥。
3. KMS 会向设备发送加密密钥。KMS 中的新密钥将取代临时的 KEK，现在用于对设备卷的 DEK 进行加密和解密。



加密设备节点连接到配置的 KMS 之前存在的任何数据都将使用临时密钥进行加密。但是，在将临时密钥替换为 KMS 加密密钥之前，不应将设备卷视为不受从数据中心删除的保护。

4. 如果设备已启动或重新启动，它将重新连接到 KMS 以请求密钥。此密钥保存在易失性内存中、无法经受断电或重新启动的影响。

使用密钥管理服务器的注意事项和要求

在配置外部密钥管理服务器（KMS）之前，您必须了解注意事项和要求。

KMIP 要求是什么？

StorageGRID 支持 KMIP 1.4 版。

["密钥管理互操作性协议规范 1.4 版"](#)

设备节点与配置的 KMS 之间的通信使用安全 TLS 连接。StorageGRID 支持 KMIP 使用以下 TLS v1.2 密码：

- `tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384`
- `tls_ECDHE_ECDSA_WIT_AES_256_GCM_SHA384`

您必须确保使用节点加密的每个设备节点都可以通过网络访问为站点配置的 KMS 或 KMS 集群。

网络防火墙设置必须允许每个设备节点通过用于密钥管理互操作性协议（Key Management Interoperability Protocol，KMIP）通信的端口进行通信。默认 KMIP 端口为 5696。

支持哪些设备？

您可以使用密钥管理服务器（Key Management Server，KMS）管理网格中启用了 * 节点加密 * 设置的任何 StorageGRID 设备的加密密钥。只有在使用 StorageGRID 设备安装程序安装设备的硬件配置阶段，才能启用此设置。



