# 配置密钥管理服务器

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/storagegrid-120/admin/kms-configuring.html on July 23, 2026. Always check docs.netapp.com for the latest.

# 目录

# 配置密钥管理服务器

## 了解 StorageGRID 中的密钥管理服务器

${post_edited_translations.segment}

StorageGRID 支持某些密钥管理服务器。有关受支持产品和版本的列表，请使用 "NetApp 互操作性矩阵工具 (IMT)"。

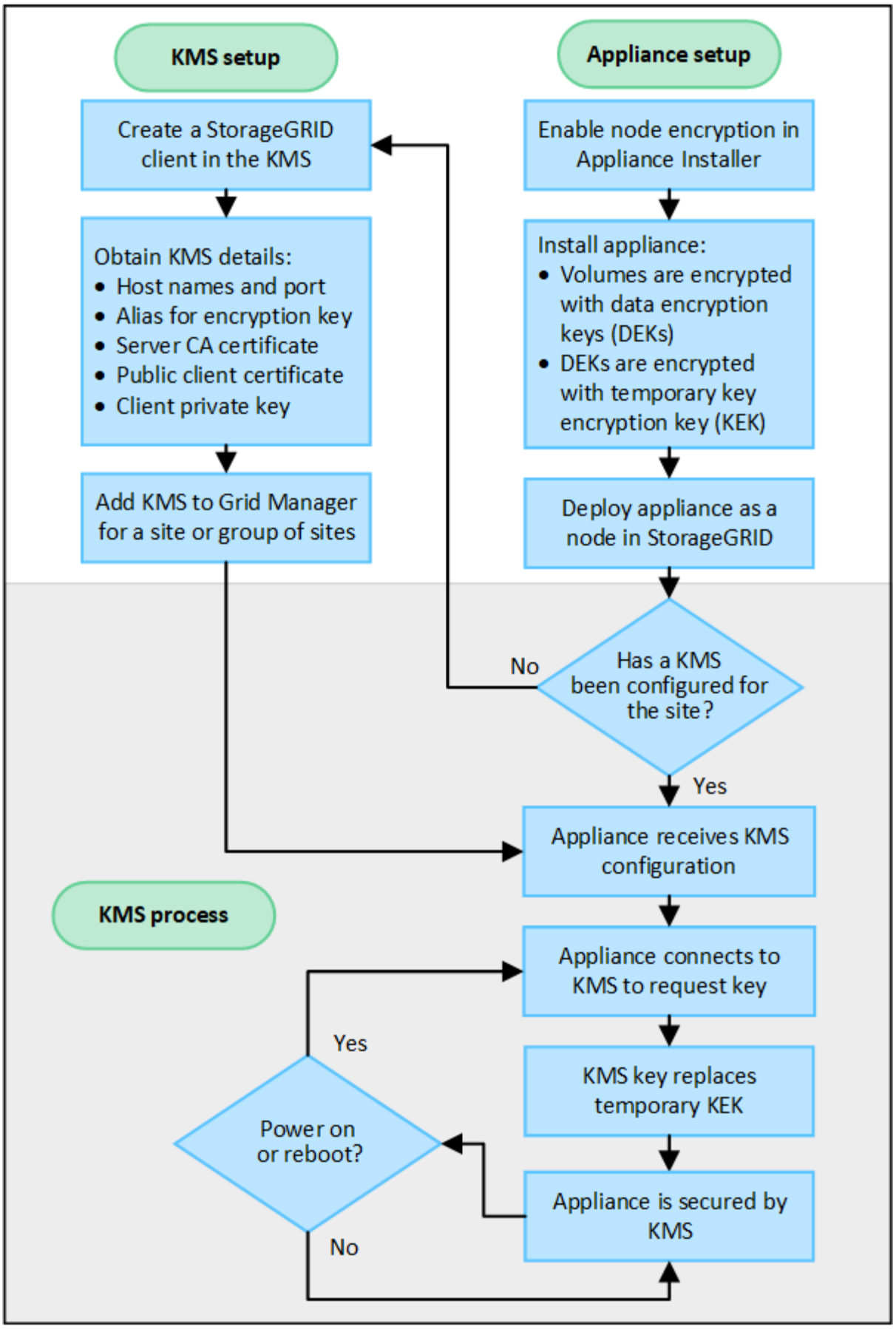
您可以使用一个或多个密钥管理服务器来管理在安装期间启用了 节点加密 设置的任何 StorageGRID 设备节点的节点加密密钥。将密钥管理服务器与这些设备节点结合使用，即使设备从数据中心移出，也可以保护您的数据。在对设备卷进行加密后，除非节点可以与 KMS 进行通信，否则您将无法访问该设备上的任何数据。

> StorageGRID 不创建或管理用于对应用装置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器来保护 StorageGRID 数据，您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。执行密钥管理任务超出了这些说明的范围。如果您需要帮助，请参见密钥管理服务器的文档或联系技术支持。

