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"

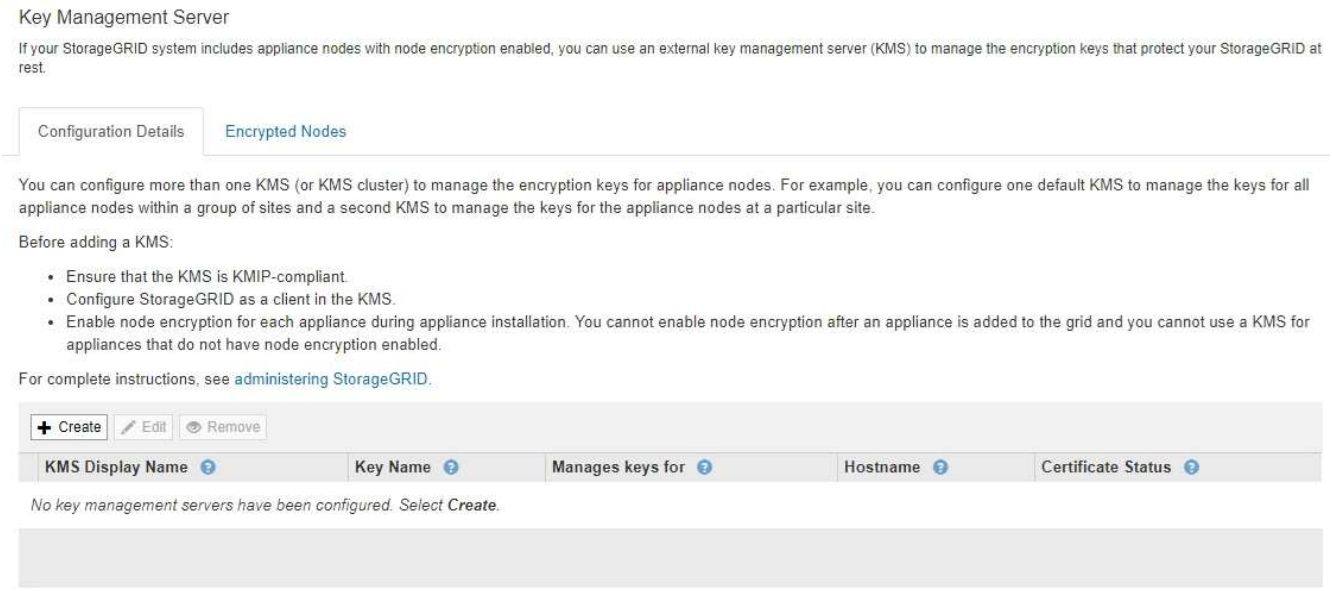
第 1 步：输入 KMS 详细信息

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

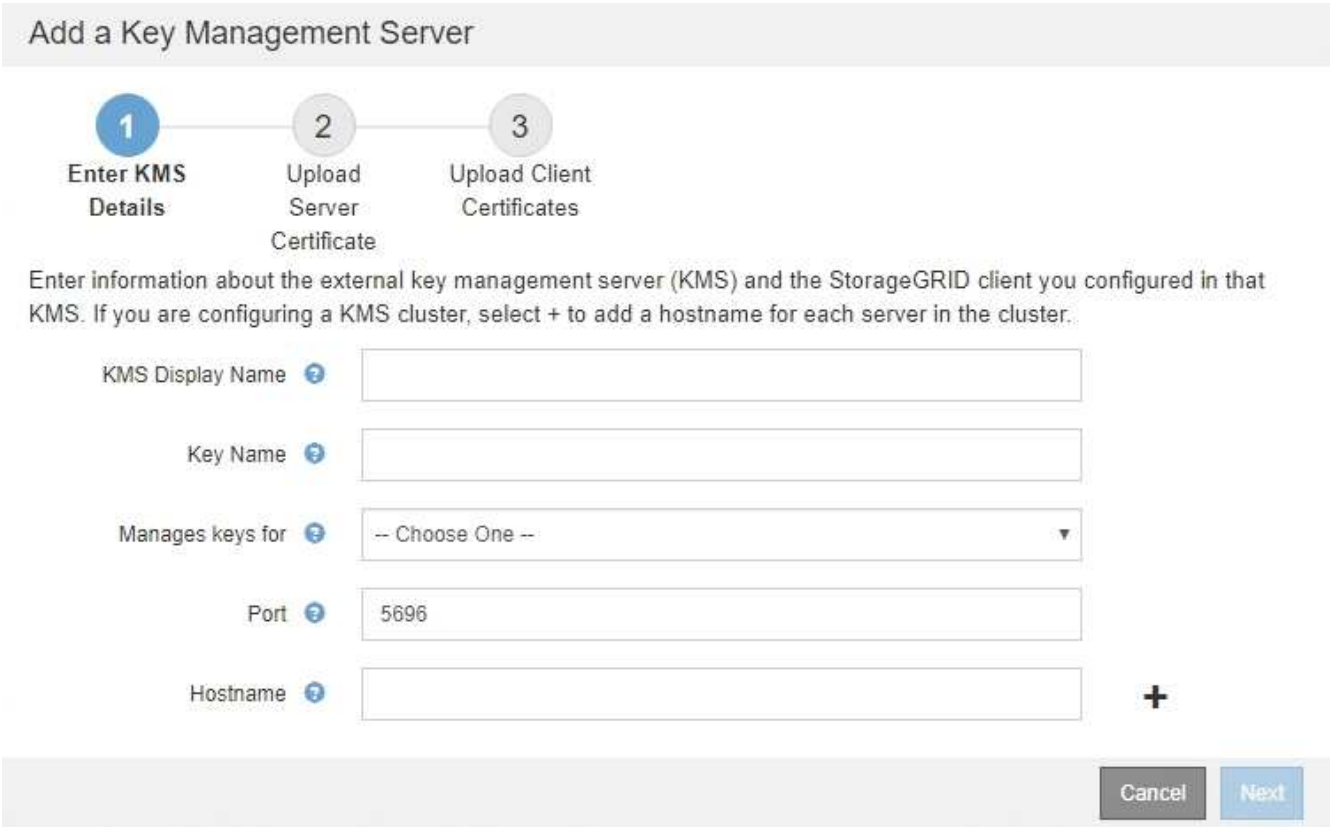
1. 选择*配置系统设置密钥管理服务器*。

   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。



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）。



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	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 。 • 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。 ◦ 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	KMS 的完全限定域名或 IP 地址。 • 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 * 。