将设备添加到网格后、您无法启用节点加密、并且无法对未启用节点加密的设备使用外部密钥管理。

您可以对 StorageGRID 设备和设备节点使用已配置的 KMS。

您不能对基于软件(非设备)的节点使用已配置的 KMS、包括以下节点：

- 部署为虚拟机（VM）的节点
- 在 Linux 主机上的容器引擎中部署的节点

在这些其他平台上部署的节点可以在数据存储库或磁盘级别使用 StorageGRID 外部的加密。

应在何时配置密钥管理服务器？

对于新安装，通常应在创建租户之前在网格管理器中设置一个或多个密钥管理服务器。此顺序可确保节点在存储任何对象数据之前受到保护。

您可以在安装设备节点之前或之后在网络管理器中配置密钥管理服务器。

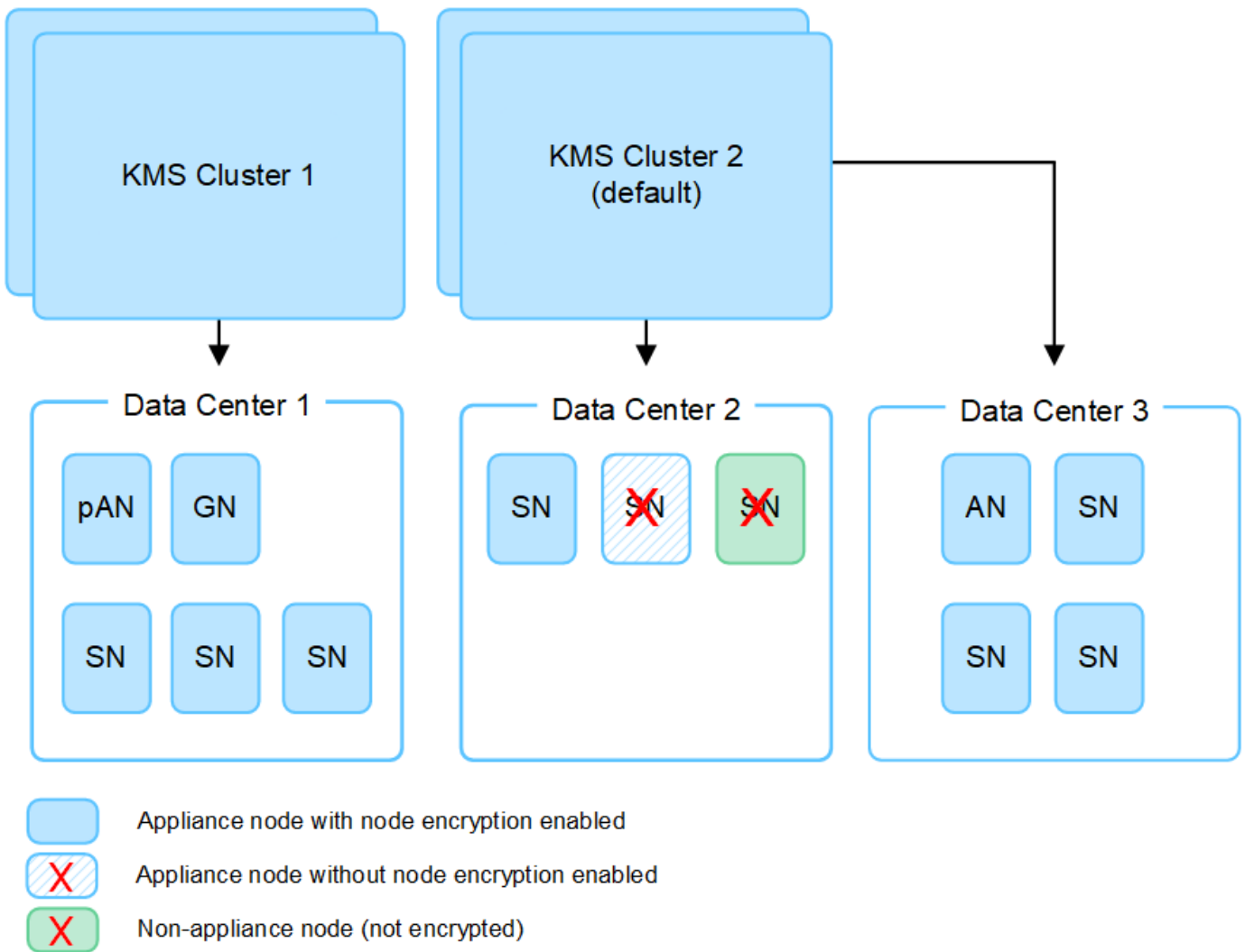
我需要多少个密钥管理服务器？

您可以配置一个或多个外部密钥管理服务器，以便为 StorageGRID 系统中的设备节点提供加密密钥。每个 KMS 都为单个站点或一组站点上的 StorageGRID 设备节点提供一个加密密钥。

StorageGRID 支持使用 KMS 集群。每个 KMS 集群都包含多个复制的密钥管理服务器，这些服务器共享配置设置和加密密钥。建议使用 KMS 集群进行密钥管理，因为它可以提高高可用性配置的故障转移功能。

例如，假设您的 StorageGRID 系统有三个数据中心站点。您可以将一个 KMS 集群配置为为 Data Center 1 上的所有设备节点提供密钥，而将另一个 KMS 集群配置为为所有其他站点上的所有设备节点提供密钥。添加第二个 KMS 集群时，您可以为 Data Center 2 和 Data Center 3 配置默认 KMS。

请注意，不能对非设备节点或安装期间未启用*Node Encryption设置的任何设备节点使用KMS。



轮换密钥时会发生什么情况？

作为安全最佳实践，您应定期轮换每个已配置的 KMS 使用的加密密钥。

在旋转加密密钥时，请使用 KMS 软件将该密钥从上次使用的版本轮换到同一密钥的新版本。不要旋转到完全不

同的键。



切勿尝试通过在网格管理器中更改 KMS 的密钥名称（别名）来轮换密钥。而是通过更新 KMS 软件中的密钥版本来轮换密钥。对新密钥使用与先前密钥相同的密钥别名。如果更改已配置 KMS 的密钥别名，则 StorageGRID 可能无法对数据进行解密。

新密钥版本可用时：

- 它会自动分发到与 KMS 关联的站点上的加密设备节点。分发应在轮换密钥后的一小时内完成。
- 如果在分发新密钥版本时加密设备节点脱机，则该节点将在重新启动后立即收到新密钥。
- 如果由于任何原因无法使用新密钥版本对设备卷进行加密、则会为此设备节点触发* KMS加密密钥轮换失败* 警报。您可能需要联系技术支持以帮助解决此警报。

是否可以在设备节点加密后重复使用它？

如果需要将加密设备安装到另一个 StorageGRID 系统中，则必须先停用网格节点，才能将对象数据移动到另一个节点。然后、您可以使用StorageGRID 设备安装程序 ["清除KMS配置"](#)。清除 KMS 配置将禁用 * 节点加密 * 设置，并删除设备节点与 StorageGRID 站点的 KMS 配置之间的关联。



