管理安全性

StorageGRID 11.7

NetApp
April 12, 2024

目录

管理安全性 1
管理安全性：概述 1
查看 StorageGRID 加密方法 1
管理证书 3
配置安全设置 31
配置密钥管理服务器 35
管理代理设置 56
控制防火墙 59

管理安全性

管理安全性：概述

您可以从网格管理器配置各种安全设置，以帮助保护 StorageGRID 系统。

管理加密

StorageGRID 提供了多种数据加密选项。您应该 "查看可用的加密方法" 以确定哪些解决方案符合您的数据保护要求。

管理证书

您可以 "配置和管理服务器证书" 用于HTTP连接或用于向服务器验证客户端或用户身份的客户端证书。

配置密钥管理服务器

使用 "密钥管理服务器" 即使从数据中心删除设备、您也可以保护StorageGRID 数据。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。

> 要使用加密密钥管理，必须在安装期间为每个设备启用 * 节点加密 * 设置，然后才能将该设备添加到网格中。

管理代理设置

如果您使用的是S3平台服务或云存储池、则可以配置 "存储代理服务器" 存储节点和外部S3端点之间。如果使用HTTPS或HTTP发送AutoSupport 消息、则可以配置 "管理代理服务器" 在管理节点和技术支持之间。

控制防火墙

为了增强系统的安全性、您可以通过在中打开或关闭特定端口来控制对StorageGRID 管理节点的访问 "外部防火墙"。您还可以通过配置每个节点来控制对其的网络访问 "内部防火墙"。您可以阻止对除部署所需端口以外的所有端口进行访问。

查看 StorageGRID 加密方法

StorageGRID 提供了多种数据加密选项。您应查看可用的方法，以确定哪些方法符合数据保护要求。

下表简要总结了 StorageGRID 中可用的加密方法。

加密选项	工作原理	适用场景
网格管理器中的密钥管理服务器（KMS）	您 "配置密钥管理服务器" 对于StorageGRID 站点、请执行以下操作：和 "为此设备启用节点加密"。然后，设备节点将连接到 KMS 以请求密钥加密密钥（Key Encryption Key， KEK）。此密钥用于对每个卷上的数据加密密钥（DEK）进行加密和解密。	安装期间启用了 * 节点加密 * 的设备节点。设备上的所有数据均可防止物理丢失或从数据中心删除。 只有存储节点和服务设备才支持使用KMS管理加密密钥。
SANtricity System Manager 中的驱动器安全性	如果为SG5700或SG6000存储设备启用了驱动器安全性功能、则可以使用 "SANtricity 系统管理器" 以创建和管理安全密钥。要访问受保护驱动器上的数据，需要使用此密钥。	具有全磁盘加密(Full Disk Encryption、FD)驱动器或FIPS驱动器的存储设备。安全驱动器上的所有数据均可防止物理丢失或从数据中心中删除。不能用于某些存储设备或任何服务设备。
存储对象加密	您可以启用 "存储对象加密" 选项。启用后、在存储分段级别或对象级别未加密的任何新对象都会在数据导入期间进行加密。	新载入的 S3 和 Swift 对象数据。 现有存储对象未加密。对象元数据和其他敏感数据不会加密。
S3 存储分段加密	问题描述 PUT 分段加密请求以对分段启用加密。在对象级别未加密的任何新对象都会在导入期间进行加密。	仅新载入的 S3 对象数据。 必须为存储分段指定加密。现有存储分段对象未加密。对象元数据和其他敏感数据不会加密。 "对存储分段执行的操作"
S3 对象服务器端加密（SS3）	您可以问题描述 S3请求以存储对象并包括 `x-amz-server-side-encryption` 请求标题。	仅新载入的 S3 对象数据。 必须为对象指定加密。对象元数据和其他敏感数据不会加密。 StorageGRID 负责管理密钥。 "使用服务器端加密"

加密选项	工作原理	适用场景
使用客户提供的密钥（SSI-C）进行 S3 对象服务器端加密	您可以问题描述 S3 请求以存储一个对象并包含三个请求标头。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	仅新载入的 S3 对象数据。 必须为对象指定加密。对象元数据和其他敏感数据不会加密。 密钥在 StorageGRID 之外进行管理。 "使用服务器端加密"
外部卷或数据存储库加密	如果您的部署平台支持，则可以在 StorageGRID 外部使用加密方法对整个卷或数据存储库进行加密。	所有对象数据，元数据和系统配置数据，假设每个卷或数据存储库都已加密。 外部加密方法可以更严格地控制加密算法和密钥。可以与列出的其他方法结合使用。
StorageGRID 外部的对象加密	在将对象数据和元数据载入 StorageGRID 之前，您可以在 StorageGRID 外部使用加密方法对这些数据和元数据进行加密。	仅限对象数据和元数据（系统配置数据不加密）。 外部加密方法可以更严格地控制加密算法和密钥。可以与列出的其他方法结合使用。 "Amazon Simple Storage Service—开发人员指南：使用客户端加密保护数据"

使用多种加密方法

根据您的要求，您一次可以使用多种加密方法。例如：

- 您可以使用 KMS 来保护设备节点，也可以使用 SANtricity 系统管理器中的驱动器安全功能在同一设备中的自加密驱动器上 " d 进行灵活加密 " 数据。
- 您可以使用KMS保护设备节点上的数据、也可以使用存储对象加密选项对所有对象进行加密。

如果只有一小部分对象需要加密，请考虑在存储分段或单个对象级别控制加密。启用多个级别的加密会产生额外的性能成本。

管理证书

管理安全证书：概述

安全证书是一个小型数据文件，用于在 StorageGRID 组件之间以及 StorageGRID 组件与外部系统之间创建安全可信的连接。

StorageGRID 使用两种类型的安全证书：

- 使用 HTTPS 连接时需要 * 服务器证书 * 。服务器证书用于在客户端和服务器之间建立安全连接，向客户端验证服务器的身份并为数据提供安全通信路径。服务器和客户端都有一个证书副本。
- * 客户端证书 * 可对服务器的客户端或用户身份进行身份验证，从而提供比单独使用密码更安全的身份验证。客户端证书不会对数据进行加密。

当客户端使用 HTTPS 连接到服务器时，服务器会使用包含公有 密钥的服务器证书进行响应。客户端通过将服务器签名与其证书副本上的签名进行比较来验证此证书。如果签名匹配，则客户端将使用相同的公有 密钥启动与服务器的会话。

StorageGRID 用作某些连接的服务器（例如负载平衡器端点）或其他连接的客户端（例如 CloudMirror 复制服务）。

- 默认网格 CA 证书 *

StorageGRID 包含一个内置证书颁发机构（ Certificate Authority ， CA ），可在系统安装期间生成内部网格 CA 证书。默认情况下，使用网格 CA 证书保护内部 StorageGRID 流量。外部证书颁发机构（ CA ）可以对完全符合组织信息安全策略的自定义证书进行问题描述 。虽然您可以在非生产环境中使用网格 CA 证书，但在生产环境中，最佳做法是使用由外部证书颁发机构签名的自定义证书。也支持不带证书的不安全连接、但不建议这样做。

- 自定义CA证书不会删除内部证书；但是、自定义证书应是为验证服务器连接而指定的证书。
- 所有自定义证书都必须满足 "服务器证书的系统强化准则"。
- StorageGRID 支持将 CA 中的证书捆绑到一个文件中（称为 CA 证书包）。

> StorageGRID 还包括在所有网格上相同的操作系统 CA 证书。在生产环境中，请确保指定一个由外部证书颁发机构签名的自定义证书，以替代操作系统 CA 证书。

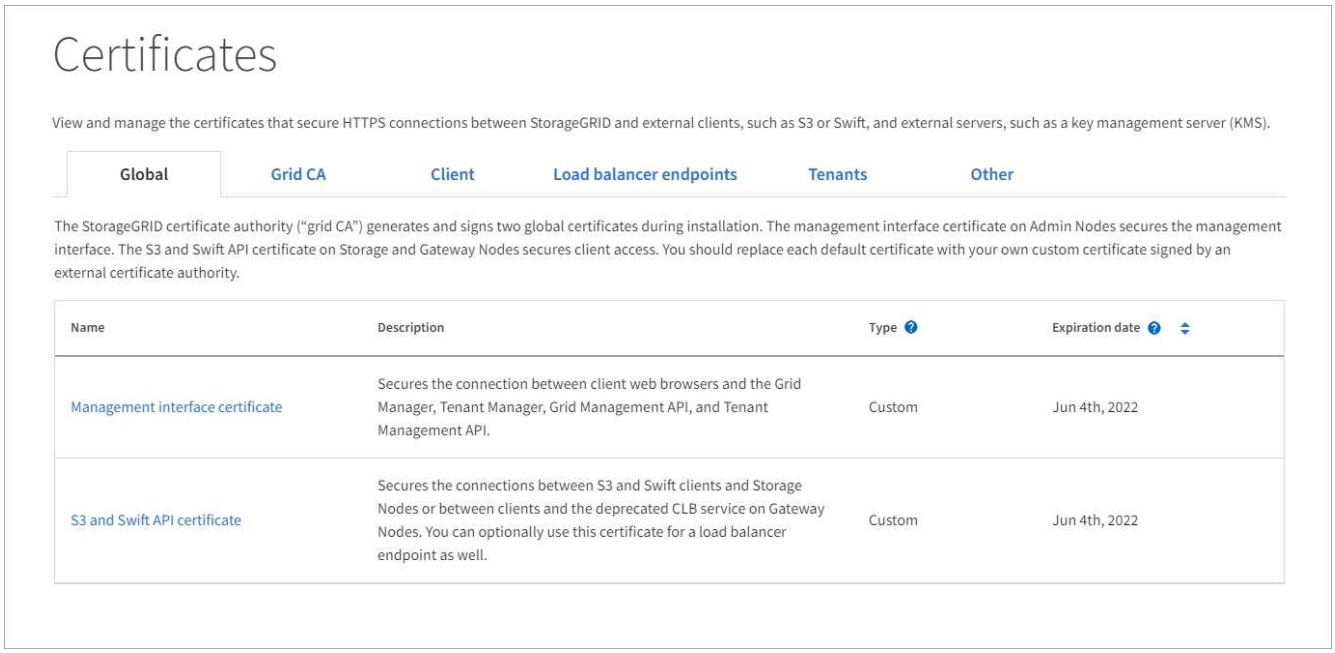
服务器和客户端证书类型的变体通过多种方式实现。在配置系统之前，您应准备好特定 StorageGRID 配置所需的所有证书。

访问安全证书

您可以在一个位置访问有关所有 StorageGRID 证书的信息，以及指向每个证书的配置工作流的链接。

步骤

1. 在网格管理器中，选择*configuration*>*Security*>*Certificates*。



2. 在证书页面上选择一个选项卡，以获取有关每个证书类别的信息并访问证书设置。只有在拥有相应权限的情况下，才能访问选项卡。

   - * 全局 *： 确保从 Web 浏览器和外部 API 客户端访问 StorageGRID 的安全。
   - * 网格 CA*： 保护内部 StorageGRID 流量的安全。
   - * 客户端 *： 保护外部客户端与 StorageGRID Prometheus 数据库之间的连接。
   - * 负载平衡器端点 *： 确保 S3 和 Swift 客户端与 StorageGRID 负载平衡器之间的连接安全。
   - * 租户 *： 保护与身份联合服务器或从平台服务端点到 S3 存储资源的连接。
   - * 其他 *： 保护需要特定证书的 StorageGRID 连接。

   下面介绍了每个选项卡，并提供了指向其他证书详细信息的链接。

全局

这些全局证书可确保从 Web 浏览器以及外部 S3 和 Swift API 客户端访问 StorageGRID 的安全。在安装期间， StorageGRID 证书颁发机构最初会生成两个全局证书。生产环境的最佳实践是使用由外部证书颁发机构签名的自定义证书。

- [管理接口证书]：确保客户端 Web 浏览器与 StorageGRID 管理界面的连接安全。
- S3 和 Swift API 证书：保护与存储节点，管理节点和网关节点的客户端 API 连接的安全， S3 和 Swift 客户端应用程序使用这些连接上传和下载对象数据。

有关已安装的全局证书的信息包括：

- * 名称 * ： 证书名称，其中包含用于管理证书的链接。
- * 问题描述 *
- * 类型 * ： 自定义或默认。+ 为了提高网格安全性，您应始终使用自定义证书。
- * 到期日期 * ： 如果使用默认证书，则不会显示到期日期。

您可以

- 将默认证书替换为由外部证书颁发机构签名的自定义证书，以提高网格安全性：
  - "替换由 StorageGRID 生成的默认管理接口证书" 用于网格管理器和租户管理器连接。
  - "替换 S3 和 Swift API 证书" 用于存储节点和负载平衡器端点(可选)连接。
- "还原默认管理接口证书。"
- "还原默认 S3 和 Swift API 证书。"
- "使用脚本生成新的自签名管理接口证书。"
- 复制或下载 "管理接口证书" 或 "S3 和 Swift API 证书"。