## StorageGRID 密钥管理服务器和设备配置

在使用密钥管理服务器 (KMS) 保护设备节点上的 StorageGRID 数据之前，您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。

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。




流程图显示并行进行的 KMS 设置和设备设置；但是，您可以根据需求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。

## ${post_edited_translations.segment}

${post_edited_translations.segment}

| 步骤 | 请参阅 |
| --- | --- |
| ${post_edited_translations.segment} | "${post_edited_translations.segment}" |
| 在 KMS 上获取 StorageGRID 客户端所需的信息。 | "${post_edited_translations.segment}" |
| 将 KMS 添加到网格管理器，将其分配给单个站点或默认站点组，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

设置用于 KMS 的设备节点包括以下高级步骤。

1. ${post_edited_translations.segment}

> 将设备添加到网格后，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 装置安装程序。在安装过程中，系统会为每个装置卷分配一个随机数据加密密钥 (DEK)，如下所示：
   - DEK 用于加密每个卷上的数据。这些密钥是使用设备 OS 中的 Linux Unified Key Setup (LUKS) 磁盘加密生成的，且无法更改。
   - 每个 DEK 都由主密钥加密密钥（KEK）加密。初始 KEK 是一个临时密钥，用于加密 DEK，直到设备可以连接到 KMS。
3. ${post_edited_translations.segment}

有关详细信息，请参见 "启用节点加密"。

## ${post_edited_translations.segment}

${post_edited_translations.segment}

1. 当您将启用了节点加密的设备安装到网格中时，StorageGRID 会确定包含新节点的站点是否存在 KMS 配置。
   - ${post_edited_translations.segment}
   - 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 并且设备收到 KMS 配置。
2. 设备使用 KMS 配置连接到 KMS 并请求加密密钥。
3. KMS 向设备发送加密密钥。来自 KMS 的新密钥取代了临时 KEK，现在用于加密和解密设备卷的 DEK。

在加密设备节点连接到配置的 KMS 之前存在的任何数据都会使用临时密钥进行加密。但是，在临时密钥被 KMS 加密密钥替换之前，不应认为设备卷已受到保护，可防止从数据中心中被移除。

4. 如果设备已通电或重新启动，则会重新连接到 KMS 以请求密钥。密钥保存在易失性内存中，无法在断电或重新启动后保留。

# StorageGRID 密钥管理服务器要求和注意事项

${post_edited_translations.segment}

## ${post_edited_translations.segment}

StorageGRID 支持 KMIP 版本 1.4。

"密钥管理互操作性协议规范 1.4 版"

### 网络注意事项有哪些?

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(KMIP)通信的端口进行通信。默认 KMIP 端口为 5696。

您必须确保使用节点加密的每个设备节点都具有对您为该站点配置的 KMS 或 KMS 集群的网络访问权限。

### 支持哪些版本的 TLS?

设备节点与配置的 KMS 之间的通信使用安全的 TLS 连接。StorageGRID 在与 KMS 或 KMS 集群建立 KMIP 连接时，可以支持 TLS 1.2 或 TLS 1.3 协议，具体取决于 KMS 支持的协议以及您正在使用的 "TLS和SSH策略"。

StorageGRID 在建立连接时与 KMS 协商协议和密码（TLS 1.2）或密码套件（TLS 1.3）。要查看可用的协议版本和密码/密码套件，请查看网格的活动 TLS 和 SSH 策略的 `tlsOutbound`部分（配置 > 安全 安全设置）。

### 支持哪些设备?

您可以使用密钥管理服务器(KMS)管理网格中已启用*节点加密*设置的任何 StorageGRID 设备的加密密钥。此设置只能在使用 StorageGRID Appliance Installer 安装设备的硬件配置阶段启用。