如果无法访问 KMS 加密密钥，则设备上保留的任何数据将无法再访问并永久锁定。

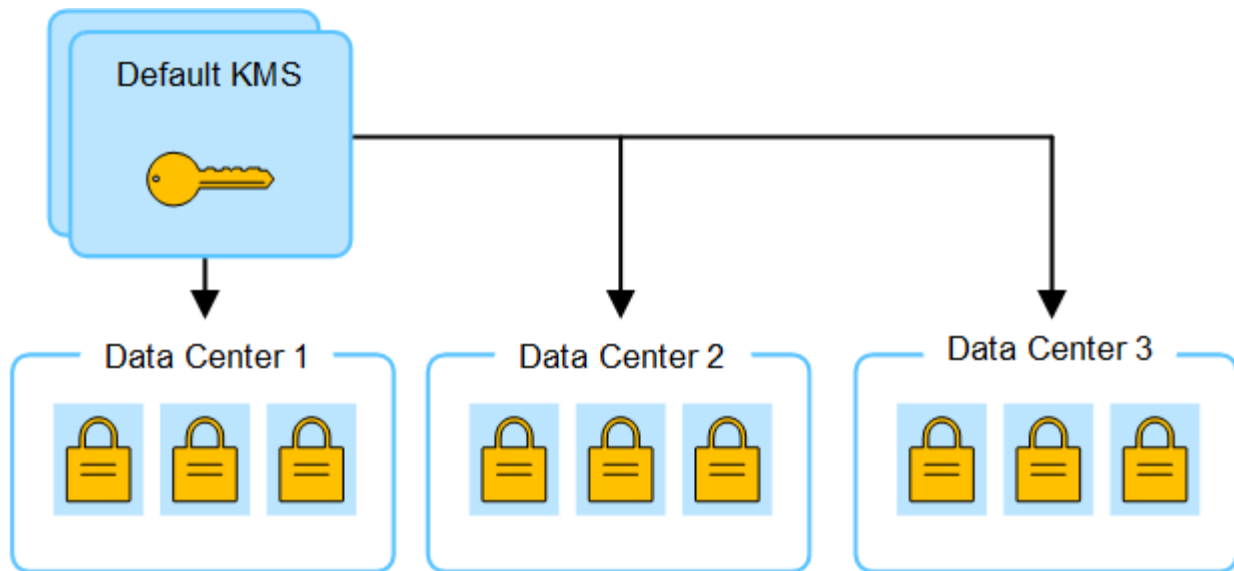
更改站点的 KMS 的注意事项

每个密钥管理服务器（Key Management Server，KMS）或 KMS 集群都会为单个站点或一组站点上的所有设备节点提供一个加密密钥。如果需要更改站点使用的 KMS，则可能需要将加密密钥从一个 KMS 复制到另一个 KMS。

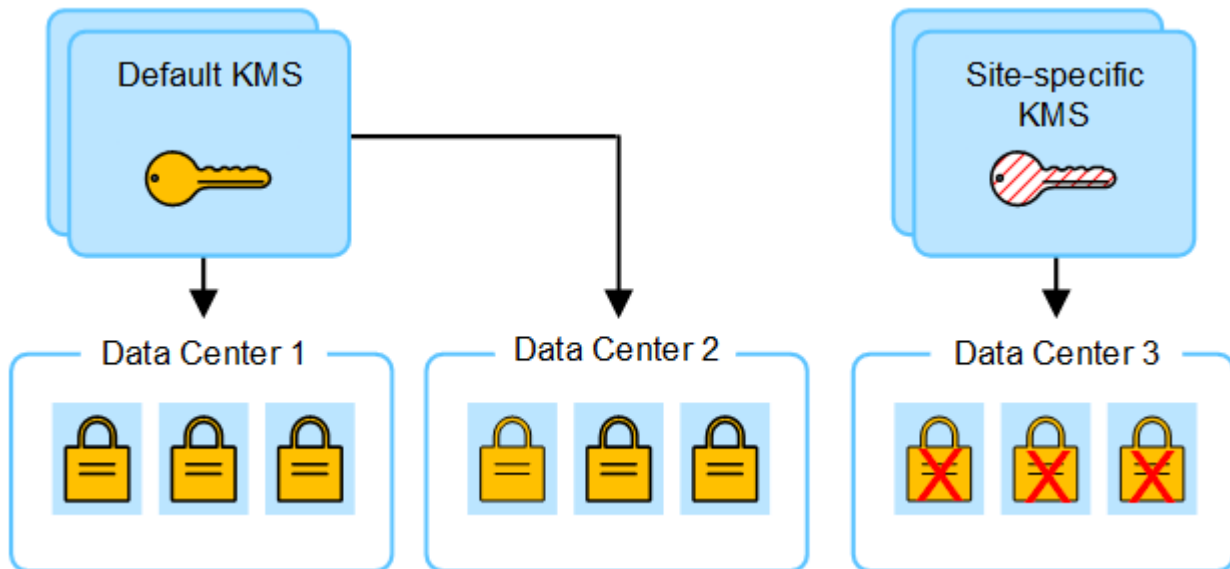
如果更改站点使用的 KMS，则必须确保可以使用存储在新 KMS 上的密钥对该站点上先前加密的设备节点进行解密。在某些情况下，您可能需要将当前版本的加密密钥从原始 KMS 复制到新 KMS。您必须确保 KMS 具有正确的密钥，以便对站点上的加密设备节点进行解密。