网格 **CA**

。 网格 CA 证书由 StorageGRID 证书颁发机构在 StorageGRID 安装期间生成，可保护所有内部 StorageGRID 流量。

证书信息包括证书到期日期和证书内容。

您可以 "复制或下载网格CA证书"，但您无法更改它。

客户端

客户端证书由外部证书颁发机构生成，用于保护外部监控工具与 StorageGRID Prometheus 数据库之间的连接。

证书表中的每个已配置客户端证书都有一行，用于指示此证书是否可用于 Prometheus 数据库访问以及证书到期日期。

您可以

- "上传或生成新的客户端证书。"
- 选择一个证书名称以显示证书详细信息，您可以在其中执行以下操作：

- "更改客户端证书名称。"
- "设置 Prometheus 访问权限。"
- "上传并替换客户端证书。"
- "复制或下载客户端证书。"
- "删除客户端证书。"

- 选择 * 操作 * 以快速执行 "编辑"， "附加"或 "删除" 客户端证书。您最多可以选择 10 个客户端证书，并使用 * 操作 * > * 删除 * 一次删除这些证书。

负载平衡器端点

负载平衡器端点证书 保护S3和Swift客户端之间的连接以及网关节点和管理节点上的StorageGRID 负载平衡器服务。

负载平衡器端点表对每个已配置的负载平衡器端点都有一行，用于指示此端点是否使用全局 S3 和 Swift API 证书或自定义负载平衡器端点证书。此外，还会显示每个证书的到期日期。

> 对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

您可以

- "查看负载平衡器端点"，包括其证书详细信息。
- "为 FabricPool 指定负载平衡器端点证书。"
- "使用全局 S3 和 Swift API 证书" 而不是生成新的负载平衡器端点证书。

Tenants

租户可以使用 身份联合服务器证书 或 平台服务端点证书 以确保其与 StorageGRID 的连接安全。

租户表中的每个租户都有一行，用于指示每个租户是否有权使用自己的身份源或平台服务。

您可以

- "选择一个租户名称以登录到租户管理器"
- "选择租户名称以查看租户身份联合详细信息"
- "选择租户名称以查看租户平台服务详细信息"
- "在创建端点期间指定平台服务端点证书"

其他

StorageGRID 会将其他安全证书用于特定目的。这些证书按其功能名称列出。其他安全证书包括：

- 云存储池证书
- 通过电子邮件发送警报通知证书
- 外部系统日志服务器证书
- 网格联合连接证书
- 身份联合证书

- 密钥管理服务器（KMS）证书
- 单点登录证书

信息指示函数使用的证书类型及其服务器和客户端证书的到期日期（如果适用）。选择功能名称将打开一个浏览器选项卡，您可以在此查看和编辑证书详细信息。

> 只有在拥有相应权限的情况下，才能查看和访问其他证书的信息。

您可以

- "为 S3， C2S S3 或 Azure 指定云存储池证书"
- "指定警报电子邮件通知的证书"
- "指定外部系统日志服务器证书"
- "旋转网格联合连接证书"
- "查看和编辑身份联合证书"
- "上传密钥管理服务器（KMS）服务器和客户端证书"
- "手动为依赖方信任指定SSO证书"

安全证书详细信息

下面介绍了每种类型的安全证书、并提供了指向实施说明的链接。

管理接口证书

证书类型	**Description**	导航位置	详细信息
服务器	对客户端 Web 浏览器和 StorageGRID 管理界面之间的连接进行身份验证，使用户能够访问网格管理器和租户管理器，而不会出现安全警告。 此证书还会对网格管理 API 和租户管理 API 连接进行身份验证。 您可以使用安装期间创建的默认证书，也可以上传自定义证书。	• 配置 * > * 安全性 * > * 证书 *，选择 * 全局 * 选项卡，然后选择 * 管理接口证书 *	"配置管理接口证书"

S3 和 Swift API 证书

证书类型	Description	导航位置	详细信息
服务器	对存储节点和负载平衡器端点的安全S3或Swift客户端连接进行身份验证(可选)。	• 配置 * > * 安全性 * > * 证书 *，选择 * 全局 * 选项卡，然后选择 * S3 和 Swift API 证书 *	"配置 S3 和 Swift API 证书"

网格 **CA** 证书

请参见 默认网格 CA 证书问题描述。

管理员客户端证书

证书类型	Description	导航位置	详细信息
客户端	安装在每个客户端上，使 StorageGRID 能够对外部客户端访问进行身份验证。 • 允许授权的外部客户端访问 StorageGRID Prometheus 数据库。 • 允许使用外部工具安全监控 StorageGRID。	• 配置 * > * 安全性 * > * 证书 *，然后选择 * 客户端 * 选项卡	"配置客户端证书"

负载平衡器端点证书

证书类型	Description	导航位置	详细信息
服务器	对 S3 或 Swift 客户端与网关节点和管理节点上的 StorageGRID 负载平衡器服务之间的连接进行身份验证。您可以在配置负载平衡器端点时上传或生成负载平衡器证书。客户端应用程序在连接到 StorageGRID 时使用负载平衡器证书来保存和检索对象数据。 您也可以使用自定义版本的全局 S3 和 Swift API 证书 用于对与负载平衡器服务的连接进行身份验证的证书。如果使用全局证书对负载平衡器连接进行身份验证、则无需为每个负载平衡器端点上载或生成单独的证书。 • 注意： * 用于负载平衡器身份验证的证书是正常 StorageGRID 操作期间使用量最多的证书。	• 配置 * > * 网络 * > * 负载平衡器端点 *	• "配置负载平衡器端点" • "为 FabricPool 创建负载平衡器端点"

云存储池端点证书

证书类型	Description	导航位置	详细信息
服务器	对从 StorageGRID 云存储池到外部存储位置（例如 S3 Glacier 或 Microsoft Azure Blob 存储）的连接进行身份验证。每种云提供商类型都需要一个不同的证书。	• ILM * > * 存储池 *	"创建云存储池"

通过电子邮件发送警报通知证书

证书类型	Description	导航位置	详细信息
服务器和客户端	对 SMTP 电子邮件服务器与用于警报通知的 StorageGRID 之间的连接进行身份验证。 • 如果与 SMTP 服务器的通信需要传输层安全（Transport Layer Security， TLS），则必须指定电子邮件服务器 CA 证书。 • 仅当 SMTP 电子邮件服务器需要客户端证书进行身份验证时，才指定客户端证书。	• 警报 * > * 电子邮件设置 *	"为警报设置电子邮件通知"

外部系统日志服务器证书

证书类型	Description	导航位置	详细信息
服务器	对在 StorageGRID 中记录事件的外部系统日志服务器之间的 TLS 或 RELP/TLS 连接进行身份验证。 • 注： * 与外部系统日志服务器的 TCP，RELP/TCP 和 UDP 连接不需要外部系统日志服务器证书。	• 配置 * > * 监控 * > * 审核和系统日志服务器 *，然后选择 * 配置外部系统日志服务器 *	"配置外部系统日志服务器"

网格联合连接证书

证书类型	Description	导航位置	详细信息
服务器和客户端	对当前StorageGRID 系统与网格联合连接中的另一个网格之间发送的信息进行身份验证和加密。	配置>*系统*>*网格联合*	• "创建网格联合连接" • "轮换连接证书"

身份联合证书

证书类型	Description	导航位置	详细信息
服务器	对 StorageGRID 与外部身份提供程序（例如 Active Directory ， OpenLDAP 或 Oracle 目录服务器）之间的连接进行身份验证。用于身份联合，允许管理组和用户由外部系统管理。	• 配置 * > * 访问控制 * > * 身份联合 *	"使用身份联合"

密钥管理服务器（ **KMS** ）证书

证书类型	Description	导航位置	详细信息
服务器和客户端	对 StorageGRID 与外部密钥管理服务器（ KMS ）之间的连接进行身份验证，该服务器可为 StorageGRID 设备节点提供加密密钥。	• 配置 * > * 安全性 * > * 密钥管理服务器 *	"添加密钥管理服务器（ KMS ）"

平台服务端点证书

证书类型	Description	导航位置	详细信息
服务器	对从 StorageGRID 平台服务到 S3 存储资源的连接进行身份验证。	• 租户管理器 * > * 存储（ S3 ） * > * 平台服务端点 *	"创建平台服务端点" "编辑平台服务端点"

单点登录（ **SSO** ）证书

证书类型	Description	导航位置	详细信息
服务器	对身份联合服务（例如 Active Directory 联合身份验证服务（ AD FS ））与用于单点登录（ SSO ）请求的 StorageGRID 之间的连接进行身份验证。	• 配置 * > * 访问控制 * > * 单点登录 *	"配置单点登录"

证书示例

示例 **1** ： 负载平衡器服务

在此示例中， StorageGRID 充当服务器。

1. 您可以在 StorageGRID 中配置负载平衡器端点并上传或生成服务器证书。
2. 您可以配置与负载平衡器端点的 S3 或 Swift 客户端连接，并将同一证书上传到客户端。

3. 当客户端要保存或检索数据时，它会使用 HTTPS 连接到负载平衡器端点。
4. StorageGRID 会使用包含公有 密钥的服务器证书进行响应，并使用基于私钥的签名进行响应。
5. 客户端通过将服务器签名与其证书副本上的签名进行比较来验证此证书。如果签名匹配，客户端将使用相同的公有 密钥启动会话。
6. 客户端将对象数据发送到 StorageGRID 。

示例 **2**： 外部密钥管理服务器（ **KMS** ）

在此示例中， StorageGRID 充当客户端。

1. 您可以使用外部密钥管理服务器软件将 StorageGRID 配置为 KMS 客户端，并获取 CA 签名的服务器证书，公有 客户端证书以及客户端证书的专用密钥。
2. 使用网格管理器，您可以配置 KMS 服务器并上传服务器和客户端证书以及客户端专用密钥。
3. 当 StorageGRID 节点需要加密密钥时，它会向 KMS 服务器发出请求，请求包含证书中的数据以及基于私钥的签名。
4. KMS 服务器会验证证书签名，并决定它可以信任 StorageGRID 。
5. KMS 服务器使用经过验证的连接进行响应。

配置服务器证书

支持的服务器证书类型

StorageGRID 系统支持使用 RSA 或 ECDSA （椭圆曲线数字签名算法）加密的自定义证书。

> 安全策略的密码类型必须与服务器证书类型匹配。例如、RSA密钥需要RSA证书、而ECDSA密钥需要ECDSA证书。请参见 "管理安全证书"。如果您配置的自定义安全策略与服务器证书不兼容、则可以执行此操作 "暂时还原为默认安全策略"。

有关StorageGRID 如何保护REST API的客户端连接的详细信息、请参阅 "为S3 REST API配置安全性" 或 "配置Swift REST API的安全性"。

配置管理接口证书

您可以将默认管理接口证书替换为一个自定义证书，使用户可以访问 Grid Manager 和租户管理器，而不会遇到安全警告。您还可以还原到默认管理接口证书或生成新的管理接口证书。

关于此任务

默认情况下，每个管理节点都会获得一个由网格 CA 签名的证书。这些 CA 签名的证书可以替换为一个通用的自定义管理接口证书和相应的专用密钥。

由于所有管理节点都使用一个自定义管理接口证书，因此，如果客户端在连接到网格管理器和租户管理器时需要验证主机名，则必须将此证书指定为通配符或多域证书。定义自定义证书，使其与网格中的所有管理节点匹配。

您需要在服务器上完成配置，根据所使用的根证书颁发机构（ CA ），用户可能还需要在用于访问网格管理器和租户管理器的 Web 浏览器中安装网格 CA 证书。

为确保操作不会因服务器证书失败而中断，当此服务器证书即将到期时，将触发*管理接口的服务器证书到期*警报。根据需要，您可以通过选择 * 配置 * > * 安全性 * > * 证书 * 并在全局选项卡上查看管理接口证书的到期日期来查看当前证书的到期时间。

如果您要使用域名而非 IP 地址访问网格管理器或租户管理器，则在发生以下任一情况时，浏览器将显示证书错误，并且无法绕过此错误：

- 您的自定义管理接口证书将过期。
- 您 从自定义管理接口证书还原到默认服务器证书。

添加自定义管理接口证书

要添加自定义管理接口证书，您可以提供自己的证书或使用网格管理器生成一个证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 使用自定义证书 * 。
4. 上传或生成证书。

上传证书

上传所需的服务器证书文件。

a. 选择 * 上传证书 * 。
b. 上传所需的服务器证书文件：
   - * 服务器证书 * ： 自定义服务器证书文件（ PEM 编码）。
   - 证书专用密钥:自定义服务器证书专用密钥文件 (`.key`）。

     EC 专用密钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

   - * CA bundle* ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。
c. 展开 * 证书详细信息 * 以查看您上传的每个证书的元数据。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。
   - 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。
d. 选择 * 保存 * 。+ 自定义管理接口证书用于此后与网格管理器，租户管理器，网格管理器 API 或租户管理器 API 的所有新连接。

生成证书

生成服务器证书文件。

生产环境的最佳实践是使用由外部证书颁发机构签名的自定义管理接口证书。

a. 选择 * 生成证书 * 。
b. 指定证书信息：

字段	**Description**
域名	要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
IP	要包含在证书中的一个或多个IP地址。
主题(可选)	证书所有者的X.509主题或可分辨名称(DN)。 如果未在此字段中输入值、则生成的证书将使用第一个域名或IP地址作为使用者公用名(CN)。

字段	Description
有效天数	创建后证书过期的天数。
添加密钥用法扩展	如果选中(默认值和建议值)、则会将密钥用法和扩展密钥用法扩展添加到生成的证书中。 这些扩展定义了证书中所含密钥的用途。 注意：除非证书包含这些扩展时遇到与旧客户端的连接问题，否则请保持选中此复选框。