将设备添加到网格后，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。

您可以将配置的 KMS 用于 StorageGRID 设备和设备节点。

您不能将配置的 KMS 用于基于软件的（非设备）节点，其中包括：

- 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

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

## 何时应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 Grid Manager 中设置一个或多个密钥管理服务器。此顺序可确保在节点上存储任何对象数据之前对其进行保护。

您可以在安装设备节点之前或之后在 Grid Manager 中配置密钥管理服务器。

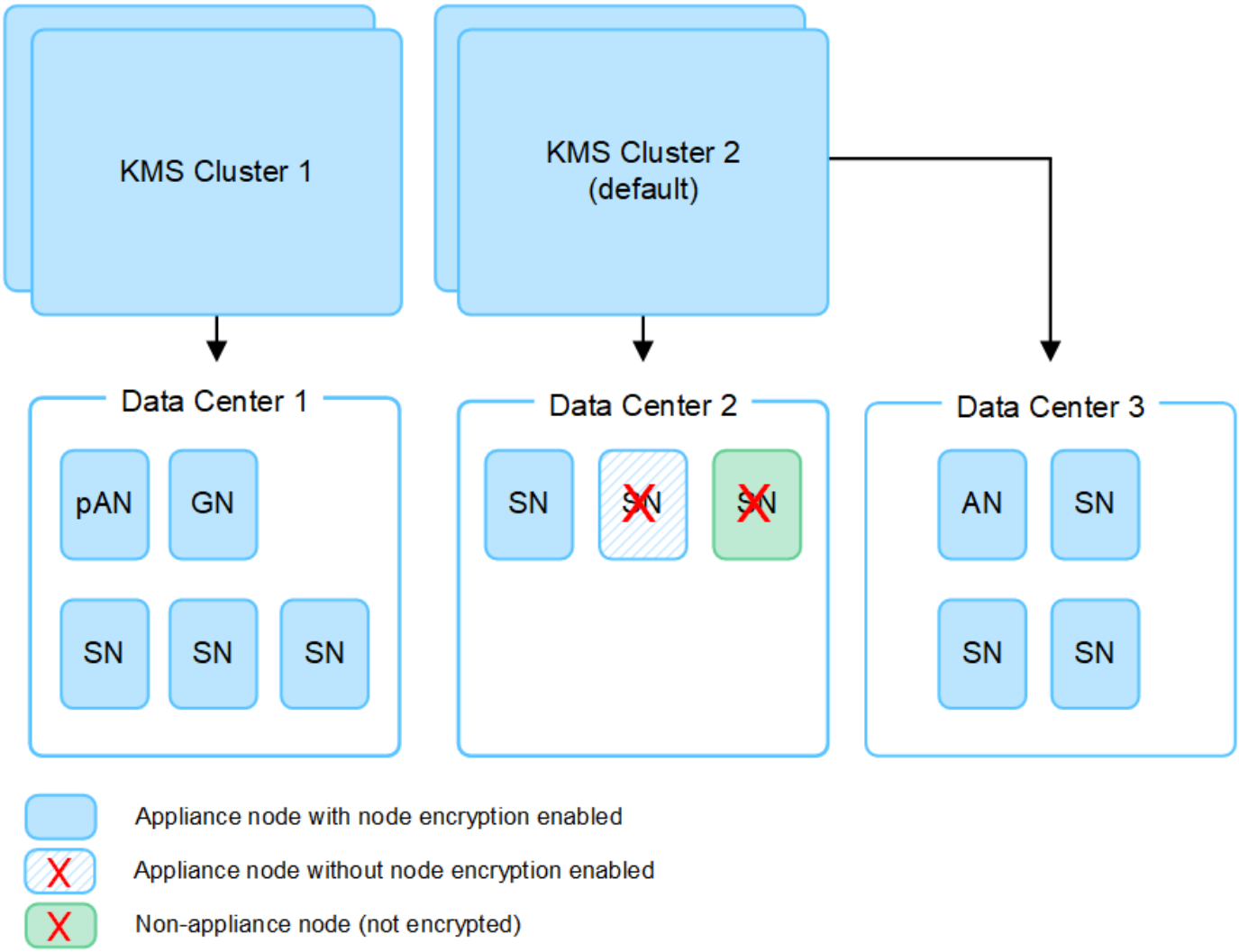
## 我需要多少密钥管理服务器?

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

StorageGRID 支持使用 KMS 集群。每个 KMS 集群包含多个共享配置设置和加密密钥的复制密钥管理服务器。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能力。

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 集群配置为向数据中心 1 的所有设备节点提供密钥，并将另一个 KMS 集群配置为向所有其他站点的所有设备节点提供密钥。添加第二个 KMS 集群时，可以为数据中心 2 和数据中心 3 配置默认 KMS。

请注意，您不能将 KMS 用于非设备节点或安装期间未启用*节点加密*设置的任何设备节点。



### 轮换密钥时会发生什么?

作为安全最佳做法，您应定期"轮换加密密钥"每个已配置的 KMS 所使用的内容。

当新的密钥版本可用时：

- 它会自动分发到与 KMS 关联的一个或多个站点上的加密设备节点。分发应在密钥轮换后的一小时内完成。
- 如果在分发新密钥版本时加密的设备节点处于离线状态，则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应用装置卷进行加密，则会针对该应用装置节点触发 **KMS** 加密密钥轮换失败 警报。您可能需要联系技术支持以协助解决此警报。

### ${post_edited_translations.segment}

如果需要将加密设备安装到另一个 StorageGRID 系统中，则必须首先停用网格节点以将对象数据移动到另一个节点。然后，您可以使用 StorageGRID Appliance Installer "清除 KMS 配置"。清除 KMS 配置将禁用 **Node Encryption** 设置，并删除设备节点与 StorageGRID 站点的 KMS 配置之间的关联。