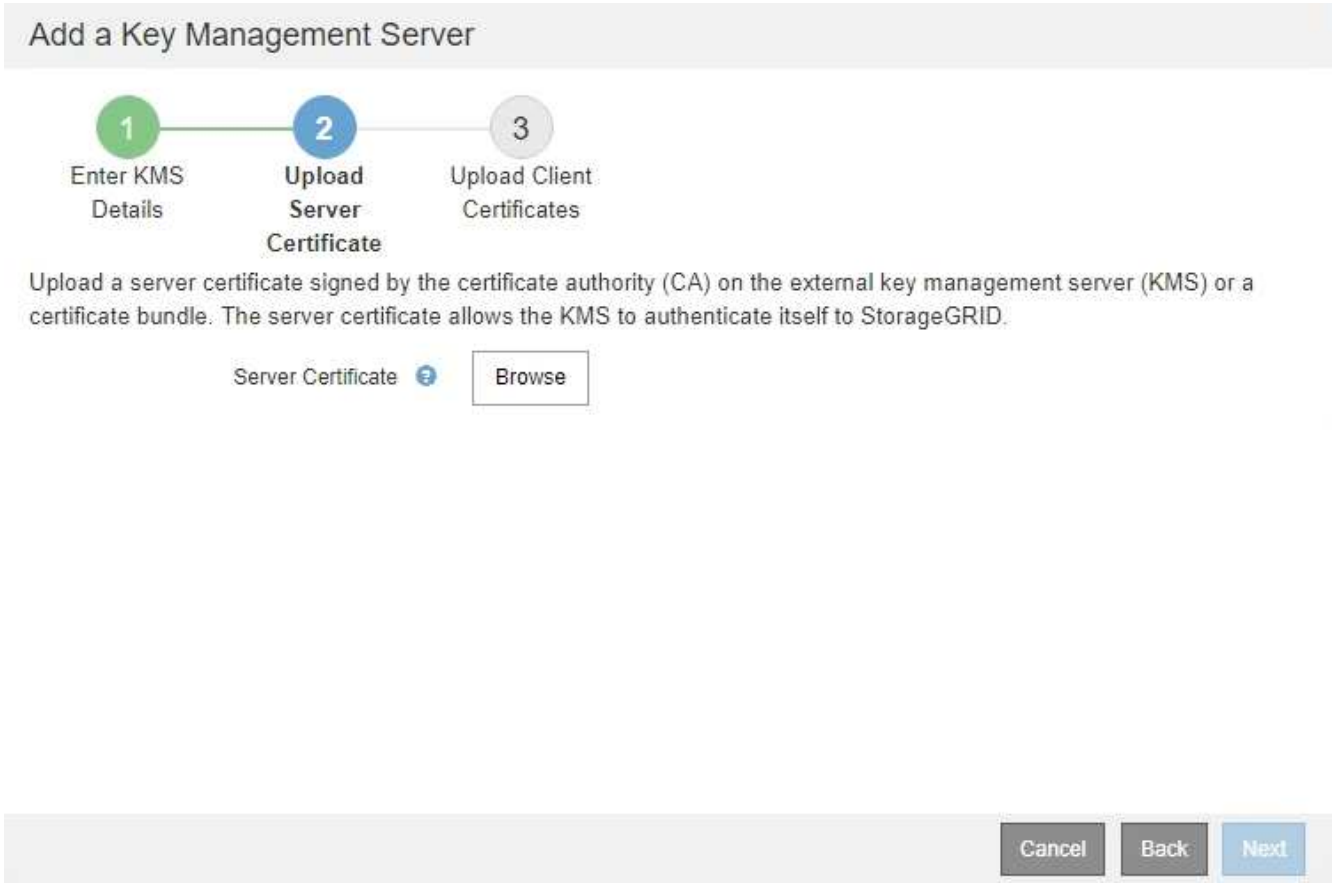
   此时将显示添加密钥管理服务器向导的第2步(上传服务器证书)。

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。

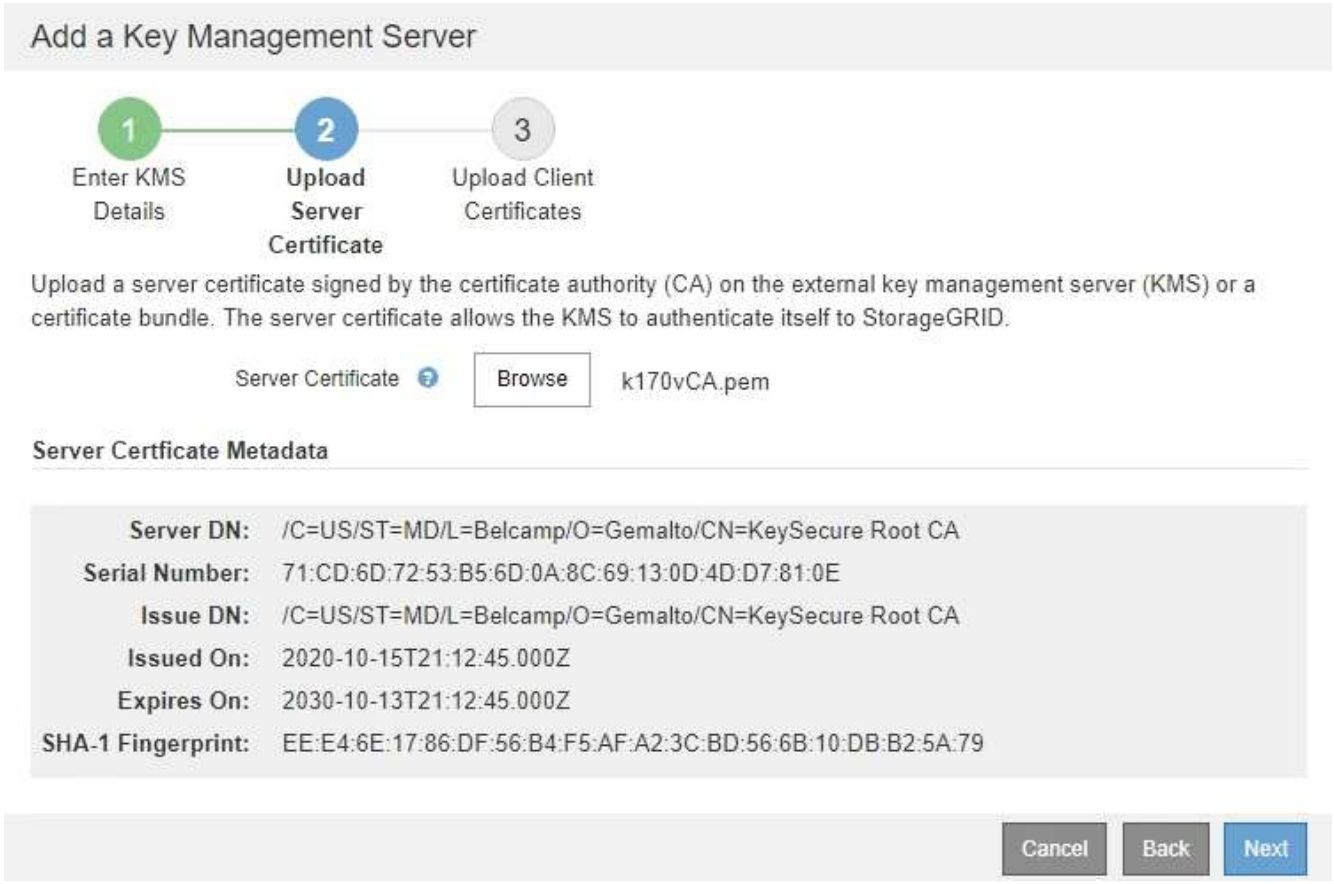
步骤

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。