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可查看生成的证书的元数据。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 保存 * 。+ 自定义管理接口证书用于此后与网格管理器，租户管理器，网格管理器 API 或租户管理器 API 的所有新连接。

5. 刷新页面以确保 Web 浏览器已更新。

   上传或生成新证书后，请留出最多一天的时间来清除任何相关证书到期警报。

6. 添加自定义管理接口证书后， " 管理接口证书 " 页面将显示正在使用的证书的详细证书信息。+ 您可以根据需要下载或复制证书 PEM 。

还原默认管理接口证书

您可以使用网格管理器和租户管理器连接的默认管理接口证书还原到。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 使用默认证书 * 。

   还原默认管理接口证书时、您配置的自定义服务器证书文件将被删除、并且无法从系统中恢复。默认管理接口证书将用于所有后续的新客户端连接。

4. 刷新页面以确保 Web 浏览器已更新。

使用脚本生成新的自签名管理接口证书

如果需要严格验证主机名，可以使用脚本生成管理接口证书。

开始之前

- 您具有特定的访问权限。
- 您拥有 `Passwords.txt` 文件

关于此任务

生产环境的最佳实践是使用由外部证书颁发机构签名的证书。

步骤

1. 获取每个管理节点的完全限定域名（FQDN）。
2. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件

   以root用户身份登录后、提示符将从变为 `$` to `#`。
3. 使用新的自签名证书配置 StorageGRID 。

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - 适用于 `--domains`下、使用通配符表示所有管理节点的完全限定域名。例如：`*.ui.storagegrid.example.com` 使用*通配符表示 `admin1.ui.storagegrid.example.com` 和 `admin2.ui.storagegrid.example.com`。
   - 设置 `--type` to `management` 配置网格管理器和租户管理器使用的管理接口证书。
   - 默认情况下，生成的证书有效期为一年（365 天），必须在证书过期之前重新创建。您可以使用 `--days` 用于覆盖默认有效期的参数。

   > 证书的有效期从何时开始 `make-certificate` 已运行。您必须确保管理客户端与 StorageGRID 同步到同一个时间源；否则，客户端可能会拒绝此证书。

   ```
   $ sudo make-certificate --domains *.ui.storagegrid.example.com --type
   management --days 720
   ```

   生成的输出包含管理 API 客户端所需的公有 证书。
4. 选择并复制证书。

   在您的选择中包括开始和结束标记。
5. 从命令 Shell 中注销。 `$ exit`

6. 确认已配置证书：
    a. 访问网格管理器。
    b. 选择 * 配置 * > * 安全性 * > * 证书 *
    c. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
7. 将管理客户端配置为使用您复制的公有 证书。包括开始和结束标记。

下载或复制管理接口证书

您可以保存或复制管理接口证书内容，以便在其他位置使用。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 服务器 * 或 * CA 捆绑包 * 选项卡，然后下载或复制证书。

下载证书文件或 **CA** 包

下载证书或CA包 `.pem` 文件如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 下载证书 * 或 * 下载 CA 捆绑包 * 。

   如果要下载 CA 包，则 CA 包二级选项卡中的所有证书将作为一个文件下载。

b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

复制证书文本以粘贴到其他位置。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* 。

   如果要复制 CA 包，则 CA 包二级选项卡中的所有证书会同时复制在一起。

b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

配置 **S3** 和 **Swift API** 证书

您可以替换或还原用于将S3或Swift客户端连接到存储节点或负载平衡器端点的服务器证书。替换的自定义服务器证书特定于您的组织。

关于此任务

默认情况下，每个存储节点都会获得一个由网格 CA 签名的 X.509 服务器证书。这些 CA 签名的证书可以替换为一个通用的自定义服务器证书和相应的专用密钥。

所有存储节点都使用一个自定义服务器证书，因此，如果客户端在连接到存储端点时需要验证主机名，则必须将此证书指定为通配符或多域证书。定义自定义证书，使其与网格中的所有存储节点匹配。

在服务器上完成配置后，您可能还需要在用于访问系统的 S3 或 Swift API 客户端中安装网格 CA 证书，具体取决于您正在使用的根证书颁发机构（ CA ）。

> 为确保操作不会因服务器证书失败而中断，根服务器证书即将到期时会触发*S3和Swift API*全局服务器证书到期*警报。根据需要，您可以通过选择 * 配置 * > * 安全性 * > * 证书 * 并在全局选项卡上查看 S3 和 Swift API 证书的到期日期来查看当前证书的到期时间。

您可以上传或生成自定义 S3 和 Swift API 证书。

添加自定义 **S3** 和 **Swift API** 证书

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。
3. 选择 * 使用自定义证书 * 。
4. 上传或生成证书。

上传证书

上传所需的服务器证书文件。

a. 选择 * 上传证书 * 。
b. 上传所需的服务器证书文件：
   - * 服务器证书 * ： 自定义服务器证书文件（ PEM 编码）。
   - 证书专用密钥:自定义服务器证书专用密钥文件 (`.key`）。

     EC 专用密钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

   - * CA bundle* ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。
c. 选择证书详细信息以显示上传的每个自定义 S3 和 Swift API 证书的元数据和 PEM 。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。
   - 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。
d. 选择 * 保存 * 。

   自定义服务器证书用于后续的新 S3 和 Swift 客户端连接。

生成证书

生成服务器证书文件。

a. 选择 * 生成证书 * 。
b. 指定证书信息：

字段	**Description**
域名	要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
IP	要包含在证书中的一个或多个IP地址。
主题(可选)	证书所有者的X.509主题或可分辨名称(DN)。 如果未在此字段中输入值、则生成的证书将使用第一个域名或IP地址作为使用者公用名(CN)。
有效天数	创建后证书过期的天数。

字段	Description
添加密钥用法扩展	如果选中(默认值和建议值)、则会将密钥用法和扩展密钥用法扩展添加到生成的证书中。 这些扩展定义了证书中所含密钥的用途。 注意：除非证书包含这些扩展时遇到与旧客户端的连接问题，否则请保持选中此复选框。

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可显示生成的自定义 S3 和 Swift API 证书的元数据和 PEM 。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 保存 * 。

   自定义服务器证书用于后续的新 S3 和 Swift 客户端连接。

5. 选择一个选项卡以显示默认 StorageGRID 服务器证书，已上传的 CA 签名证书或已生成的自定义证书的元数据。

   上传或生成新证书后，请留出最多一天的时间来清除任何相关证书到期警报。

6. 刷新页面以确保 Web 浏览器已更新。

7. 添加自定义 S3 和 Swift API 证书后， S3 和 Swift API 证书页面将显示正在使用的自定义 S3 和 Swift API 证书的详细证书信息。+ 您可以根据需要下载或复制证书 PEM 。

还原默认 S3 和 Swift API 证书

您可以还原为使用默认的S3和Swift API证书进行S3和Swift客户端与存储节点的连接。但是、不能对负载平衡器端点使用默认的S3和Swift API证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。

2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。

3. 选择 * 使用默认证书 * 。

   还原全局S3和Swift API证书的默认版本时、您配置的自定义服务器证书文件将被删除、并且无法从系统中恢复。默认的S3和Swift API证书将用于后续与存储节点的新S3和Swift客户端连接。

4. 选择 * 确定 * 确认警告并还原默认 S3 和 Swift API 证书。

如果您拥有根访问权限，并且自定义 S3 和 Swift API 证书用于负载平衡器端点连接，则会显示一个负载平衡器端点列表，这些端点将无法再使用默认 S3 和 Swift API 证书进行访问。转至 "配置负载平衡器端点" 编辑或删除受影响的端点。

5. 刷新页面以确保 Web 浏览器已更新。

下载或复制 **S3** 和 **Swift API** 证书

您可以保存或复制 S3 和 Swift API 证书内容，以便在其他位置使用。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。
3. 选择 * 服务器 * 或 * CA 捆绑包 * 选项卡，然后下载或复制证书。

下载证书文件或 **CA** 包

下载证书或CA包 `.pem` 文件如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 下载证书 * 或 * 下载 CA 捆绑包 * 。

   如果要下载 CA 包，则 CA 包二级选项卡中的所有证书将作为一个文件下载。

b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

复制证书文本以粘贴到其他位置。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* 。

   如果要复制 CA 包，则 CA 包二级选项卡中的所有证书会同时复制在一起。

b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

相关信息

- "使用S3 REST API"
- "使用Swift REST API"
- "配置S3端点域名"

复制网格 **CA** 证书

StorageGRID 使用内部证书颁发机构（CA）来保护内部流量。如果您上传自己的证书，则此证书不会更改。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

关于此任务

如果配置了自定义服务器证书，则客户端应用程序应使用自定义服务器证书验证服务器。他们不应从 StorageGRID 系统复制 CA 证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 网格 CA* 选项卡。
2. 在*Certificate PEM*部分，下载或复制证书。

下载证书文件

下载证书 `.pem` 文件

a. 选择 * 下载证书 * 。
b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

复制证书 **PEM**

复制证书文本以粘贴到其他位置。

a. 选择 * 复制证书 PEM* 。
b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

为 **FabricPool** 配置 **StorageGRID** 证书

对于执行严格主机名验证但不支持禁用严格主机名验证的S3客户端(例如使用FabricPool的ONTAP 客户端)、您可以在配置负载平衡器端点时生成或上传服务器证书。

开始之前

- 您具有特定的访问权限。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。

关于此任务

创建负载平衡器端点时，您可以生成自签名服务器证书或上传由已知证书颁发机构（ CA ）签名的证书。在生产环境中，您应使用由已知 CA 签名的证书。由 CA 签名的证书可以无中断地轮换。它们也更安全，因为它们可以更好地防止中间人攻击。

以下步骤为使用 FabricPool 的 S3 客户端提供了一般准则。有关更多详细信息和过程，请参见 "为 FabricPool 配置 StorageGRID"。

步骤

1. （可选）配置一个高可用性（ High Availability ， HA ）组以供 FabricPool 使用。
2. 创建 S3 负载平衡器端点以供 FabricPool 使用。

   创建 HTTPS 负载平衡器端点时，系统会提示您上传服务器证书，证书专用密钥和可选的 CA 捆绑包。

3. 在 ONTAP 中将 StorageGRID 附加为云层。

   指定负载平衡器端点端口以及上载的 CA 证书中使用的完全限定域名。然后，提供 CA 证书。

   > 如果中间 CA 颁发了 StorageGRID 证书，则必须提供中间 CA 证书。如果 StorageGRID 证书是直接由根 CA 颁发的，则必须提供根 CA 证书。

配置客户端证书

客户端证书允许授权的外部客户端访问 StorageGRID Prometheus 数据库，从而为外部工具监控 StorageGRID 提供了一种安全的方式。

如果您需要使用外部监控工具访问StorageGRID 、则必须使用网格管理器上传或生成客户端证书、并将证书信息复制到外部工具。

请参见 "管理安全证书" 和 "配置自定义服务器证书"。

> 为确保操作不会因服务器证书失败而中断，当此服务器证书即将到期时，将触发“证书页上配置的客户端证书*到期”警报。根据需要，您可以通过选择 * 配置 * > * 安全性 * > * 证书 * 并在客户端选项卡上查看客户端证书的到期日期来查看当前证书的到期时间。

> 如果您使用密钥管理服务器（ KMS ）保护专门配置的设备节点上的数据，请参见有关的特定信息 "上传 KMS 客户端证书"。

开始之前

- 您具有 root 访问权限。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 配置客户端证书：
  - 您拥有管理节点的 IP 地址或域名。
  - 如果已配置StorageGRID 管理接口证书、则可以使用CA、客户端证书和专用密钥来配置管理接口证书。
  - 要上传您自己的证书、您的本地计算机上提供了证书的专用密钥。

    - 私钥必须在创建时已保存或记录。如果您没有原始私钥、则必须创建一个新的私钥。
- 编辑客户端证书：
    - 您拥有管理节点的 IP 地址或域名。
    - 要上传您自己的证书或新证书、您的本地计算机上提供了私钥、客户端证书和CA (如果使用)。

添加客户端证书

要添加客户端证书、请使用以下过程之一：

- [已配置管理接口证书]
- CA颁发的客户端证书
- [从网格管理器生成的证书]

已配置管理接口证书

如果已使用客户提供的CA、客户端证书和专用密钥配置管理接口证书、请使用此操作步骤 添加客户端证书。

步骤

1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择 * 添加 * 。
3. 输入证书名称。
4. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
5. 选择 * 继续 * 。
6. 对于*attach certificates*步骤，请上传管理接口证书。
    a. 选择 * 上传证书 * 。
    b. 选择*浏览*并选择管理接口证书文件 (`.pem`) 。
        - 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。
        - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
    c. 选择 * 创建 * 以在网格管理器中保存证书。

    新证书将显示在客户端选项卡上。
7. 配置外部监控工具，如Grafana。

CA颁发的客户端证书

如果未配置管理接口证书、并且您计划为使用CA颁发的客户端证书和专用密钥的Prometheus添加客户端证书、请使用此操作步骤 添加管理员客户端证书。

步骤

1. 执行步骤至 "配置管理接口证书"。
2. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。

3. 选择 * 添加 * 。
4. 输入证书名称。
5. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
6. 选择 * 继续 * 。
7. 对于*attach certificates*步骤，上传客户端证书、私钥和CA包文件：
   a. 选择 * 上传证书 * 。
   b. 选择*浏览*并选择客户证书、私钥和CA包文件（`.pem`）。
      - 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。
      - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
   c. 选择 * 创建 * 以在网格管理器中保存证书。