由于无法访问 KMS 加密密钥，设备上的任何剩余数据将无法再被访问，并被永久锁定。

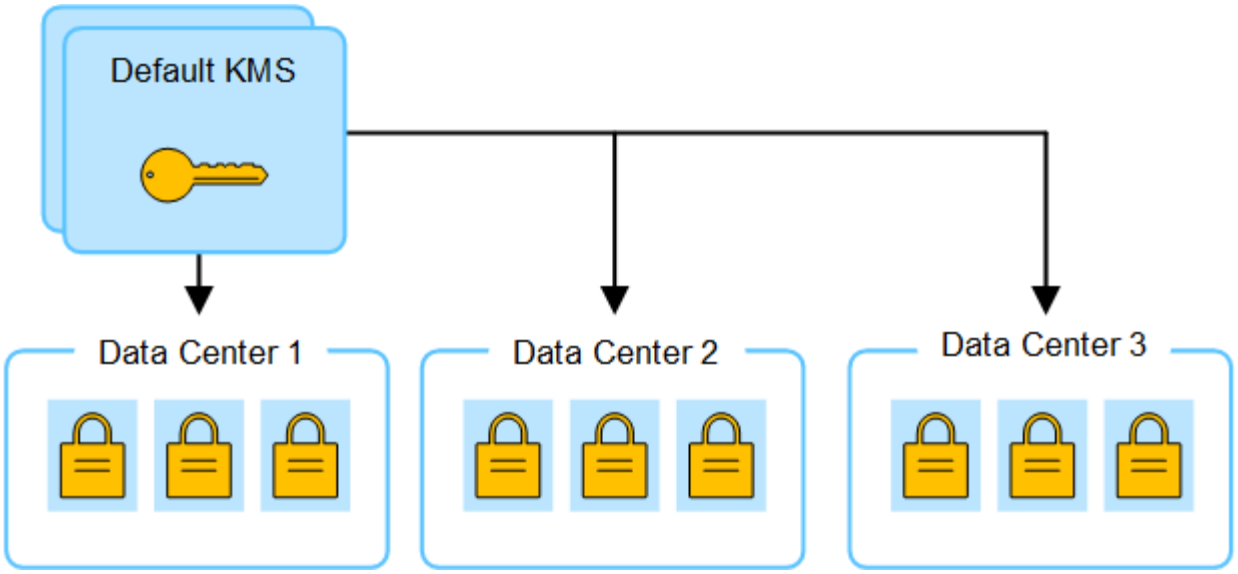
# 更改 StorageGRID 站点 KMS 的注意事项

## 每个密钥管理服务器(KMS)或 KMS 集群为单个站点或一组站点的所有设备节点提供加密密钥。如果您需要更改用于站点的 KMS，则可能需要将加密密钥从一个 KMS 复制到另一个 KMS。

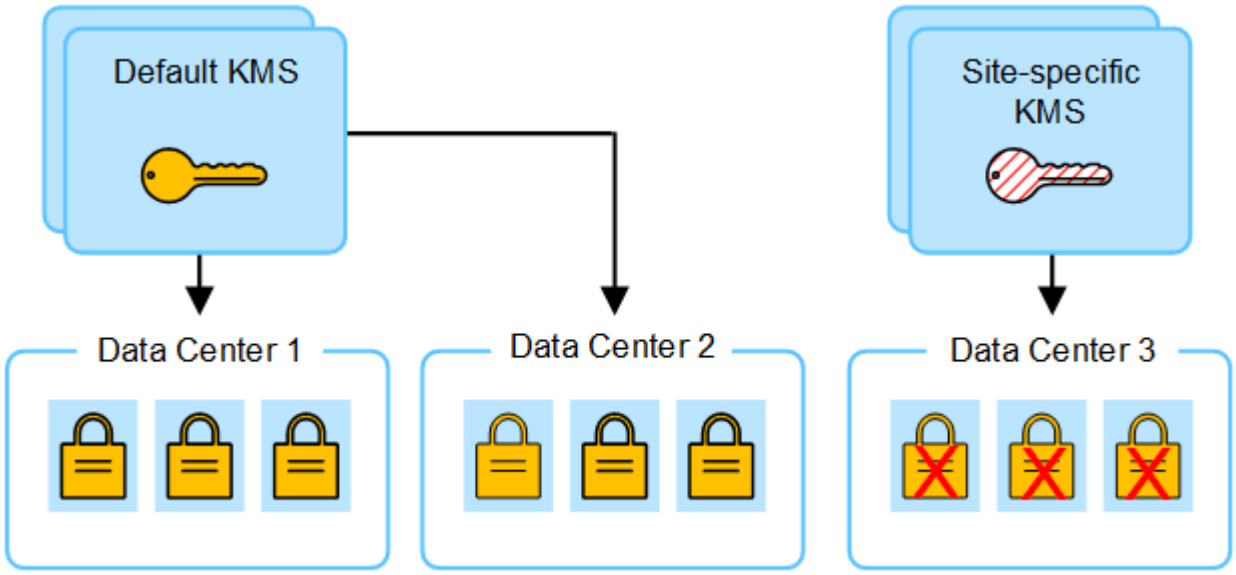
如果您更改了用于某个站点的 KMS，则必须确保可以使用存储在新 KMS 上的密钥对该站点上先前加密的设备节点进行解密。在某些情况下，您可能需要将当前版本的加密密钥从原始 KMS 复制到新 KMS。您必须确保 KMS 具有正确的密钥，以便对该站点上加密的设备节点进行解密。