2. 上传证书文件。

   此时将显示服务器证书元数据。



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 * 。

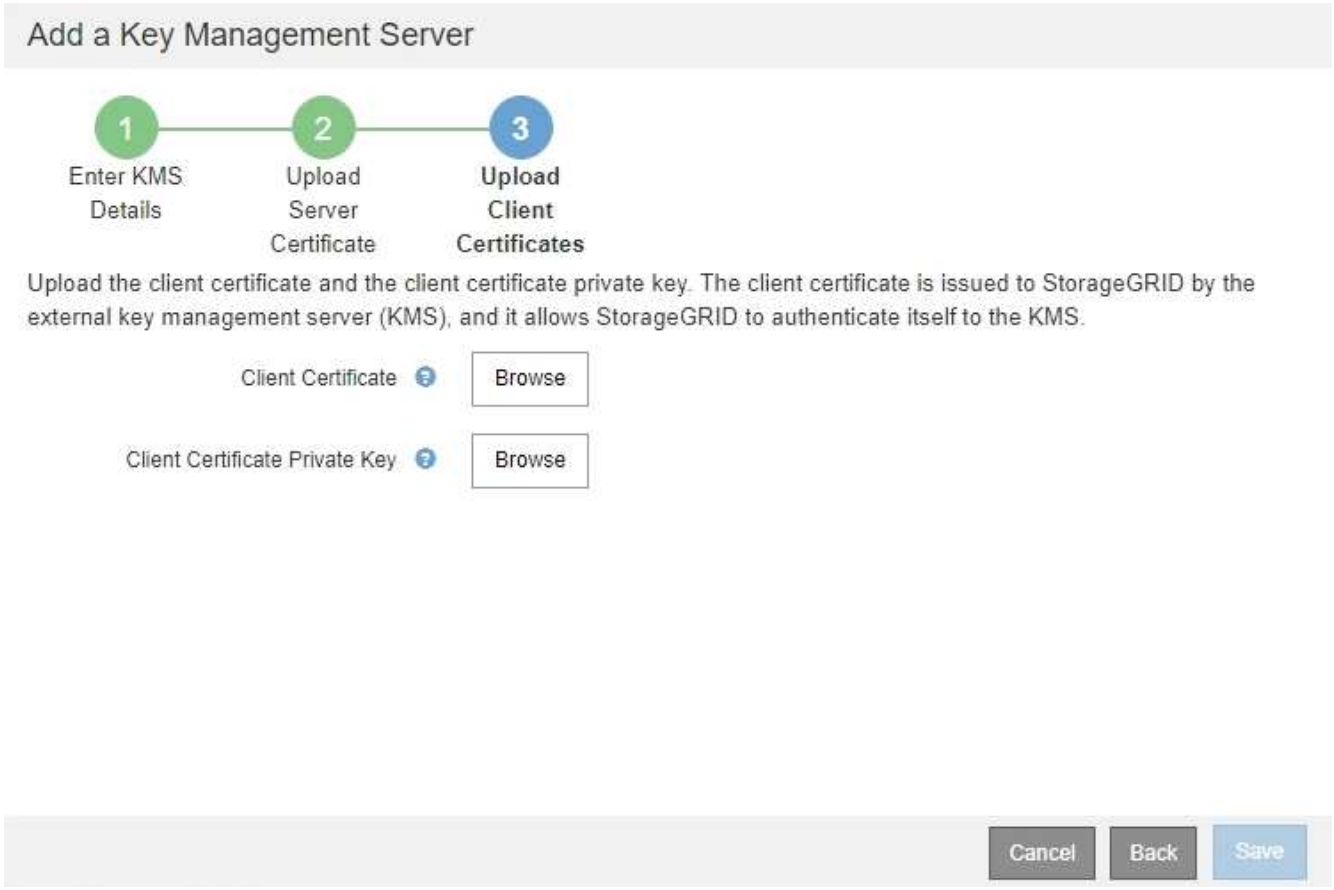
此时将显示添加密钥管理服务器向导的第3步(上传客户端证书)。