      新证书将显示在客户端选项卡上。
8. 配置外部监控工具，如Grafana。

从网格管理器生成的证书

如果未配置管理接口证书、并且您计划为使用网格管理器中的生成证书功能的Prometheus添加客户端证书、请使用此操作步骤 添加管理员客户端证书。

步骤

1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择 * 添加 * 。
3. 输入证书名称。
4. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
5. 选择 * 继续 * 。
6. 对于*attach certificates*步骤，选择*Generate certificates*。
7. 指定证书信息：
   - 主题(可选)：证书所有者的X.509主题或可分辨名称(DN)。
   - 有效天数：生成的证书自生成之日起生效的天数。
   - 添加密钥用法扩展：如果选择(默认值和建议值)，则会将密钥用法扩展和扩展密钥用法扩展添加到生成的证书中。

     这些扩展定义了证书中所含密钥的用途。

     > 除非在证书包含这些扩展时遇到与旧客户端的连接问题、否则保持选中此复选框。
8. 选择 * 生成 * 。
9. 【客户端证书详细信息】选择*客户端证书详细信息*可显示证书元数据和证书PEM。

关闭此对话框后，您将无法查看此证书专用密钥。将密钥复制或下载到安全位置。

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制私钥 * 可复制证书私钥以粘贴到其他位置。
- 选择 * 下载私钥 * 将私钥另存为文件。

  指定私钥文件名和下载位置。

10. 选择 * 创建 * 以在网格管理器中保存证书。

    新证书将显示在客户端选项卡上。

11. 在网格管理器中、选择*配置*>*安全性*>*证书*、然后选择*全局*选项卡。
12. 选择*管理接口证书*。
13. 选择 * 使用自定义证书 * 。
14. 从上传certificate.pem和private_key.pem文件 客户端证书详细信息 步骤。无需上传CA捆绑包。
    a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
    b. 上传每个证书文件（`.pem`）。
    c. 选择 * 创建 * 以在网格管理器中保存证书。

       新证书将显示在客户端选项卡上。

15. 配置外部监控工具，如Grafana。

[[configure-External monitoring-tool]]配置外部监控工具

步骤

1. 在外部监控工具上配置以下设置，例如 Grafana 。
   a. * 名称 * ： 输入连接的名称。

      StorageGRID 不需要此信息，但您必须提供一个名称来测试连接。

   b. * URL * ： 输入管理节点的域名或 IP 地址。指定 HTTPS 和端口 9091 。

      例如： `https://admin-node.example.com:9091`

   c. 启用 * TLS 客户端身份验证 * 和 * 使用 CA 证书 * 。
   d. 在TLS/SSL身份验证详细信息下、复制并粘贴：+
      - 管理接口CA证书到"** CA证书"

    - 到"Client Cert"的客户端证书
    - "**客户端密钥"的专用密钥

  e. * 服务器名称 *： 输入管理节点的域名。

     servername 必须与管理接口证书中显示的域名匹配。

2. 保存并测试从 StorageGRID 或本地文件复制的证书和私钥。

   现在，您可以使用外部监控工具从 StorageGRID 访问 Prometheus 指标。

   有关指标的信息，请参见 "有关监控 StorageGRID 的说明"。

编辑客户端证书

您可以编辑管理员客户端证书以更改其名称，启用或禁用 Prometheus 访问，或者在当前证书已过期时上传新证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。

   表中列出了证书到期日期和 Prometheus 访问权限。如果证书即将过期或已过期，则表中会显示一条消息并触发警报。

2. 选择要编辑的证书。
3. 选择 * 编辑 * ，然后选择 * 编辑名称和权限 *
4. 输入证书名称。
5. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
6. 选择 * 继续 * 以在网格管理器中保存证书。

   更新后的证书将显示在客户端选项卡上。

附加新的客户端证书

您可以在当前证书过期后上传新证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。

   表中列出了证书到期日期和 Prometheus 访问权限。如果证书即将过期或已过期，则表中会显示一条消息并触发警报。

2. 选择要编辑的证书。
3. 选择 * 编辑 * ，然后选择编辑选项。

上传证书

复制证书文本以粘贴到其他位置。

a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
b. 上传客户端证书名称 (`.pem`) 。

   选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
c. 选择 * 创建 * 以在网格管理器中保存证书。

   更新后的证书将显示在客户端选项卡上。

生成证书

生成要粘贴到其他位置的证书文本。

a. 选择 * 生成证书 * 。
b. 指定证书信息：

   - 主题(可选)：证书所有者的X.509主题或可分辨名称(DN)。
   - 有效天数：生成的证书自生成之日起生效的天数。
   - 添加密钥用法扩展：如果选择(默认值和建议值)，则会将密钥用法扩展和扩展密钥用法扩展添加到生成的证书中。

     这些扩展定义了证书中所含密钥的用途。

     除非在证书包含这些扩展时遇到与旧客户端的连接问题、否则保持选中此复选框。
c. 选择 * 生成 * 。
d. 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。

   关闭此对话框后，您将无法查看此证书专用密钥。将密钥复制或下载到安全位置。

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

- 选择 * 复制私钥 * 可复制证书私钥以粘贴到其他位置。
- 选择 * 下载私钥 * 将私钥另存为文件。

  指定私钥文件名和下载位置。

e. 选择 * 创建 * 以在网格管理器中保存证书。

新证书将显示在客户端选项卡上。

下载或复制客户端证书

您可以下载或复制客户端证书以供其他位置使用。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择要复制或下载的证书。
3. 下载或复制证书。

下载证书文件

下载证书 `.pem` 文件

a. 选择 * 下载证书 * 。
b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

复制证书

复制证书文本以粘贴到其他位置。

a. 选择 * 复制证书 PEM* 。
b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

删除客户端证书

如果您不再需要管理员客户端证书，可以将其删除。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择要删除的证书。

3. 选择 * 删除 * ，然后确认。

> 要删除最多 10 个证书，请在客户端选项卡上选择要删除的每个证书，然后选择 * 操作 * > * 删除 * 。

删除证书后，使用该证书的客户端必须指定一个新的客户端证书，才能访问 StorageGRID Prometheus 数据库。

配置安全设置

管理**TLS**和**SSH**策略

TLS和SSH策略用于确定使用哪些协议和加密方法与客户端应用程序建立安全TLS连接、以及与内部StorageGRID 服务建立安全SSH连接。

此安全策略控制TLS和SSH如何对移动数据进行加密。通常、请使用现代兼容性(默认)策略、除非您的系统需要符合通用标准或您需要使用其他密钥。

> 某些StorageGRID 服务尚未更新、无法在这些策略中使用这些加密方法。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "root访问权限"。

选择一个安全策略

步骤

1. 选择*configuration*>*Security*>*Security settings。

   TLS和SSH策略*选项卡显示可用策略。当前活动的策略会在策略磁贴上标记为绿色复选标记。

2. 查看图块、了解可用策略。

策略	Description
现代兼容性(默认)	如果需要强加密、则使用默认策略、除非您有特殊要求。此策略与大多数TLS和SSH客户端兼容。

策略	Description
传统兼容性	如果需要为旧客户端提供其他兼容性选项、请使用此策略。此策略中的其他选项可能会使其不如现代兼容性策略安全。
通用标准	如果您需要通用标准认证、请使用此策略。
FIPS严格	如果您需要通用标准认证、并且需要使用NetApp加密安全模块3.0.0进行外部客户端连接以连接到负载平衡器端点、租户管理器和网格管理器、请使用此策略。使用此策略可能会降低性能。
自定义	如果需要应用您自己的用户名或用户名、请创建自定义策略。

3. 要查看有关每个策略的加密、协议和算法的详细信息，请选择*查看详细信息*。
4. 要更改当前策略，请选择*使用策略*。

   策略磁贴上的*current policy*旁边会出现一个绿色复选标记。

创建自定义安全策略

如果需要应用自己的用户名、可以创建自定义策略。

步骤

1. 从与要创建的自定义策略最相似的策略的磁贴中，选择*查看详细信息*。
2. 选择*复制到剪贴板*，然后选择*取消*。

3. 从“自定义策略”磁贴中，选择“配置和使用”。
4. 粘贴您复制的JSON并进行所需的任何更改。
5. 选择*使用策略*。

   自定义策略磁贴上的*当前策略*旁边会出现一个绿色复选标记。

6. (可选)选择*Edit configuration*对新的自定义策略进行更多更改。

暂时还原为默认安全策略

如果配置了自定义安全策略、并且配置的TLS策略与不兼容、则可能无法登录到网格管理器 "已配置服务器证书"。

您可以临时还原为默认安全策略。

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@Admin_Node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件

      以root用户身份登录后、提示符将从变为 `$` to `#`。

2. 运行以下命令：

```
restore-default-cipher-configurations
```

3. 从 Web 浏览器访问同一管理节点上的网格管理器。
4. 按照中的步骤进行操作 选择一个安全策略 以重新配置策略。

配置网络和对象安全性

您可以将网络和对象安全性配置为对存储的对象进行加密、防止某些S3和Swift请求、或者允许客户端连接到存储节点时使用HTTP而不是HTTPS。

存储对象加密

通过存储对象加密、可以在通过S3读取所有对象数据时对这些数据进行加密。默认情况下、存储的对象不会进行加密、但您可以选择使用AES‐128或AES‐256加密算法对对象进行加密。启用此设置后，所有新载入的对象都将被加密，但不会对现有存储的对象进行任何更改。如果禁用加密、则当前加密的对象仍会保持加密状态、但不会对新加装的对象进行加密。

存储的对象加密设置仅适用于尚未通过存储分段级或对象级加密进行加密的S3对象。

有关StorageGRID 加密方法的更多详细信息、请参见 "查看 StorageGRID 加密方法"。

防止修改客户端

防止客户端修改是一项系统范围的设置。如果选择了*prevent client修改*选项，则会拒绝以下请求。

S3 REST API

- 删除存储分段请求

- 修改现有对象数据，用户定义的元数据或 S3 对象标记的任何请求

Swift REST API

- 删除容器请求
- 修改任何现有对象的请求。例如，以下操作被拒绝： PUT 覆盖，删除，元数据更新等。

为存储节点连接启用**HTTP**

默认情况下、客户端应用程序会使用HTTPS网络协议直接连接到存储节点。您可以选择为这些连接启用 HTTP ，例如在测试非生产网格时。

仅当S3和Swift客户端需要直接与存储节点建立HTTP连接时、才使用HTTP进行存储节点连接。对于仅使用HTTPS连接的客户端或连接到负载平衡器服务的客户端、您无需使用此选项(因为您可以 "配置每个负载平衡器端点" 以使用HTTP或HTTPS)。

请参见 "摘要：客户端连接的 IP 地址和端口" 了解S3和Swift客户端在使用HTTP或HTTPS连接到存储节点时使用的端口。

选择选项

开始之前

- 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*configuration*>*Security*>*Security settings。
2. 选择*网络和对象*选项卡。
3. 对于存储的对象加密，如果不希望对存储的对象进行加密，请使用*None*(默认)设置，或者选择*AES-128*或*AES-256*对存储的对象进行加密。
4. 如果要阻止S3和Swift客户端发出特定请求，可选择*prevent client修改*。

   > 如果更改此设置，则应用新设置需要大约一分钟的时间。已配置的值将进行缓存以提高性能和扩展能力。

5. 如果客户端直接连接到存储节点并且您要使用HTTP连接，则可以选择*为存储节点连接启用HTTP *。

   > 为生产网格启用 HTTP 时请务必小心，因为请求会以未加密方式发送。

6. 选择 * 保存 * 。

更改浏览器非活动超时

如果 Grid Manager 和租户管理器用户处于非活动状态的时间超过一段时间，您可以控制他们是否已注销。

开始之前

- 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

浏览器非活动超时默认为15分钟。如果用户的浏览器在此时间段内未处于活动状态、则该用户将被注销。

您可以根据需要通过设置*注销非活动用户*选项来增加或减少超时期限。

浏览器非活动超时还受以下因素控制：

- 一个单独的不可配置 StorageGRID 计时器，其中包括用于系统安全保护的计时器。默认情况下，每个用户的身份验证令牌在用户登录后 16 小时到期。当用户的身份验证过期时、即使禁用了浏览器非活动超时或尚未达到浏览器超时值、该用户也会自动注销。要续订令牌，用户必须重新登录。
- 身份提供程序的超时设置(假设为StorageGRID 启用了单点登录(SSO))。

  如果启用了SSO且用户的浏览器超时、则用户必须重新输入其SSO凭据才能再次访问StorageGRID。请参见 "配置单点登录"。

步骤

1. 选择*configuration*>*Security*>*Security settings。
2. 选择*浏览器非活动超时*选项卡。
3. 在*注销非活动用户后*字段中，指定浏览器超时期限，介于60秒到7天之间。

   您可以指定浏览器超时期限(以秒、分钟、小时或天为单位)。

4. 选择 * 保存 * 。如果浏览器在指定时间内处于非活动状态、则用户将从网格管理器或租户管理器中注销。

   新设置不会影响当前已登录的用户。用户必须重新登录或刷新浏览器，新的超时设置才能生效。

配置密钥管理服务器

配置密钥管理服务器：概述

您可以配置一个或多个外部密钥管理服务器（ 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器（ **KMS** ）？