例如：

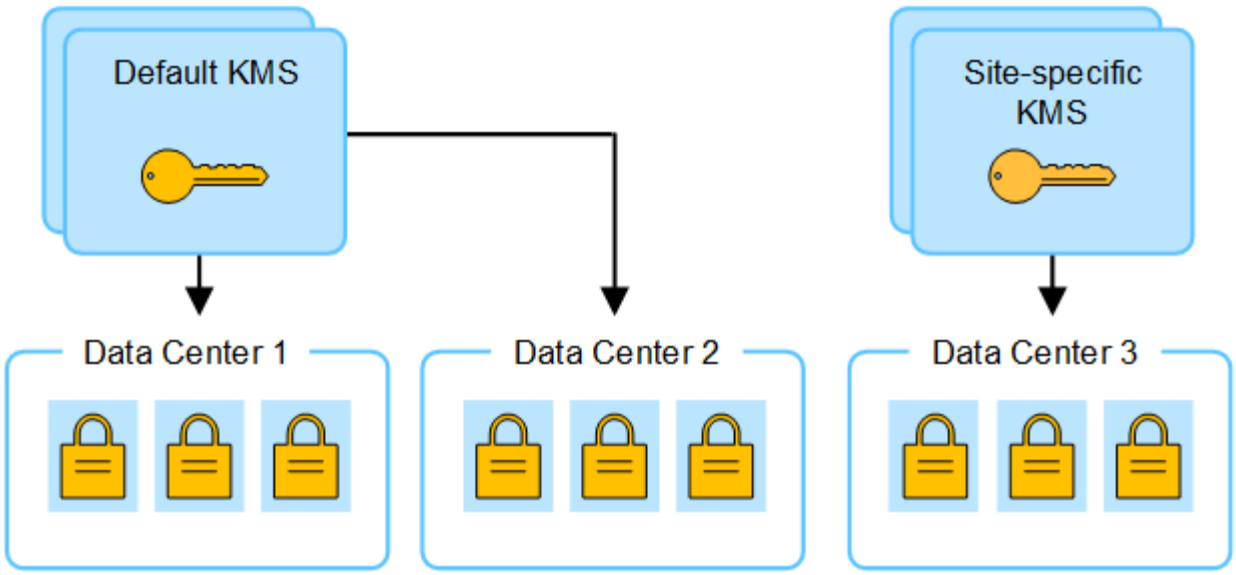
1. ${post_edited_translations.segment}
2. 保存 KMS 时，所有启用了 节点加密 设置的设备节点都会连接到 KMS 并请求加密密钥。此密钥用于加密所有站点上的设备节点。必须使用同一密钥对这些设备进行解密。




3. 您决定为一个站点添加特定于站点的 KMS（图中的数据中心 3）。但是，由于设备节点已加密，因此在尝试保存站点特定 KMS 的配置时会出现验证错误。此错误的原因是站点特定的 KMS 没有正确的密钥来解密该站点上的节点。




4. 要解决此问题，请将当前版本的加密密钥从默认 KMS 复制到新 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。）站点特定的 KMS 现在具有正确的密钥来解密 Data Center 3 的设备节点，因此可以将其保存在 StorageGRID 中。




### 用于更改站点使用的 **KMS** 的用例

该表总结了更改站点 KMS 的最常见情况所需的步骤。

| 更改站点 **KMS** 的用例 | 所需步骤 |
| --- | --- |
| ${post_edited_translations.segment} | 编辑站点特定的 KMS。在 **Manages keys for** 字段中，选择 **Sites not managed by another KMS (default KMS)**。站点特定的 KMS 现在将用作默认 KMS。它将适用于任何没有专用 KMS 的站点。<br><br>"编辑密钥管理服务器（KMS）" |
| 您拥有默认 KMS，并在扩容中添加了新站点。您不想对新站点使用默认 KMS。 | 1. ${post_edited_translations.segment}<br>2. ${post_edited_translations.segment}<br><br>"添加密钥管理服务器 (KMS)" |
| 您希望站点的 KMS 使用其他服务器。 | 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。<br>2. 使用 Grid Manager，编辑现有 KMS 配置并输入新的主机名或 IP 地址。<br><br>"添加密钥管理服务器 (KMS)" |