例如：

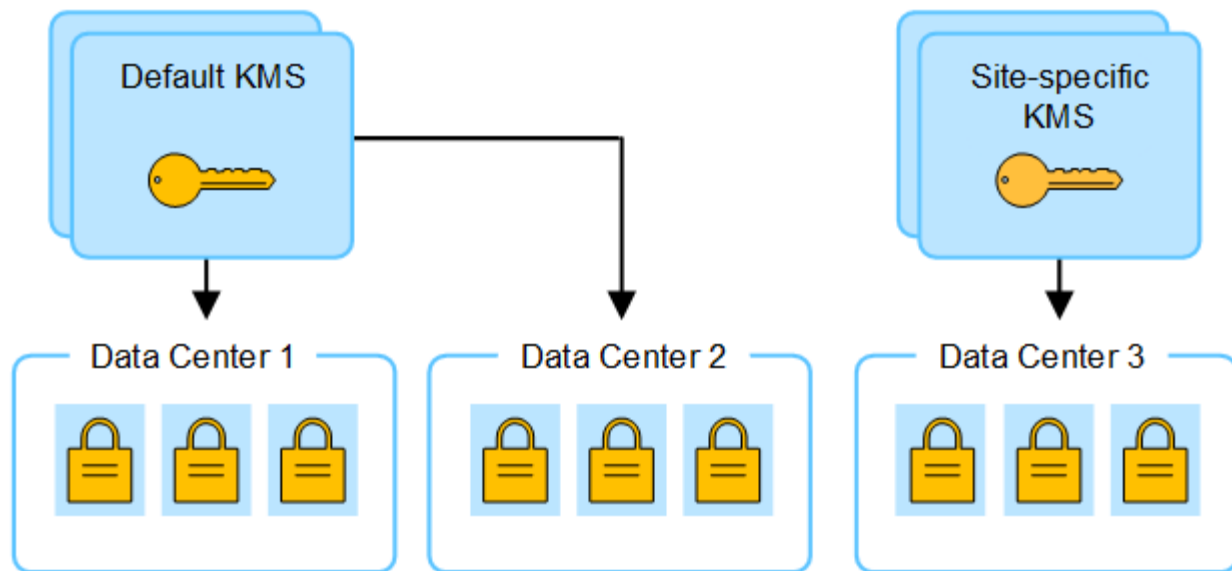
1. 您最初会配置一个默认KMS、用于适用场景 所有没有专用KMS的站点。
2. 保存 KMS 后，所有启用了 * 节点加密 * 设置的设备节点都会连接到 KMS 并请求加密密钥。此密钥用于对所有站点上的设备节点进行加密。此外，还必须使用此相同密钥对这些设备进行解密。



3. 您决定为一个站点（图中的数据中心 3）添加站点专用的 KMS。但是，由于设备节点已加密，因此在尝试保存站点专用 KMS 的配置时会发生验证错误。之所以出现此错误，是因为站点特定的 KMS 没有正确的密钥来对该站点上的节点进行解密。



4. 要解决问题描述 问题，请将当前版本的加密密钥从默认 KMS 复制到新的 KMS。（从技术上讲，您可以将原始密钥复制到具有相同别名的新密钥。原始密钥将成为新密钥的先前版本。）现在，站点特定的 KMS 具有用于对数据中心 3 上的设备节点进行解密的正确密钥，因此可以将其保存在 StorageGRID 中。



更改站点使用的 **KMS** 的用例

下表总结了更改站点 KMS 的最常见情况下所需的步骤。

更改站点 KMS 的用例	所需步骤
您有一个或多个站点特定的 KMS 条目，并且希望使用其中一个条目作为默认 KMS。	<p>编辑站点特定的 KMS。在 * 管理密钥 * 字段中，选择 * 不受其他 KMS（默认 KMS）管理的站点 *。现在，站点专用的 KMS 将用作默认 KMS。它将适用于没有专用 KMS 的任何站点。</p> <p>"编辑密钥管理服务器（KMS）"</p>
您有一个默认 KMS，并且在扩展中添加了一个新站点。您不想对新站点使用默认 KMS。	<ol style="list-style-type: none"> 1. 如果新站点上的设备节点已被默认 KMS 加密，请使用 KMS 软件将当前版本的加密密钥从默认 KMS 复制到新 KMS。 2. 使用网络管理器添加新的 KMS 并选择站点。 <p>"添加密钥管理服务器（KMS）"</p>
您希望站点的 KMS 使用其他服务器。	<ol style="list-style-type: none"> 1. 如果站点上的设备节点已由现有 KMS 加密，请使用 KMS 软件将当前版本的加密密钥从现有 KMS 复制到新 KMS。 2. 使用网络管理器编辑现有 KMS 配置并输入新的主机名或 IP 地址。 <p>"添加密钥管理服务器（KMS）"</p>