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。

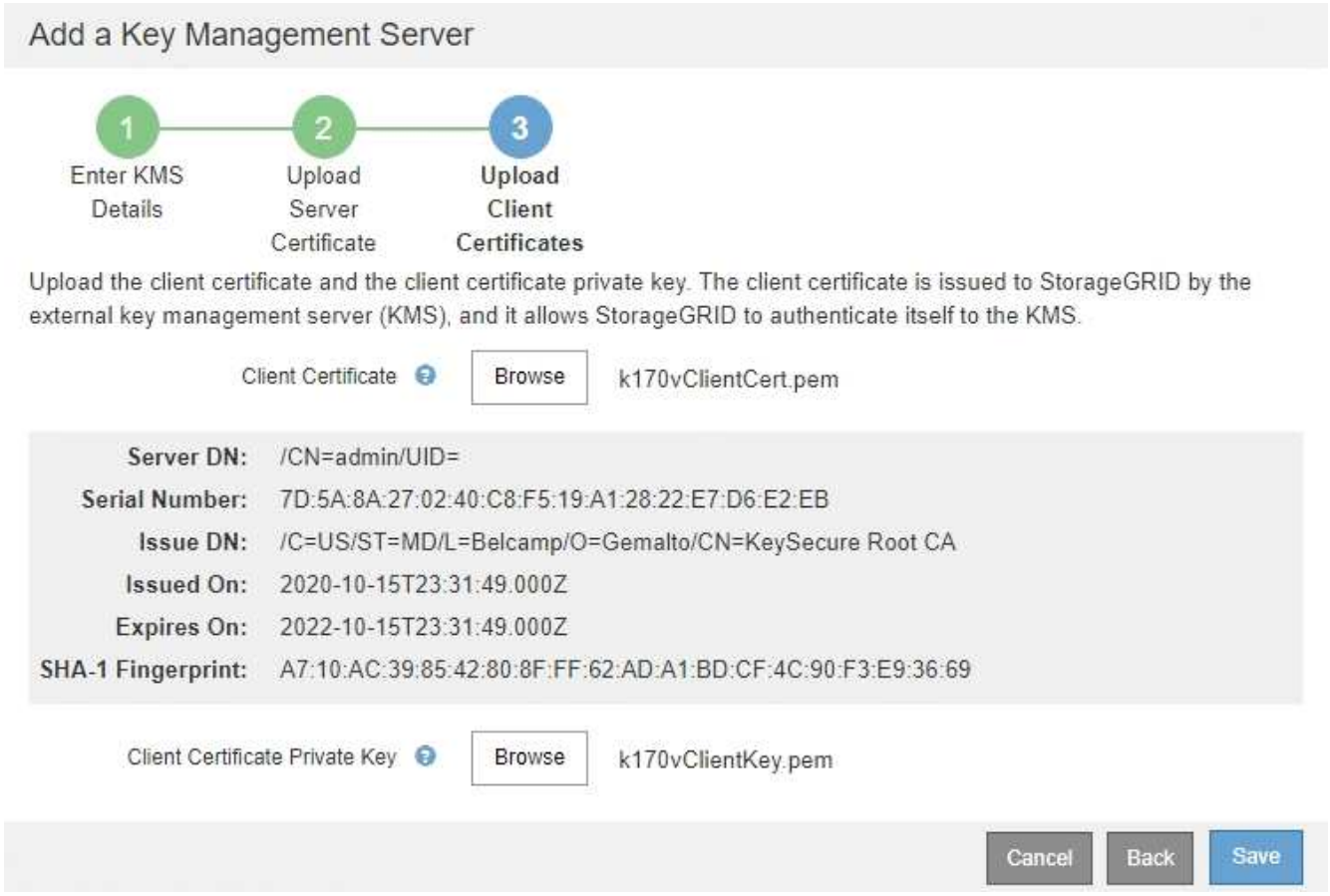


2. 上传客户端证书文件。

   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。



5. 选择 * 保存 * 。

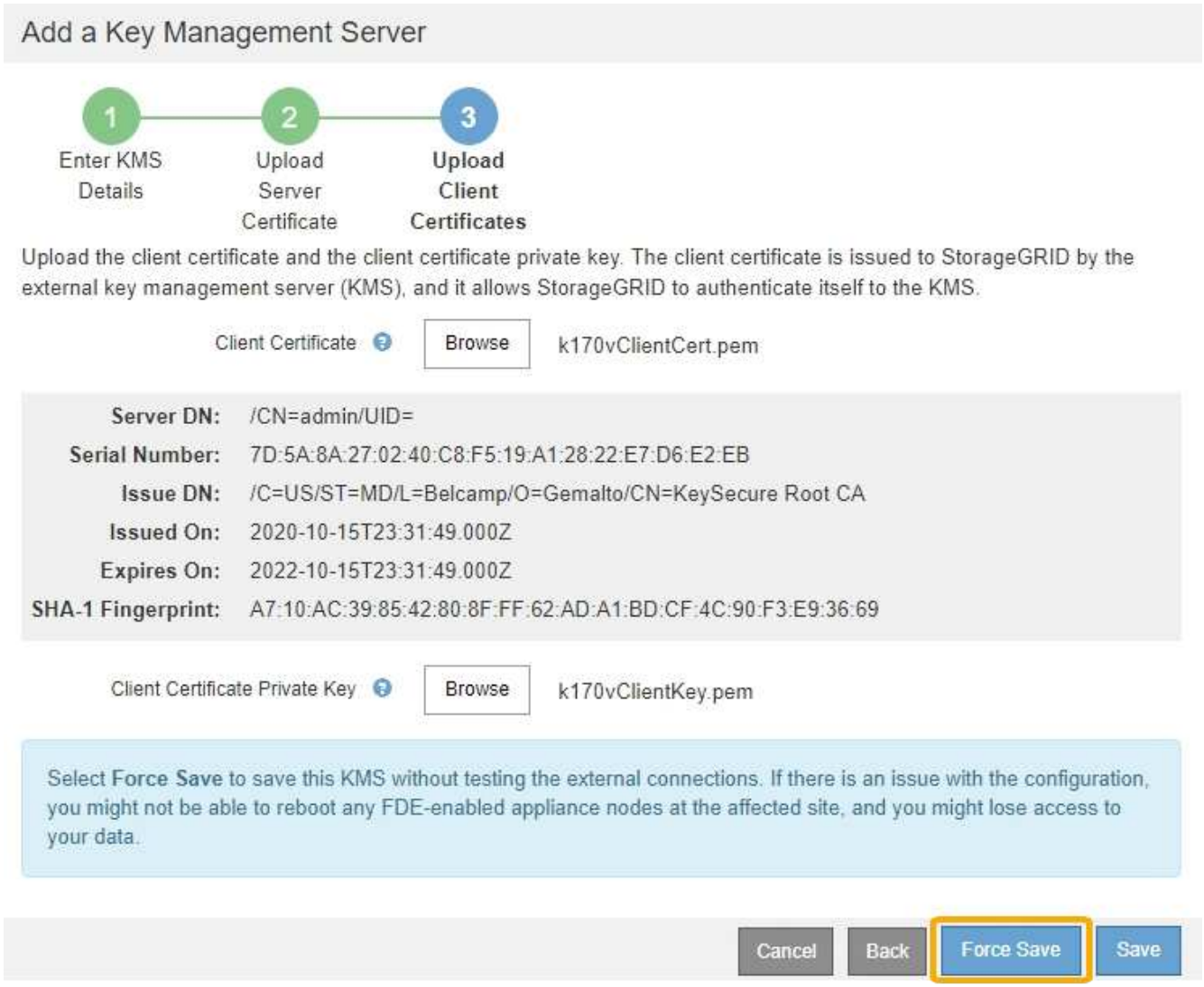