密钥管理服务器（ 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。

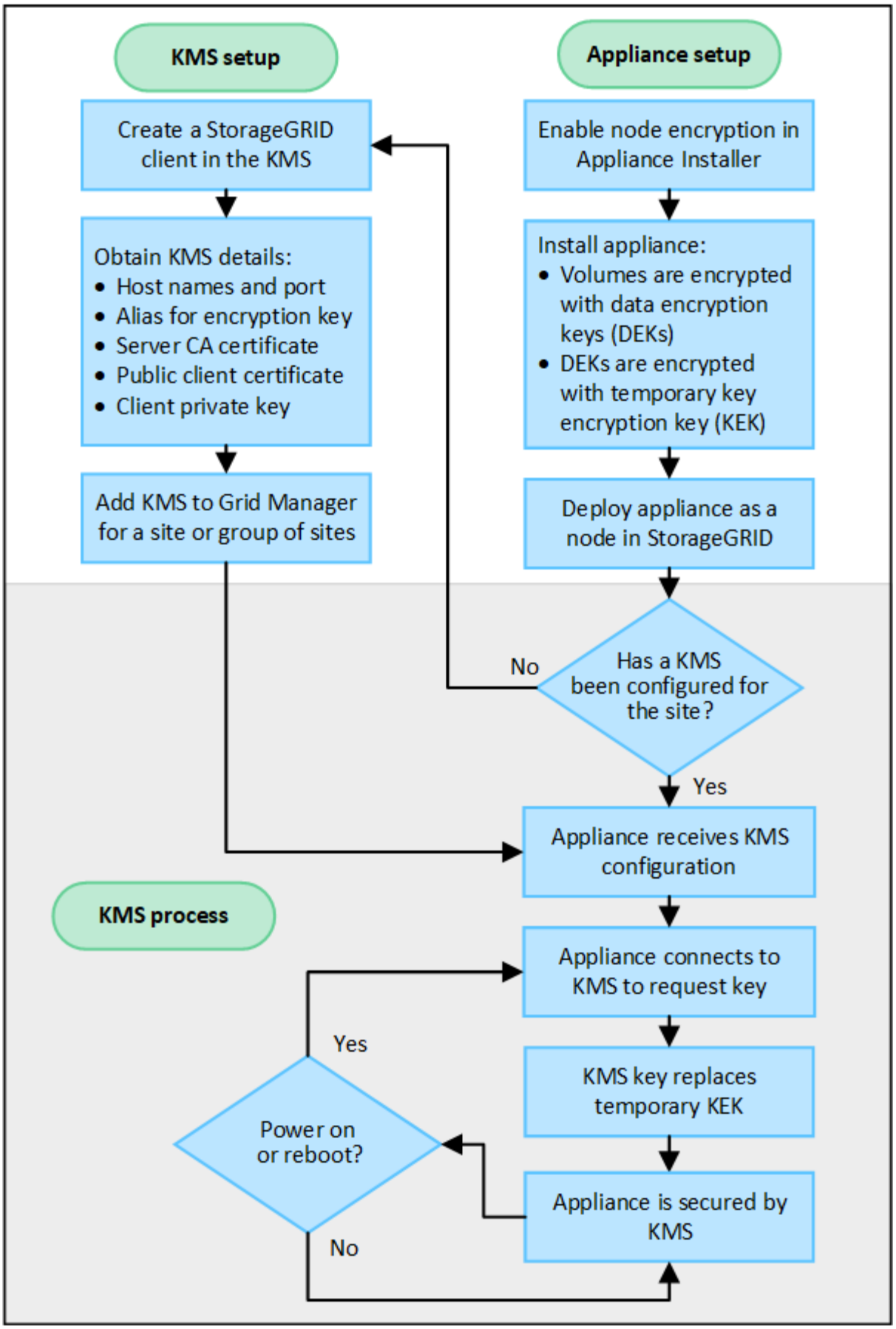
您可以使用一个或多个密钥管理服务器来管理安装期间启用了 * 节点加密 * 设置的任何 StorageGRID 设备节点的节点加密密钥。通过将密钥管理服务器与这些设备节点结合使用，您可以保护数据，即使设备已从数据中心中删除也是如此。对设备卷进行加密后、您将无法访问设备上的任何数据、除非此节点可以与KMS进行通信。

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器来保护 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器（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格管理器中配置密钥管理服务器。

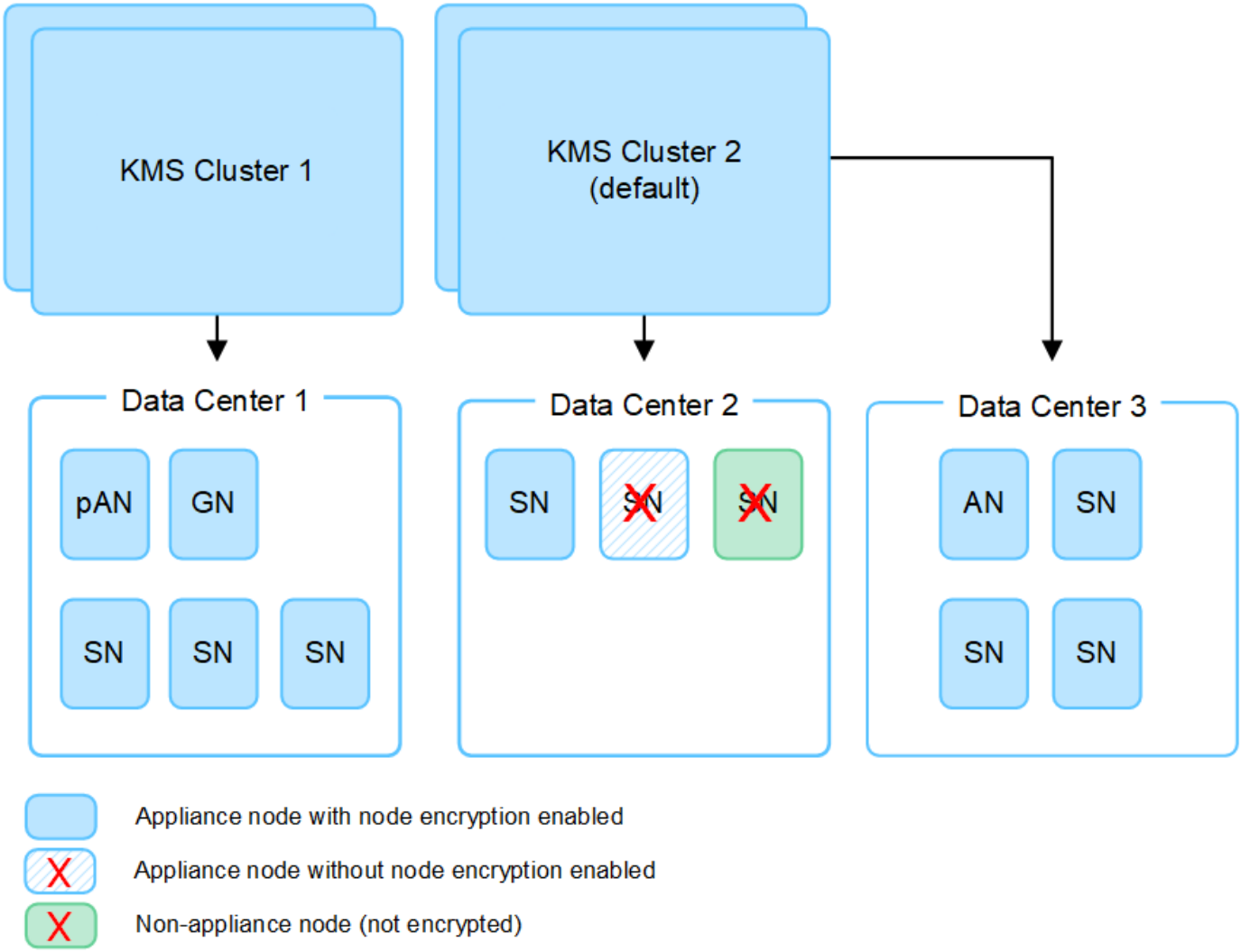
我需要多少个密钥管理服务器?

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。

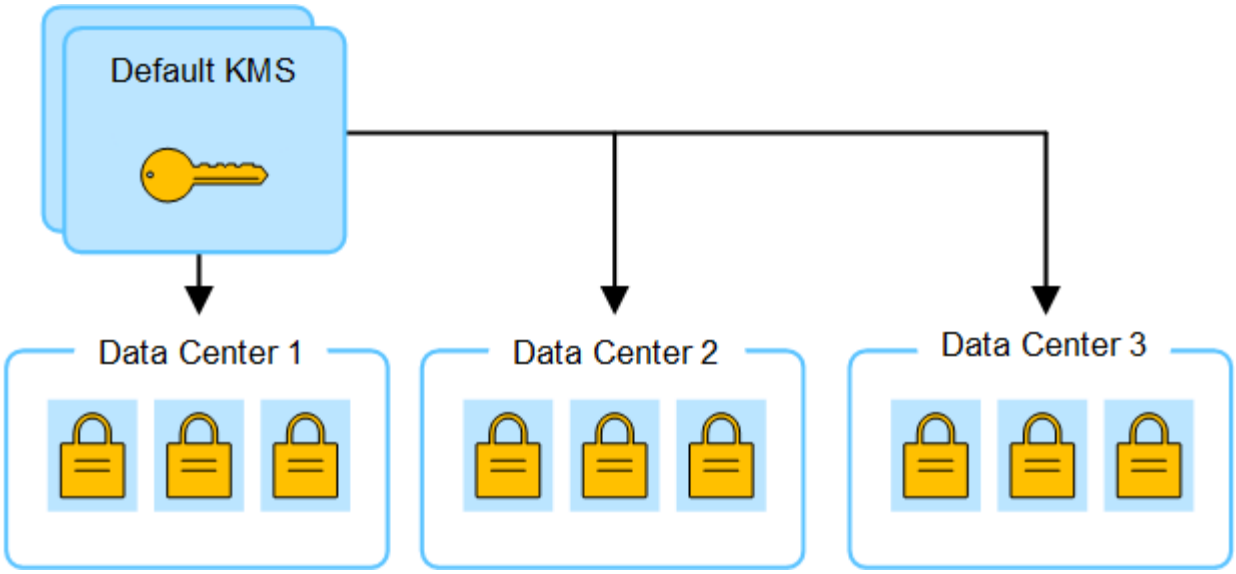
更改站点的 **KMS** 的注意事项

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 。

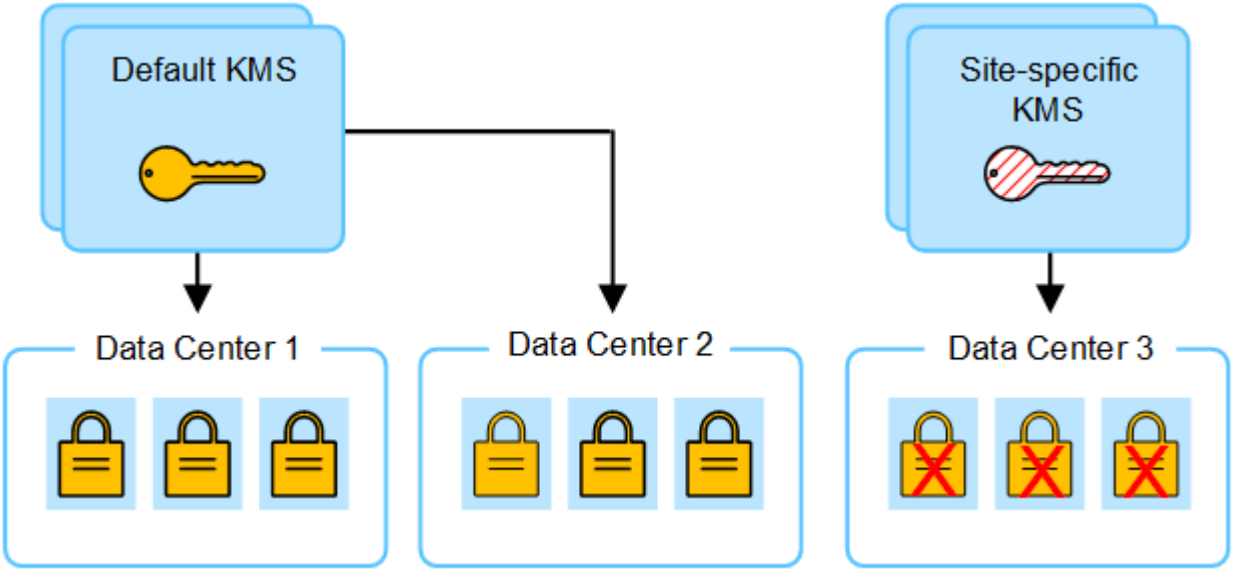
如果更改站点使用的 KMS ，则必须确保可以使用存储在新 KMS 上的密钥对该站点上先前加密的设备节点进行解密。在某些情况下，您可能需要将当前版本的加密密钥从原始 KMS 复制到新 KMS 。您必须确保 KMS 具有正确的密钥，以便对站点上的加密设备节点进行解密。