在 **KMS** 中将 **StorageGRID** 配置为客户端

您必须将 StorageGRID 配置为每个外部密钥管理服务器或 KMS 集群的客户端，然后才能将 KMS 添加到 StorageGRID。

关于此任务

以下说明适用于 Thales CipherTrust Manager。有关支持的版本列表、请使用 "[NetApp 互操作性表工具（IMT）](#)"

"。

步骤

1. 在 KMS 软件中，为计划使用的每个 KMS 或 KMS 集群创建一个 StorageGRID 客户端。

每个 KMS 都会为单个站点或一组站点上的 StorageGRID 设备节点管理一个加密密钥。

2. 在 KMS 软件中，为每个 KMS 或 KMS 集群创建 AES 加密密钥。

加密密钥必须为 2、048 位或更多、并且必须可导出。

3. 记录每个 KMS 或 KMS 集群的以下信息。

将 KMS 添加到 StorageGRID 时需要此信息。

- 每个服务器的主机名或 IP 地址。
- KMS 使用的 KMIP 端口。
- KMS 中加密密钥的密钥别名。



此加密密钥必须已存在于 KMS 中。StorageGRID 不会创建或管理 KMS 密钥。

4. 对于每个 KMS 或 KMS 集群，获取一个由证书颁发机构（CA）签名的服务器证书，或者一个包含 PEM 编码的每个 CA 证书文件的证书捆绑包，这些证书按证书链顺序串联。

通过服务器证书，外部 KMS 可以向 StorageGRID 进行身份验证。

- 证书必须使用 Privacy Enhanced Mail（PEM）Base — 64 编码的 X.509 格式。
- 每个服务器证书中的 "使用者备用名称（SAN）" 字段必须包含 StorageGRID 要连接到的完全限定域名（FQDN）或 IP 地址。



在 StorageGRID 中配置 KMS 时，必须在 * 主机名 * 字段中输入相同的 FQDN 或 IP 地址。

- 服务器证书必须与 KMS 的 KMIP 接口使用的证书匹配，该接口通常使用端口 5696。

5. 获取外部 KMS 颁发给 StorageGRID 的公有客户端证书以及客户端证书的专用密钥。

客户端证书允许 StorageGRID 向 KMS 进行身份验证。

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。

开始之前

- 您已查看 ["使用密钥管理服务器的注意事项和要求"](#)。
- 您已拥有 ["已在 KMS 中将 StorageGRID 配置为客户端"](#)和您具有每个 KMS 或 KMS 集群所需的信息。
- 您将使用登录到网格管理器 ["支持的 Web 浏览器"](#)。

- 您具有 root 访问权限。

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。请参见 ["更改站点的 KMS 的注意事项"](#) 了解详细信息。

第1步：公理详细信息

在添加密钥管理服务器向导的步骤1 (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 * > * 安全性 * > * 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。

Configuration > Key management server

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 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.

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 [Configure key management servers](#).

Create | Actions | Search...

Displaying one result

<input type="checkbox"/>	KMS name	Key name	Manages keys for	Hostname	Certificate expiration
<input type="checkbox"/>	KMS	SG-Global	nmakmipdc1	thales1.vtc.englab.netapp.com and 2 others	All certificates are valid

← Previous 1 Next →

2. 选择 * 创建 *。

此时将显示"Add a Key Management Server"(添加密钥管理服务器)向导的第1步(KMS详细信息)。

×

Add a Key Management Server

1 KMS Details

2 Upload server certificate

3 Upload client certificates

KMS details

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 **Add another hostname** to add a hostname for each server in the cluster.

KMS name ?

Key name ?

Manages keys for ?

Port ?

5696

Hostname ?

Add another hostname

Cancel

Continue

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。
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。

字段	Description
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*不由其他KMS管理的站点(默认KMS)*以配置默认KMS，该KMS将应用于任何没有专用KMS的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> <p>*注意： *服务器证书的使用者替代名称(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。</p>

4. 如果要配置KMS群集，请选择*添加另一主机名*为群集中的每台服务器添加主机名。

5. 选择 * 继续 * 。

第2步：上传服务器证书

在添加密钥管理服务器向导的步骤2 (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 (上载服务器证书)*中，浏览到保存的服务器证书或证书包所在的位置。

Add a Key Management Server

1
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

Previous
Continue

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

1
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

Cert.pem

Server certificate details
Uploaded successfully

Download certificate
Copy certificate PEM

Metadata

Subject DN: /CN=1bdd91b0-3f9e-4934-8b85-83d949e0a43f/UID=nmanohar
Serial number: F8:4C:34:24:2C:CD:22:77:39:1A:BD:07:62:B1:32:D9
Issuer DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued on: 2022-05-23T16:15:24.000Z
Expires on: 2024-05-22T16:15:24.000Z
SHA-1 fingerprint: DF:AF:A8:33:34:69:54:C6:F3:7A:07:DD:17:54:88:DD:11:BB:38:E8
SHA-256 fingerprint: 75:E0:8D:7B:C7:CF:28:87:62:BA:82:4A:46:6F:CD:94:69:C7:B7:82:58:26:3F:58:95:B2:B6:FB:94:70:2B:81
Alternative names:

Previous
Continue



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。

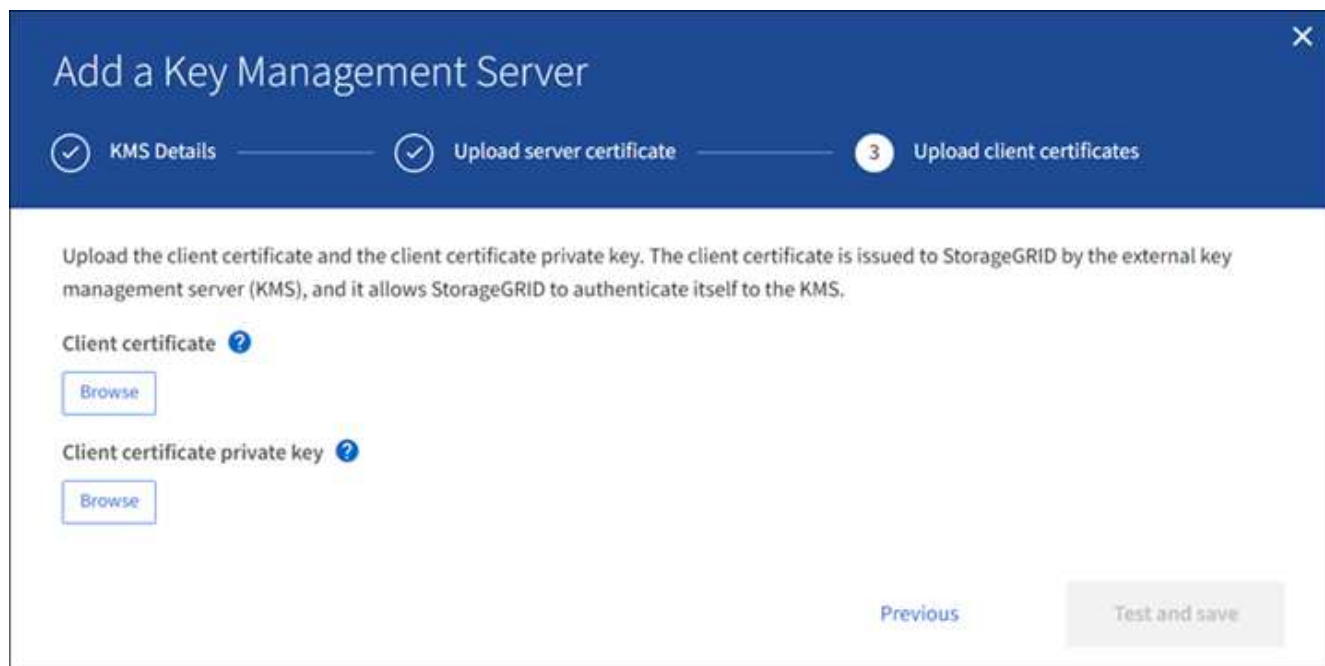
3. 选择 * 继续 *。

第3步：上传客户端证书

在添加密钥管理服务向导的步骤3 (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。



The screenshot shows a web-based wizard titled "Add a Key Management Server". The wizard has three steps: "KMS Details", "Upload server certificate", and "Upload client certificates". The third step is currently active. The main content area explains that the user needs to upload a client certificate and its private key for StorageGRID authentication. There are two "Browse" buttons for uploading these files. At the bottom, there are "Previous" and "Test and save" buttons.

Add a Key Management Server

✓ KMS Details — ✓ Upload server certificate — **3 Upload client certificates**

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 ?

Browse

Client certificate private key ?

Browse

Previous Test and 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。

Add a Key Management Server

1 KMS Details — 2 Upload server certificate — **3 Upload client certificates**

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 ?

✓ Cert.pem

Client certificate details Uploaded successfully

Metadata

Subject DN:	/CN=1bdd91b0-3f9e-4934-8b85-83d949e0a43f/UID=nmanohar
Serial number:	F8:4C:34:24:2C:CD:22:77:39:1A:BD:07:62:B1:32:D9
Issuer DN:	/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued on:	2022-05-23T16:15:24.000Z
Expires on:	2024-05-22T16:15:24.000Z
SHA-1 fingerprint:	DF:AF:A8:33:34:69:54:C6:F3:7A:07:0D:17:54:88:DD:11:BB:38:E8
SHA-256 fingerprint:	75:E0:8D:7B:C7:CF:28:87:62:BA:82:AA:46:6F:CD:94:69:C7:87:82:58:26:8F:56:95:B2:B6:FB:94:70:2B:B1
Alternative names:	

Client certificate private key ?