# ${post_edited_translations.segment}

在将 KMS 添加到 StorageGRID 之前，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。

这些说明适用于 Thales CipherTrust Manager 和 Hashicorp Vault。有关受支持产品和版本的列表，请使用 "NetApp 互操作性矩阵工具 (IMT)"。

步骤

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

   ${post_edited_translations.segment}

2. 使用以下两种方法之一创建密钥：

   - 使用 KMS 产品的密钥管理页面。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。

   - 让 StorageGRID 创建密钥。在 "上传客户端证书" 之后进行测试并保存时，系统将提示您。

3. 记录每个KMS或KMS集群的以下信息。

   将 KMS 添加到 StorageGRID 时，您需要以下信息：

   - 每台服务器的主机名或 IP 地址。
   - KMS 使用的 KMIP 端口。
   - ${post_edited_translations.segment}

4. 对于每个 KMS 或 KMS 集群，获取由证书颁发机构 (CA) 签名的服务器证书，或包含以证书链顺序连接的每个 PEM 编码的 CA 证书文件的证书包。

   ${post_edited_translations.segment}

   - 证书必须使用隐私增强邮件 (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将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 **Hostname** 字段中输入相同的 FQDN 或 IP 地址。

   - ${post_edited_translations.segment}

5. 获取外部 KMS 颁发给 StorageGRID 的公共客户端证书和客户端证书的私钥。

   客户端证书允许StorageGRID向KMS进行身份验证。

# 在 StorageGRID 中添加密钥管理服务器

${post_edited_translations.segment}

开始之前

- 您已审阅 "使用密钥管理服务器的注意事项和要求"。
- 您拥有"在 KMS 中将 StorageGRID 配置为客户端"，并且您拥有每个KMS或KMS集群所需的信息。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

关于此任务

如果可能，在配置适用于不由其他 KMS 管理的所有站点的默认 KMS 之前，请配置任何特定于站点的密钥管理服务器。如果首先创建默认 KMS，则网格中的所有节点加密设备都将使用默认 KMS 进行加密。如果要在以后创建站点特定的 KMS，则必须首先将当前版本的加密密钥从默认 KMS 复制到新 KMS。有关详细信息，请参阅"更改站点 KMS 的注意事项"。

## 步骤 1：KMS 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，提供有关 KMS 或 KMS 集群的详细信息。

步骤

1. 选择*配置* > 安全 > 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。

2. 选择 **Create**。

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

| 字段 | 问题描述 |
| --- | --- |
| KMS 名称 | 用于帮助您识别此 KMS 的描述性名称。必须介于 1 到 64 个字符之间。 |
| 密钥名称 | KMS 中 StorageGRID 客户端的确切密钥别名。必须介于 1 到 255 个字符之间。<br><br>注意：如果您尚未使用 KMS 产品创建密钥，系统将提示您让 StorageGRID 创建密钥。 |
| ${post_edited_translations.segment} | 将与此 KMS 关联的 StorageGRID 站点。如果可能，应先配置特定站点的密钥管理服务器，再配置适用于所有非其他 KMS 管理站点的默认 KMS。<br><br>• 如果此 KMS 将管理特定站点上设备节点的加密密钥，请选择一个站点。<br>• 选择 **Sites not managed by another KMS (default KMS)** 以配置默认 KMS，该默认 KMS 将应用于没有专用 KMS 的任何站点以及您在后续扩展中添加的任何站点。<br><br>${post_edited_translations.segment} |
| 端口 | KMS 服务器用于密钥管理互操作性协议 (KMIP) 通信的端口。默认为 5696，即 KMIP 标准端口。 |

| 字段 | 问题描述 |
| --- | --- |
| 主机名称 | ${post_edited_translations.segment}<br><br>注意： 服务器证书的“主题备用名称 (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。 |

4. 如果要配置 KMS 集群，请选择 添加另一个主机名 为集群中的每个服务器添加主机名。
5. 选择 **Continue**。

## ${post_edited_translations.segment}

在“添加密钥管理服务器”向导的第 2 步（上传服务器证书）中，您需要上传 KMS 的服务器证书（或证书包）。服务器证书允许外部 KMS 向 StorageGRID 进行自身身份验证。

步骤

1. ${post_edited_translations.segment}
2. 上传证书文件。

   此时将显示服务器证书元数据。

   ${post_edited_translations.segment}

3. 选择 **Continue**。

## ${post_edited_translations.segment}

在添加密钥管理服务器向导的步骤 3（上载客户端证书）中，上载客户端证书和客户端证书私钥。客户端证书允许 StorageGRID 向 KMS 进行身份验证。

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

3. 浏览到客户端证书专用密钥的位置。
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

   如果密钥不存在，系统会提示您让 StorageGRID 创建一个密钥。

   测试密钥管理服务器和设备节点之间的连接。如果所有连接都有效，并且在 KMS 上找到了正确的密钥，则会将新的密钥管理服务器添加到"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. ${post_edited_translations.segment}