例如：

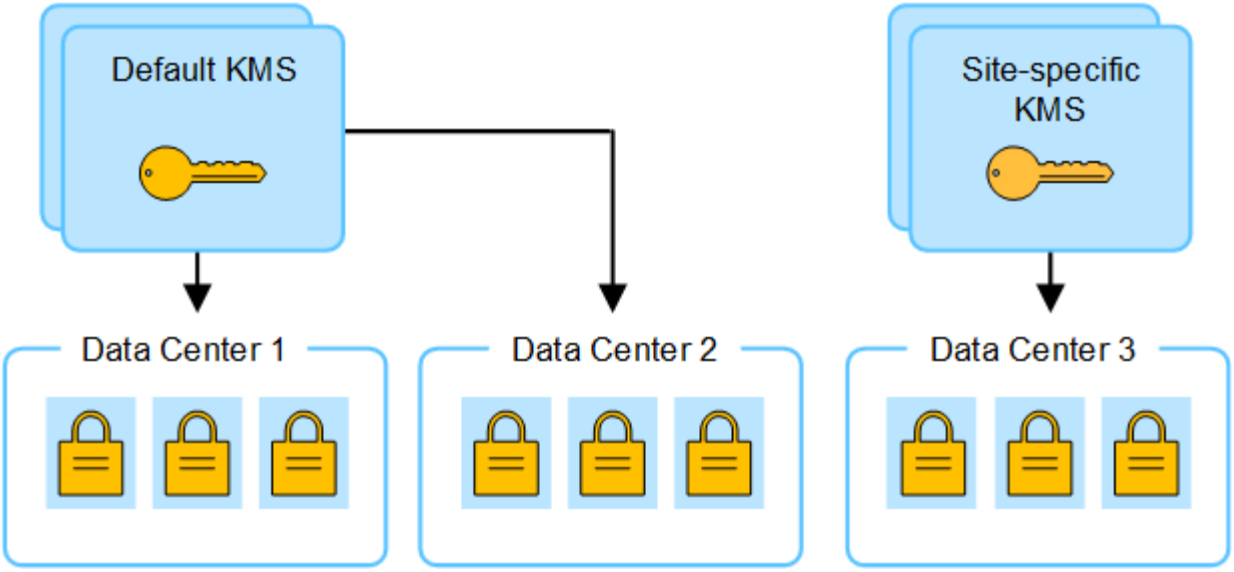
1. 您最初会配置一个默认KMS、用于适用场景 所有没有专用KMS的站点。
2. 保存 KMS 后，所有启用了 * 节点加密 * 设置的设备节点都会连接到 KMS 并请求加密密钥。此密钥用于对所有站点上的设备节点进行加密。此外，还必须使用此相同密钥对这些设备进行解密。



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 。	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。 "编辑密钥管理服务器（KMS）"
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。	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. 使用网格管理器添加新的 KMS 并选择站点。 "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 。 2. 使用网格管理器编辑现有 KMS 配置并输入新的主机名或 IP 地址。 "添加密钥管理服务器（KMS）"

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Thles 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。

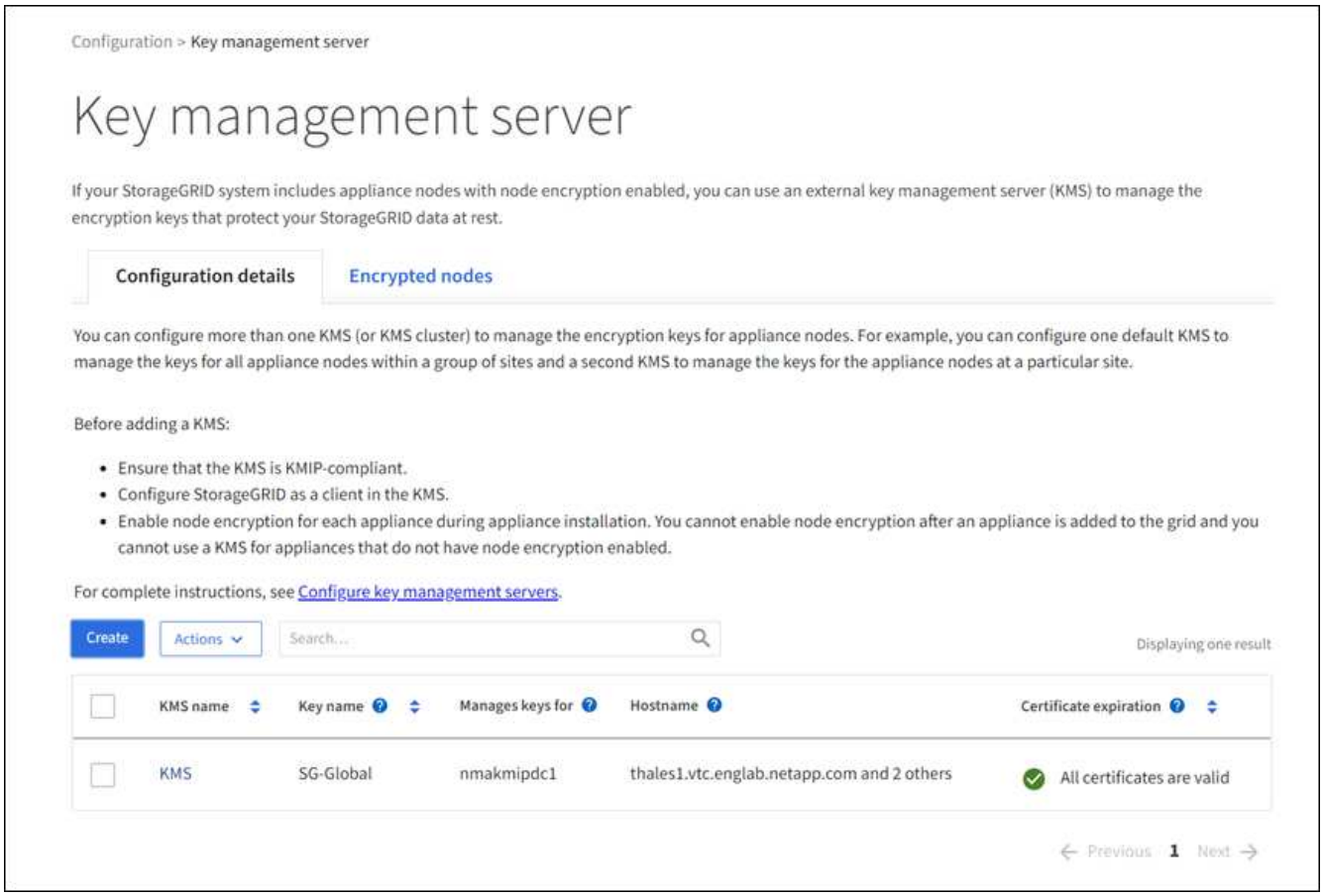
第**1**步：公里详细信息

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

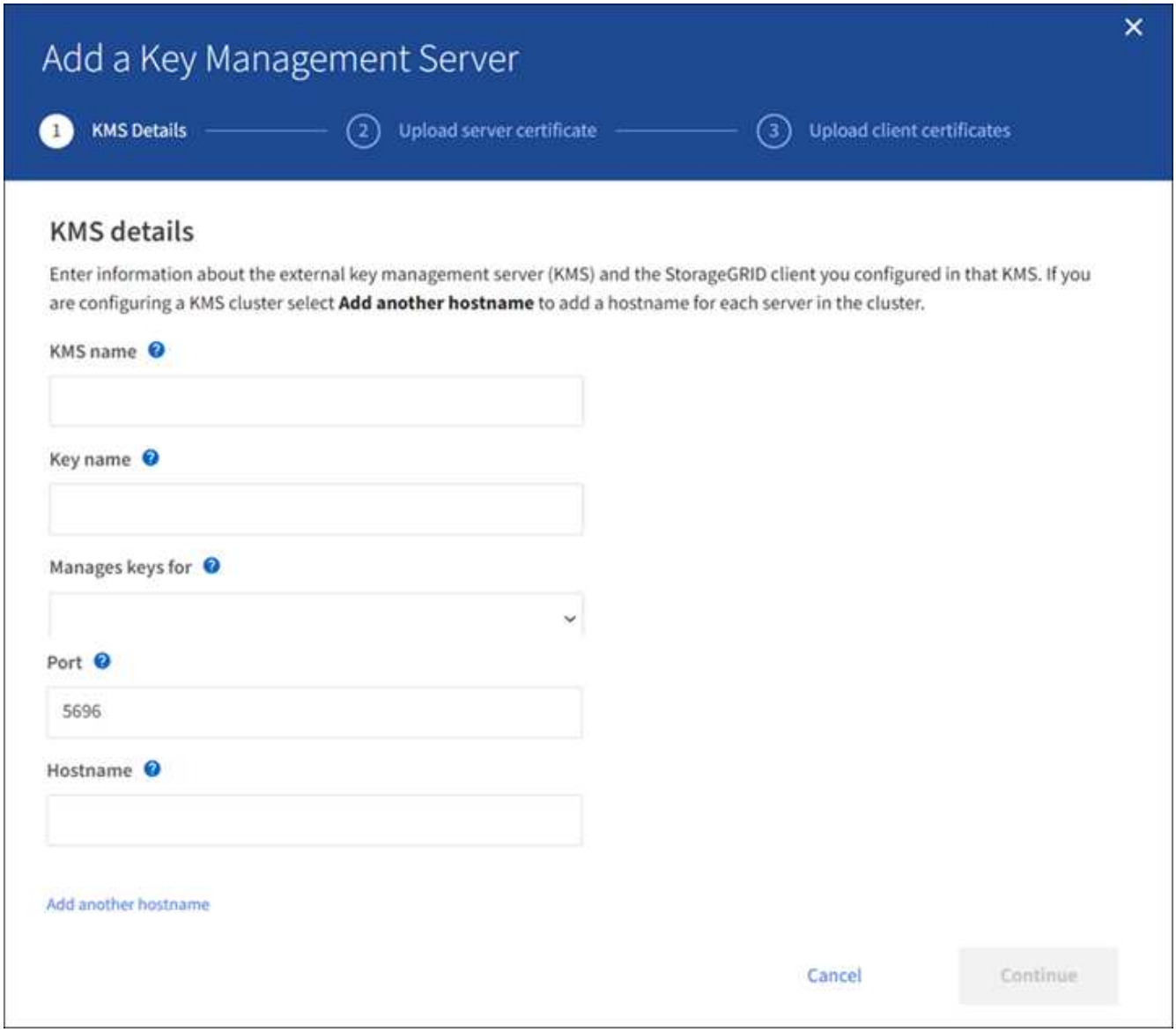
1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

   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。



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)。



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	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。 ◦ 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。

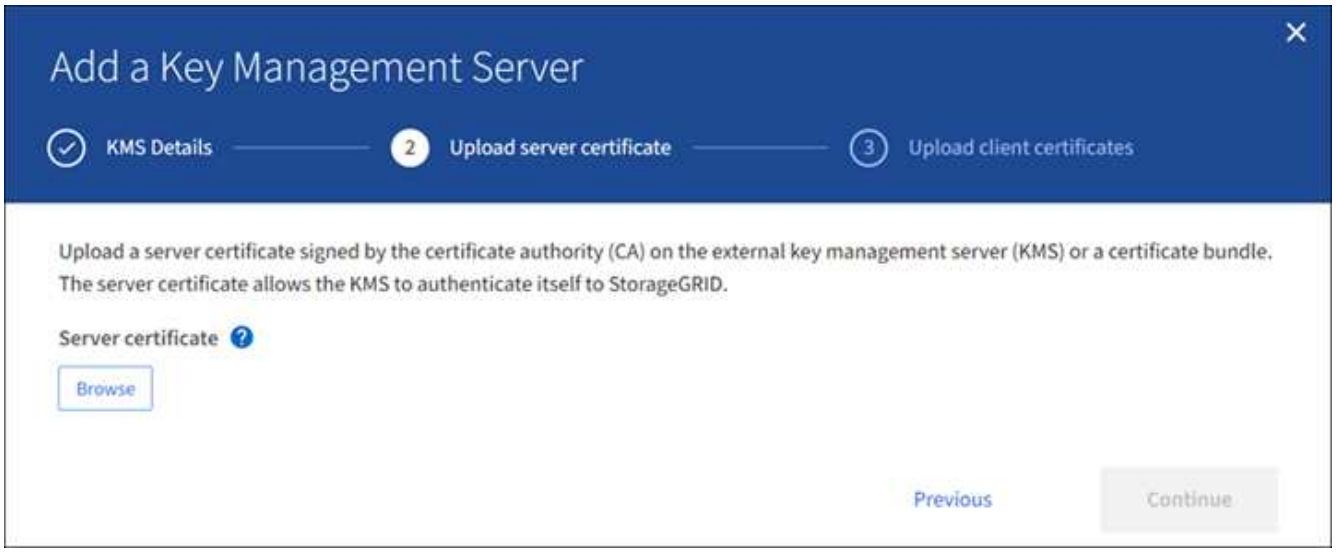
4. 如果要配置KMS群集，请选择*添加另一主机名*为群集中的每台服务器添加主机名。
5. 选择 * 继续 * 。