✓ Key.pem

[Previous](#)

5. 选择*测试并保存*。

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. 如果在选择*测试并保存*时出现错误信息，请查看消息详细信息，然后选择*OK*。

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

7. 如果需要在不测试外部连接的情况下保存当前配置，请选择*Force save*。



选择*强制保存*可保存KMS配置，但不会测试从每个设备到该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。

8. 查看确认警告，如果确实要强制保存配置，请选择 * 确定 *。

已保存 KMS 配置，但未测试与 KMS 的连接。

查看 KMS 详细信息

您可以查看有关 StorageGRID 系统中每个密钥管理服务器（KMS）的信息，包括服务器和客户端证书的当前状态。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 *。

此时将显示密钥管理服务器页面。配置详细信息选项卡将显示已配置的任何密钥管理服务器。

2. 查看每个 KMS 的表中的信息。

字段	Description
Kms名称	KMS 的描述性名称。
密钥名称	KMS 中 StorageGRID 客户端的密钥别名。
管理的密钥	与 KMS 关联的 StorageGRID 站点。 此字段显示特定 StorageGRID 站点的名称或 * 不由其他 KMS （默认 KMS ）管理的站点。 *
主机名	KMS 的完全限定域名或 IP 地址。 如果集群包含两个密钥管理服务器，则会列出这两个服务器的完全限定域名或 IP 地址。如果集群中有两个以上的密钥管理服务器，则会列出第一个 KMS 的完全限定域名或 IP 地址以及集群中其他密钥管理服务器的数量。 例如： 10.10.10.10 and 10.10.10.11 或 10.10.10.10 and 2 others。 要查看集群中的所有主机名，请打开KMS并选择*Edit* 或*Actions*>*Edit*。
证书到期	服务器证书，可选 CA 证书和客户端证书的当前状态：有效，已过期，即将到期或未知。 注意： StorageGRID 可能需要长达30分钟才能获得证书到期更新。您必须刷新 Web 浏览器才能查看当前值。

3. 如果证书到期时间未知、请等待30分钟、然后刷新Web浏览器。



添加KMS后、“密钥管理服务器”页面上的证书过期将立即显示为“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 浏览器才能查看实际状态。

4. 如果证书到期列指示某个证书已到期或即将到期、请尽快联系问题描述。

触发*KMS CA证书到期*、*KMS客户端证书到期*和*KMS服务器证书到期*警报时，请记下每个警报的问题描述 并执行建议的操作。



要保持数据访问，您必须尽快解决任何证书问题。

5. 要查看此KMS的证书详细信息、请从表中选择KMS名称。
6. 在KMS摘要页面上、查看服务器证书和客户端证书的元数据和证书PEM。根据需要，选择*编辑证书*以将证书替换为新证书。

查看加密节点

您可以查看有关 StorageGRID 系统中已启用 * 节点加密 * 设置的设备节点的信息。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 *。

此时将显示密钥管理服务器页面。配置详细信息选项卡显示已配置的任何密钥管理服务器。

2. 从页面顶部选择*加密节点*选项卡。

加密节点选项卡列出了StorageGRID 系统中启用了*Node Encryption *设置的设备节点。

3. 查看表中每个设备节点的信息。

列	Description
Node name	设备节点的名称。
节点类型	节点的类型：存储，管理或网关。
站点	安装节点的 StorageGRID 站点的名称。
Kms名称	用于节点的 KMS 的描述性名称。 如果未列出KMS、请选择配置详细信息选项卡以添加KMS。 "添加密钥管理服务器（ KMS ）"

列	Description
密钥 UID	<p>用于对设备节点上的数据进行加密和解密的加密密钥的唯一 ID 。要查看整个密钥UID、请将光标置于单元格上方。</p> <p>短划线（ - ）表示密钥 UID 未知，可能是因为设备节点和 KMS 之间存在连接问题描述。</p>
Status	<p>KMS 与设备节点之间的连接状态。如果节点已连接，则时间戳每 30 分钟更新一次。更改 KMS 配置后，可能需要几分钟才能更新连接状态。</p> <ul style="list-style-type: none"> • 注意： * 您必须刷新 Web 浏览器才能查看新值。

4. 如果状态列指示 KMS 问题描述，请立即解决此问题描述。

在正常的 KMS 操作期间，状态将为 * 已连接到 KMS* 。如果节点与网格断开连接，则会显示节点连接状态（ administratively down 或 Unknown ）。

其他状态消息对应于同名的 StorageGRID 警报：

- 无法加载 Kms 配置
- Kms 连接错误
- 未找到 Kms 加密密钥名称
- Kms 加密密钥轮换失败
- Kms 密钥无法对设备卷进行解密
- 未配置公里