   测试密钥管理服务器与设备节点之间的连接。如果所有连接均有效，并且在 KMS 上找到正确的密钥，则新的密钥管理服务器将添加到密钥管理服务器页面上的表中。

   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 * 。

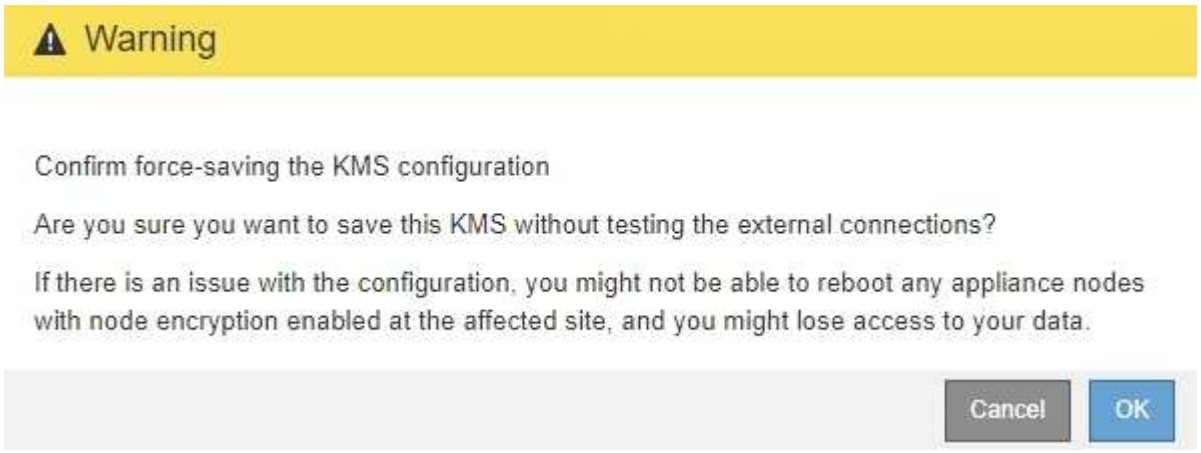
   例如，如果连接测试失败，您可能会收到 422： Unprocessable Entity 错误。

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 * 。



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。

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。