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。

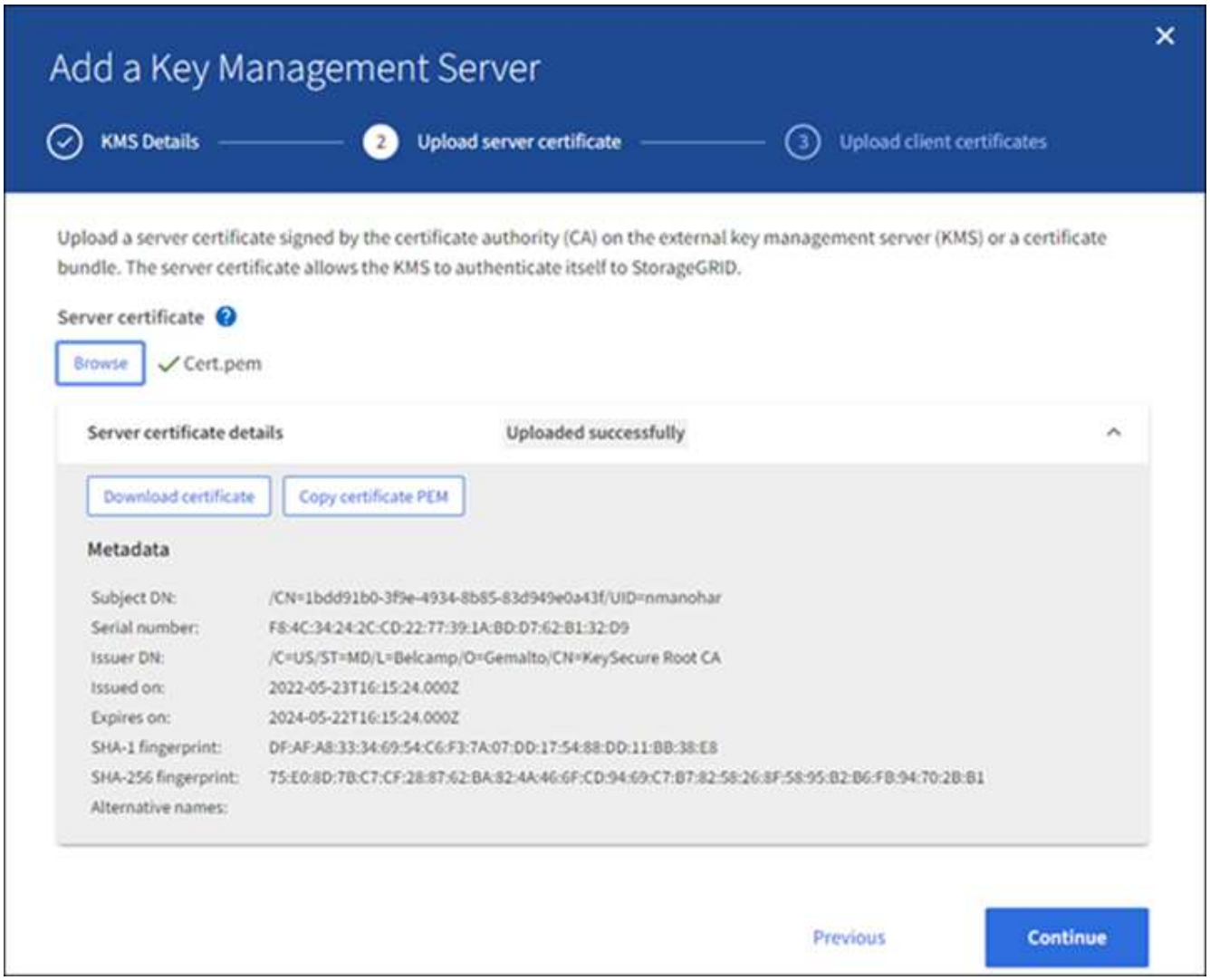
步骤

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。



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。

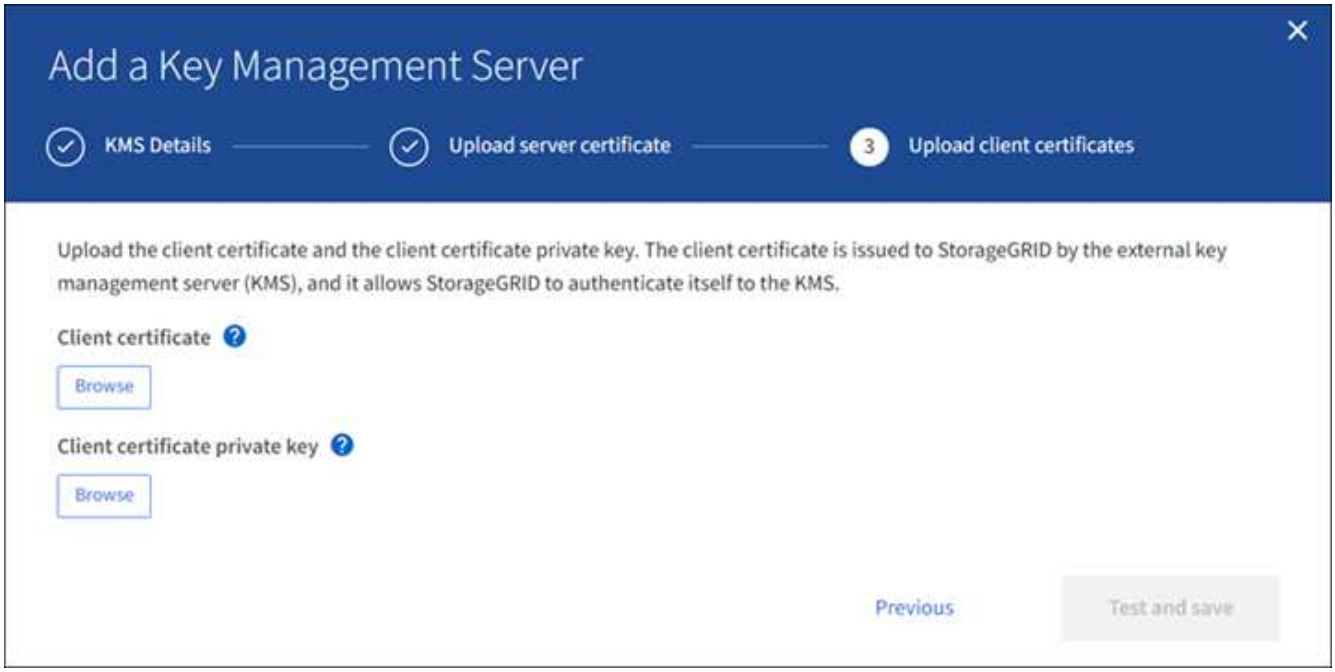
3. 选择 * 继续 * 。

第3步：上传客户端证书

在添加密钥管理服务器向导的步骤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

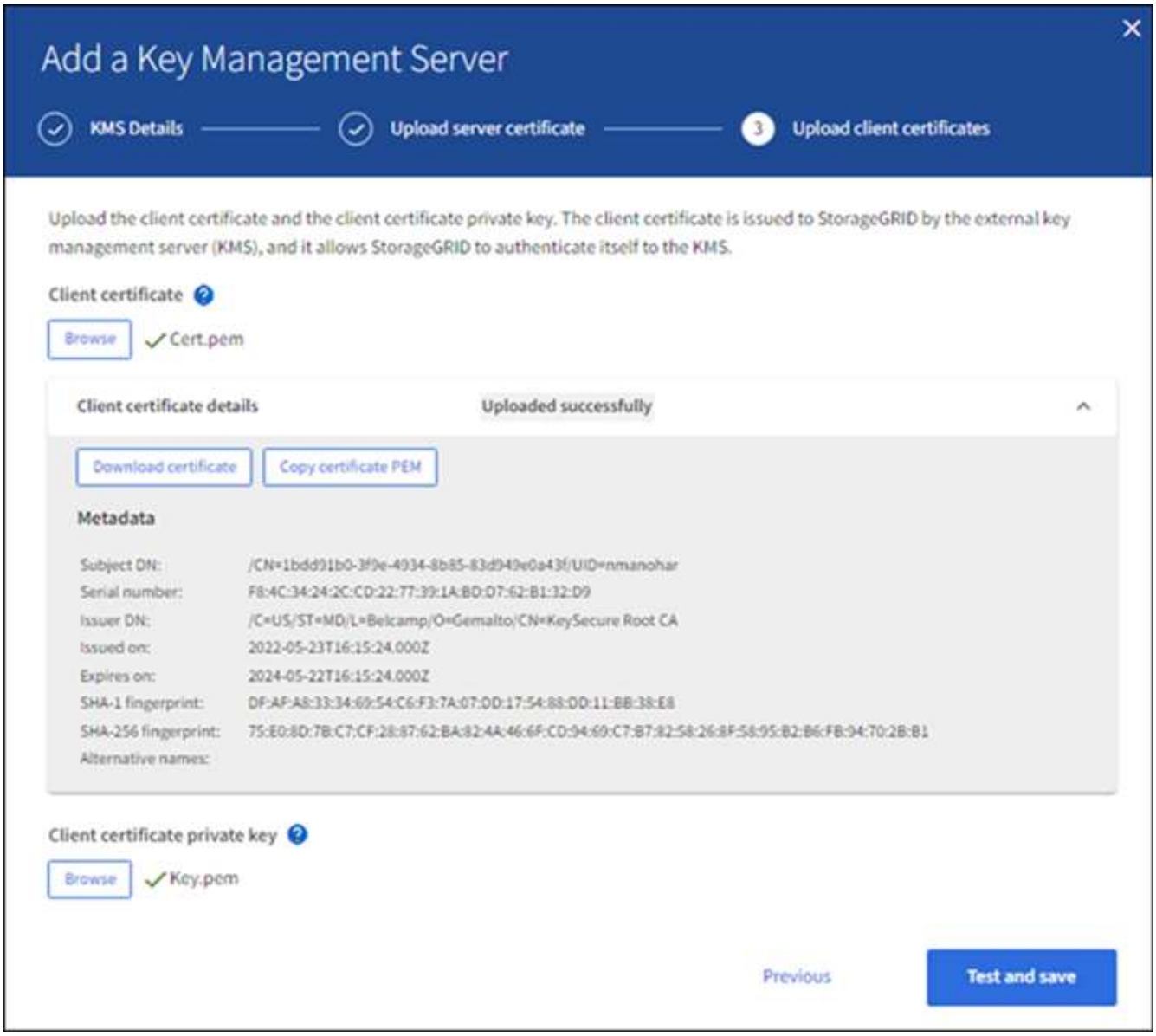
1. 从*步骤3 (上传客户端证书)*中，浏览到客户端证书的位置。



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。



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	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。 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 。
Status	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。 • 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*。

   您也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	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。 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。 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。 "使用密钥管理服务器的注意事项和要求"
管理的密钥	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。 *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。
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。

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"。
- 您将使用登录到网格管理器 "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。

管理代理设置

配置存储代理设置

如果您使用的是平台服务或云存储池，则可以在存储节点和外部 S3 端点之间配置非透明代理。例如，您可能需要一个非透明代理来允许将平台服务消息发送到外部端点，例如 Internet 上的端点。

开始之前

- 您具有特定的访问权限。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。

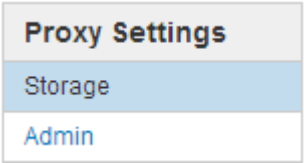
关于此任务

您可以为单个存储代理配置设置。

步骤

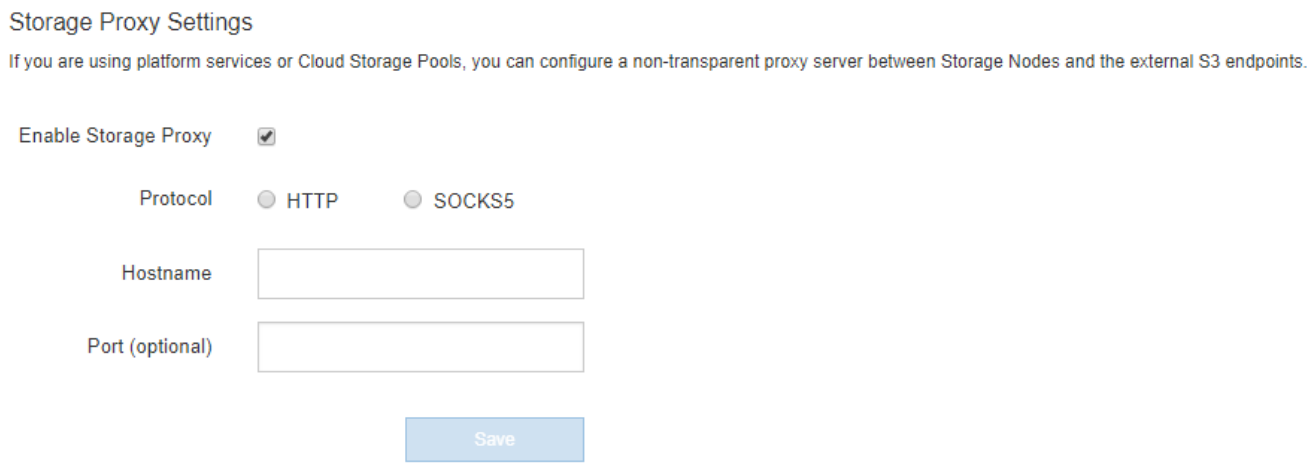
1. 选择 * 配置 * > * 安全性 * > * 代理设置 * 。

   此时将显示存储代理设置页面。默认情况下，在边栏菜单中选择了 * 存储 * 。

2. 选中*启用存储代理*复选框。

   此时将显示用于配置存储代理的字段。



3. 为非透明存储代理选择协议。
4. 输入代理服务器的主机名或 IP 地址。
5. （可选）输入用于连接到代理服务器的端口。

   如果对协议使用默认端口，则可以将此字段留空： 80 表示 HTTP ， 1080 表示 SOCKS5 。

6. 选择 * 保存 * 。

   保存存储代理后，可以配置和测试平台服务或云存储池的新端点。

   > 代理更改可能需要长达 10 分钟才能生效。

7. 检查代理服务器的设置，以确保不会阻止来自 StorageGRID 的平台服务相关消息。

完成后

如果需要禁用存储代理，请清除*启用存储代理*复选框，然后选择*保存*。

相关信息

- "用于平台服务的网络和端口"
- "使用 ILM 管理对象"