对这些警报执行建议的操作。



您必须立即解决任何问题，以确保您的数据得到完全保护。

编辑密钥管理服务器（ KMS ）

例如，如果证书即将到期，您可能需要编辑密钥管理服务器的配置。

开始之前

- 您已查看 ["使用密钥管理服务器的注意事项和要求"](#)。
- 如果您计划更新为 KMS 选择的站点，则已查看 ["更改站点的 KMS 的注意事项"](#)。
- 您将使用登录到网格管理器 ["支持的 Web 浏览器"](#)。
- 您具有 root 访问权限。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

此时将显示密钥管理服务器页面、并显示已配置的所有密钥管理服务器。

2. 选择要编辑的KMS，然后选择*Actions*>*Edit*。

您可以通过在表中选择KMS名称并在KMS详细信息页面上选择*Edit*来编辑KMS。

3. (可选)更新编辑密钥管理服务器向导的*步骤1 (KMS详细信息)*中的详细信息。

字段	Description
Kms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。
密钥名称	<div><div>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。</div><div>在极少数情况下，您只需要编辑密钥名称。例如，如果在 KMS 中重命名了别名，或者先前密钥的所有版本都已复制到新别名的版本历史记录中，则必须编辑密钥名称。</div><div><div></div><div>切勿尝试通过更改 KMS 的密钥名称（别名）来旋转密钥。而是通过更新 KMS 软件中的密钥版本来轮换密钥。StorageGRID 要求使用相同密钥别名从 KMS 访问以前使用的所有密钥版本（以及将来的任何密钥版本）。如果更改已配置 KMS 的密钥别名，则 StorageGRID 可能无法对数据进行解密。</div><div>"使用密钥管理服务器的注意事项和要求"</div></div></div>
管理的密钥	<div>如果您正在编辑特定于站点的KMS，并且还没有默认的KMS，则可以选择*不由另一个KMS管理的站点(默认KMS)*。此选择会将特定于站点的KMS转换为默认KMS、这将应用于没有专用KMS的所有站点以及扩展中添加的任何站点。</div> <div>*注:*如果您正在编辑特定于站点的KMS，则不能选择其他站点。如果您正在编辑默认KMS、则无法选择特定站点。</div>
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	<div>KMS 的完全限定域名或 IP 地址。</div> <div>*注意：*服务器证书的使用者替代名称(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。</div>

4. 如果要配置KMS群集，请选择*添加另一主机名*为群集中的每台服务器添加主机名。

5. 选择 * 继续 * 。

此时将显示编辑密钥管理服务器向导的第2步(上传服务器证书)。

6. 如果需要替换服务器证书，请选择 * 浏览 * 并上传新文件。

7. 选择 * 继续 *。

此时将显示编辑密钥管理服务器向导的第3步(上传客户端证书)。

8. 如果需要替换客户端证书和客户端证书专用密钥，请选择 * 浏览 * 并上传新文件。
9. 选择*测试并保存*。

测试密钥管理服务器与受影响站点上的所有节点加密设备节点之间的连接。如果所有节点连接均有效，并且在 KMS 上找到正确的密钥，则密钥管理服务器将添加到密钥管理服务器页面上的表中。

10. 如果显示错误消息，请查看消息详细信息，然后选择 * 确定 *。

例如，如果为此 KMS 选择的站点已由另一个 KMS 管理，或者连接测试失败，则可能会收到 422 : Unprocessable Entity 错误。

11. 如果需要在解决连接错误之前保存当前配置，请选择*Force save*。



选择*强制保存*可保存KMS配置，但不会测试从每个设备到该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。

此时将保存 KMS 配置。

12. 查看确认警告，如果确实要强制保存配置，请选择 * 确定 *。

已保存 KMS 配置，但未测试与 KMS 的连接。

删除密钥管理服务器（ KMS ）

在某些情况下，您可能需要删除密钥管理服务器。例如，如果您已停用站点，则可能需要删除站点专用的 KMS 。

开始之前

- 您已查看 ["使用密钥管理服务器的注意事项和要求"](#)。
- 您将使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您具有 root 访问权限。

关于此任务

在以下情况下，您可以删除 KMS：

- 如果站点已停用，或者站点中没有启用节点加密的设备节点，则可以删除站点专用的 KMS 。
- 如果每个站点已存在站点专用的 KMS，并且已启用设备节点加密，则可以删除默认 KMS 。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 *。

此时将显示密钥管理服务器页面、并显示已配置的所有密钥管理服务器。

2. 选择要删除的KMS，然后选择*Actions*>*Remove*。

您也可以通过在表中选择KMS名称并从KMS详细信息页面中选择*Remove*来删除KMS。

3. 确认满足以下条件：

- 您要删除某个站点的特定于站点的KMS、而此站点没有启用节点加密的设备节点。
- 您要删除默认KMS、但每个站点都已存在具有节点加密的站点专用KMS。

4. 选择 * 是 *。

此时将删除 KMS 配置。

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，本文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。