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

7. ${post_edited_translations.segment}

   选择*强制保存*将保存 KMS 配置，但不会测试每个设备到该 KMS 的外部连接。如果配置出现问题，则可能无法重新启动在受影响站点上启用了节点加密的设备节点。在问题得到解决之前，您可能会失去对数据的访问权限。

8. 查看确认警告，如果确定要强制保存配置，请选择*OK*。

   ${post_edited_translations.segment}

# 在 StorageGRID 中管理密钥管理服务器

管理密钥管理服务器 (KMS) 涉及查看或编辑详细信息、管理证书、查看加密节点以及在不再需要时删除 KMS。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "所需的访问权限"。

## 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，包括密钥详细信息以及服务器和客户端证书的当前状态。

步骤

1. 选择*配置* > 安全 > 密钥管理服务器。

   此时将显示密钥管理服务器页面，并显示以下信息：

   - 配置详细信息选项卡列出了已配置的任何密钥管理服务器。
   - 已加密节点选项卡列出已启用节点加密的任何节点。

2. 要查看特定 KMS 的详细信息并对该 KMS 执行操作，请选择 KMS 的名称。KMS 的详细信息页面列出了以下信息：

| 字段 | 问题描述 |
| --- | --- |
| ${post_edited_translations.segment} | 与 KMS 关联的 StorageGRID 站点。<br><br>此字段显示特定 StorageGRID 站点或*不由其他 KMS 管理的站点的名称（默认 KMS）。* |
| 主机名称 | KMS 的完全限定域名或 IP 地址。<br><br>如果有两个密钥管理服务器的集群，则列出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。<br><br>例如： `10.10.10.10 and 10.10.10.11` 或 `10.10.10.10 and 2 others`。<br><br>要查看集群中的所有主机名，请选择一个 KMS 并选择*编辑*或*操作* > 编辑。 |

3. 在 KMS 详细信息页面上选择一个选项卡以查看以下信息：

| 选项卡 | 字段 | 问题描述 |
| --- | --- | --- |
| 关键详细信息 | 密钥名称 | KMS 中 StorageGRID 客户端的密钥别名。 |
| 密钥 UID | 最新版本密钥的唯一标识符。 | 上次修改时间 |
| 最新版本密钥的日期和时间。 | 服务器证书 | 元数据 |
| 证书的元数据，例如序列号、到期日期和时间以及证书 PEM。 | 证书 PEM | 证书的 PEM（隐私增强邮件）文件的内容。 |
| 客户端证书 | 元数据 | 证书的元数据，例如序列号、到期日期和时间以及证书 PEM。 |

4. 根据组织安全实践的要求，选择*Rotate key*，或使用 KMS 软件创建新版本的密钥。

密钥轮换成功后，将更新密钥 UID 和上次修改字段。

> 如果您使用 KMS 软件轮换加密密钥，请将其从该密钥上次使用的版本轮换为同一密钥的新版本。请勿轮换为完全不同的密钥。
>
> 切勿尝试通过更改 KMS 的密钥名称（别名）来轮换密钥。StorageGRID 要求所有以前使用的密钥版本（以及任何未来的密钥版本）都可以使用相同的密钥别名从 KMS 访问。如果更改已配置的 KMS 的密钥别名，StorageGRID 可能无法解密您的数据。

## 管理证书

及时解决任何服务器或客户端证书问题。如果可能，请在证书过期前更换。

您必须尽快解决任何证书问题，以保持数据访问权限。

步骤

1. 选择*配置* > 安全 > 密钥管理服务器。
2. 在表中，查看每个 KMS 的证书过期值。
3. 如果任何 KMS 的证书过期时间为未知，请等待最多 30 分钟，然后刷新您的 Web 浏览器。
4. ${post_edited_translations.segment}
   a. 选择 **Server certificate** 并验证"Expires on"字段的值。
   b. 要替换证书，请选择*编辑证书*以上传新证书。
   c. 重复这些子步骤，选择*客户端证书*而不是服务器证书。
5. 当 **KMS CA** 证书过期、*KMS 客户端证书过期*和 *KMS 服务器证书过期*警报触发时，请注意每个警报的描述并执行建议的操作。

   StorageGRID 可能需要长达 30 分钟才能获取证书过期的更新。刷新 Web 浏览器以查看当前值。

${post_edited_translations.segment}

## 查看加密节点

您可以查看有关在您的 StorageGRID 系统中启用了 **Node Encryption** 设置的设备节点的信息。

步骤

1. 选择*配置* > 安全 > 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. ${post_edited_translations.segment}

   加密节点选项卡列出了 StorageGRID 系统中已启用*节点加密*设置的设备节点。

3. 查看表格中每个设备节点的信息。

| 列 | 问题描述 |
| --- | --- |
| 节点名称 | ${post_edited_translations.segment} |
| 节点类型 | 节点的类型：Storage、Admin 或 Gateway。 |
| 站点 | 安装节点的 StorageGRID 站点的名称。 |

| 列 | 问题描述 |
| --- | --- |
| KMS 名称 | 用于节点的KMS的描述性名称。<br><br>如果未列出 KMS，请选择"配置详细信息"选项卡以添加 KMS。<br><br>"添加密钥管理服务器 (KMS)" |
| 密钥 UID | 用于对应用装置节点上的数据进行加密和解密的加密密钥的唯一 ID。要查看完整的密钥 UID，请选择该文本。<br><br>破折号(--)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。 |
| 状态 | 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，连接状态可能需要几分钟才能更新。<br><br>*注意：*刷新您的网络浏览器以查看新值。 |

4. ${post_edited_translations.segment}

   在正常的 KMS 操作期间，状态将为 **Connected to 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：

   - ${post_edited_translations.segment}
   - KMS 连接错误
   - 未找到 KMS 加密密钥名称
   - KMS加密密钥轮换失败
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

${post_edited_translations.segment}

> 您必须立即解决任何问题，以确保您的数据得到充分保护。

## 编辑 KMS

您可能需要编辑密钥管理服务器的配置，例如，如果证书即将过期。

开始之前

- 如果您计划更新为 KMS 选择的站点，则表示您已阅读 "${post_edited_translations.segment}"。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

步骤

1. 选择*配置* > 安全 > 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. ${post_edited_translations.segment}

   您还可以通过在表中选择KMS名称并在KMS详细信息页面上选择*编辑*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 | 问题描述 |
| --- | --- |
| KMS 名称 | 用于帮助您识别此 KMS 的描述性名称。必须介于 1 到 64 个字符之间。 |
| 密钥名称 | KMS 中 StorageGRID 客户端的确切密钥别名。必须介于 1 到 255 个字符之间。<br><br>您只需要在极少数情况下编辑密钥名称。例如，如果别名在 KMS 中重命名，或者如果上一个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。 |
| ${post_edited_translations.segment} | 如果您正在编辑特定于站点的 KMS，并且尚无默认 KMS，则可以选择 未由其他 **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，该 KMS 将适用于所有没有专用 KMS 的站点以及在扩容中添加的任何站点。<br><br>*注意：*如果您正在编辑特定于站点的 KMS，则无法选择其他站点。如果您正在编辑默认 KMS，则无法选择特定站点。 |
| 端口 | KMS 服务器用于密钥管理互操作性协议 (KMIP) 通信的端口。默认为 5696，即 KMIP 标准端口。 |
| 主机名称 | ${post_edited_translations.segment}<br><br>注意： 服务器证书的“主题备用名称 (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。 |

4. 如果要配置 KMS 集群，请选择 添加另一个主机名 为集群中的每个服务器添加主机名。
5. 选择 **Continue**。

   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. 如果需要更换服务器证书，请选择*浏览*并上传新文件。
7. 选择 **Continue**。

   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. ${post_edited_translations.segment}

9. ${post_edited_translations.segment}

   对受影响站点的密钥管理服务器和所有节点加密设备节点之间的连接进行了测试。如果所有节点连接都有效，并且在 KMS 上找到了正确的密钥，则会将密钥管理服务器添加到"密钥管理服务器"页面上的表中。

10. 如果出现错误消息，请查看消息详情，然后选择*OK*。

    ${post_edited_translations.segment}

11. 如果需要在解决连接错误之前保存当前配置，请选择*强制保存*。

    > 选择*强制保存*将保存 KMS 配置，但不会测试每个设备到该 KMS 的外部连接。如果配置出现问题，则可能无法重新启动在受影响站点上启用了节点加密的设备节点。在问题得到解决之前，您可能会失去对数据的访问权限。

    KMS 配置已保存。

12. 查看确认警告，如果确定要强制保存配置，请选择*OK*。

    已保存 KMS 配置，但未测试与 KMS 的连接。

## ${post_edited_translations.segment}

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，则可能需要删除特定于站点的KMS。

开始之前

- 您已审阅 "使用密钥管理服务器的注意事项和要求"。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

关于此任务

在以下情况下，您可以删除 KMS：

- 如果站点已停用或站点不包括启用了节点加密的设备节点，则可以删除站点特定的KMS。
- ${post_edited_translations.segment}

步骤

1. 选择*配置* > 安全 > 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*操作* > 删除。

   ${post_edited_translations.segment}

3. 确认是否满足以下条件：
   - ${post_edited_translations.segment}

- 您正在删除默认的 KMS，但每个具有节点加密的站点已经存在特定于站点的 KMS。

4. ${post_edited_translations.segment}

   已删除 KMS 配置。

版权信息

版权所有 © 2026 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。