配置管理员代理设置

如果使用 HTTP 或 HTTPS 发送 AutoSupport 消息（请参见 "配置 AutoSupport"），您可以在管理节点和技术支持（AutoSupport）之间配置非透明代理服务器。

开始之前

- 您具有特定的访问权限。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。

关于此任务

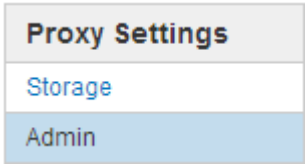
您可以为单个管理员代理配置设置。

步骤

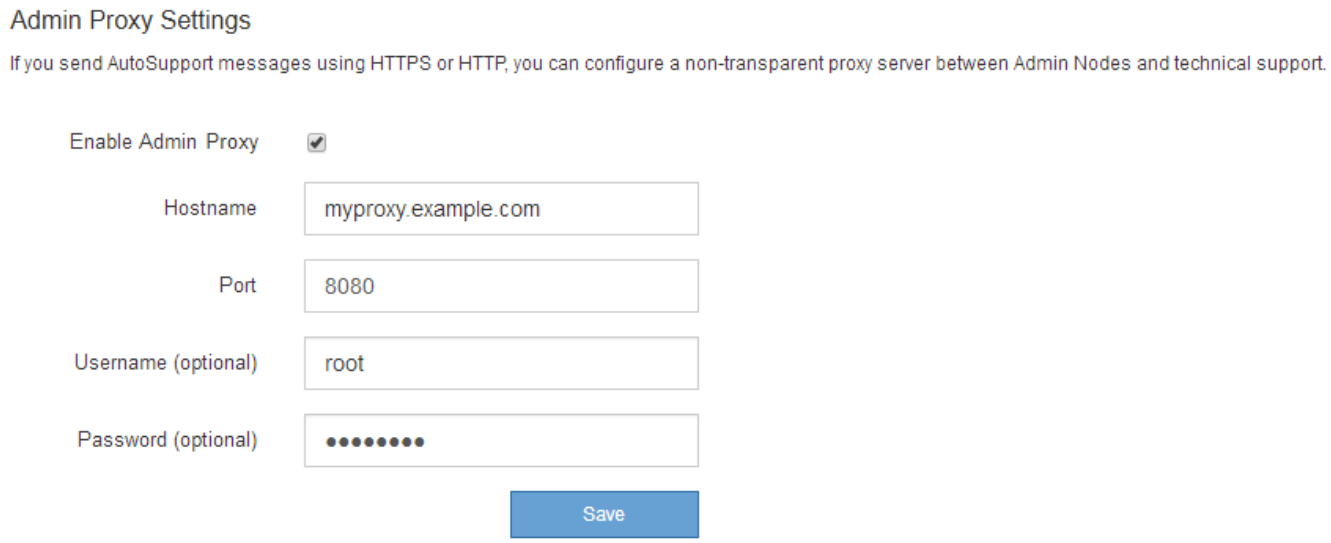
1. 选择 * 配置 * > * 安全性 * > * 代理设置 * 。

   此时将显示 Admin Proxy Settings 页面。默认情况下，在边栏菜单中选择了 * 存储 * 。

2. 从边栏菜单中选择 * 管理 * 。



3. 选中*启用管理员代理*复选框。



4. 输入代理服务器的主机名或 IP 地址。
5. 输入用于连接到代理服务器的端口。
6. （可选）输入代理用户名。

   如果您的代理服务器不需要用户名，请将此字段留空。

7. （可选）输入代理密码。

   如果您的代理服务器不需要密码，请将此字段留空。

8. 选择 * 保存 * 。

   保存管理代理后，将在管理节点和技术支持之间配置代理服务器。

   > 代理更改可能需要长达 10 分钟才能生效。

9. 如果需要禁用代理，请清除*启用管理员代理*复选框，然后选择*保存*。

控制防火墙

在外部防火墙处控制访问

您可以在外部防火墙处打开或关闭特定端口。

您可以通过在外部防火墙中打开或关闭特定端口来控制对 StorageGRID 管理节点上用户界面和 API 的访问。例如，除了使用其他方法控制系统访问之外，您可能还希望防止租户能够在防火墙处连接到网格管理器。

如果要配置StorageGRID 内部防火墙、请参见 "配置内部防火墙"。

Port	Description	端口是否已打开 ...
443.	管理节点的默认 HTTPS 端口	Web 浏览器和管理 API 客户端可以访问网格管理器，网格管理 API ，租户管理器和租户管理 API 。 • 注： * 端口 443 也用于某些内部流量。
8443	管理节点上的网格管理器端口受限	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问网格管理器和网格管理 API 。 • Web浏览器和管理API客户端无法访问租户管理器或租户管理API。 • 请求内部内容将被拒绝。
9443	管理节点上的租户管理器端口受限	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问租户管理器和租户管理 API 。 • Web浏览器和管理API客户端无法访问网格管理器或网格管理API。 • 请求内部内容将被拒绝。

受限网格管理器或租户管理器端口上不提供单点登录（ SSO ）。如果您希望用户通过单点登录进行身份验证，则必须使用默认 HTTPS 端口（ 443 ）。

相关信息

- "登录到网格管理器"
- "创建租户帐户"
- "外部通信"

管理内部防火墙控制

StorageGRID 在每个节点上都包含一个内部防火墙、可通过控制对节点的网络访问来增强网格的安全性。使用防火墙可阻止对特定网格部署所需端口以外的所有端口进行网络访问。在防火墙控制页面上所做的配置更改将部署到每个节点。

使用防火墙控制页面上的三个选项卡自定义网格所需的访问权限。

- 特权地址列表：使用此选项卡允许对关闭的端口进行选定访问。您可以使用CIDR表示法添加IP地址或子网、以访问使用管理外部访问选项卡关闭的端口。
- 管理外部访问：使用此选项卡关闭默认打开的端口，或重新打开先前关闭的端口。
- 不可信客户端网络：使用此选项卡指定节点是否信任来自客户端网络的入站流量。

  此选项卡还提供了指定在配置了不可信客户端网络时要打开的其他端口的选项。这些端口可以提供对网格管理器和/或租户管理器的访问。

  此选项卡上的设置将覆盖管理外部访问选项卡中的设置。

  - 具有不可信客户端网络的节点仅接受在该节点上配置的负载平衡器端点端口(全局端点、节点接口和受节点类型制约的端点)上的连接。
  - 在不可信客户端网络选项卡下打开的其他端口将在所有不可信客户端网络上打开、即使未配置负载平衡器端点也是如此。
  - 无论"管理外部网络"选项卡上的设置如何、负载平衡器端点端口和选定的其他端口_都是不可信客户端网络上唯一打开的端口_。
  - 如果受信任、则可以访问在"管理外部访问"选项卡下打开的所有端口以及在客户端网络上打开的任何负载平衡器端点。

> 您在一个选项卡上所做的设置可能会影响您在另一个选项卡上所做的访问更改。请务必检查所有选项卡上的设置、以确保您的网络按预期方式运行。

要配置内部防火墙控制、请参见 "配置防火墙控件"。

有关外部防火墙和网络安全的详细信息、请参阅 "在外部防火墙处控制访问"。

特权地址列表和管理外部访问选项卡

通过特权地址列表选项卡、您可以注册一个或多个被授予对关闭的网格端口访问权限的IP地址。通过"管理外部访问"选项卡、您可以关闭对选定外部端口或所有打开的外部端口的外部访问(默认情况下、外部端口可由非网格节点访问)。这两个选项卡通常可结合使用来定制网格所需的确切网络访问。

> 默认情况下、有权限的IP地址不具有内部网格端口访问权限。

示例**1**：使用跳转主机执行维护任务

假设您要使用跳转主机(一个增强安全的主机)进行网络管理。您可以使用以下常规步骤：

1. 使用特权地址列表选项卡添加跳转主机的IP地址。
2. 使用管理外部访问选项卡阻止所有端口。

> 在阻止端口443和8443之前、请添加特权IP地址。当前连接到被阻止端口的任何用户(包括您)将无法访问Grid Manager、除非其IP地址已添加到特权地址列表中。

保存配置后、网格中管理节点上的所有外部端口都将被阻止用于除跳转主机之外的所有主机。然后、您可以使用跳转主机更安全地在网格上执行维护任务。

示例**2**：限制对网格管理器和租户管理器的访问

假设出于安全原因、您希望限制对网格管理器和租户管理器的访问。您可以使用以下常规步骤：

1. 使用"管理外部访问"选项卡上的切换功能阻止端口443。
2. 使用管理外部访问选项卡上的切换以允许访问端口8443。
3. 使用管理外部访问选项卡上的切换以允许访问端口9443。

保存配置后、主机将无法访问端口443、但仍可通过端口8443访问网格管理器、并通过端口9443访问租户管理器。

示例**3**：锁定敏感端口

假设您要锁定敏感端口以及该端口上的服务(例如、端口22上的SSH)。您可以使用以下常规步骤：

1. 使用特权地址列表选项卡仅向需要访问服务的主机授予访问权限。
2. 使用管理外部访问选项卡阻止所有端口。

> 在阻止端口443和8443之前、请添加特权IP地址。当前连接到被阻止端口的任何用户(包括您)将无法访问Grid Manager、除非其IP地址已添加到特权地址列表中。

保存配置后、端口22和SSH服务将可供特权地址列表中的主机使用。无论请求来自哪个接口、所有其他主机都将被拒绝访问此服务。

示例**4**：禁止访问未使用的服务

在网络级别、您可以禁用一些不打算使用的服务。例如、如果您不提供Swift访问、则应执行以下常规步骤：

1. 使用管理外部访问选项卡上的切换功能阻止端口18083。
2. 使用管理外部访问选项卡上的切换功能阻止端口18085。

保存配置后、存储节点将不再允许Swift连接、而是继续允许访问未阻止的端口上的其他服务。

不可信客户端网络选项卡

如果您使用的是客户端网络、则可以通过仅在显式配置的端点或您在此选项卡上选择的其他端口上接受入站客户端流量来帮助保护StorageGRID 免受恶意攻击。

默认情况下，每个网格节点上的客户端网络均为 *trusted* 。也就是说、默认情况下、StorageGRID 信任所有网格节点的入站连接 "可用外部端口"。

您可以通过指定每个节点上的客户端网络为 *untrused_* 来减少对 StorageGRID 系统的恶意攻击威胁。如果节点的客户端网络不可信、则该节点仅接受显式配置为负载平衡器端点的端口以及使用防火墙控制页面上的不可信客户端网络选项卡指定的任何其他端口上的入站连接。请参见 "配置负载平衡器端点" 和 "配置防火墙控件"。

示例 **1** ： 网关节点仅接受 **HTTPS S3** 请求

假设您希望网关节点拒绝客户端网络上除 HTTPS S3 请求以外的所有入站流量。您应执行以下常规步骤：

1. 从 "负载平衡器端点" 页面上、通过端口443为基于HTTPS的S3配置负载平衡器端点。

2. 在防火墙控制页面中、选择不可信以指定网关节点上的客户端网络不可信。

保存配置后，网关节点客户端网络上的所有入站流量都会被丢弃，但端口 443 上的 HTTPS S3 请求和 ICMP 回显（ping）请求除外。

示例 **2**：存储节点发送 **S3** 平台服务请求

假设您要启用来自存储节点的出站S3平台服务流量、但要阻止客户端网络上与该存储节点的任何入站连接。您应执行此常规步骤：

- 在防火墙控制页面的不可信客户端网络选项卡中、指示存储节点上的客户端网络不可信。

保存配置后、存储节点将不再接受客户端网络上的任何传入流量、但仍允许向已配置的平台服务目标发出出站请求。

示例**3**：限制对网格管理器的子网访问

假设您希望仅允许对特定子网进行网格管理器访问。您应执行以下步骤：

1. 将管理节点的客户端网络连接到子网。
2. 使用不可信客户端网络选项卡将客户端网络配置为不可信。
3. 在选项卡的*在不可信客户端网络上打开的其他端口*部分，添加端口443或8443。
4. 使用管理外部访问选项卡阻止所有外部端口(无论是否为该子网以外的主机设置了特权IP地址)。

保存配置后、只有指定子网上的主机才能访问网格管理器。所有其他主机均被阻止。

配置内部防火墙

您可以配置StorageGRID 防火墙以控制对StorageGRID 节点上特定端口的网络访问。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 您已查看中的信息 "管理防火墙控制" 和 "网络连接准则"。
- 如果您希望管理节点或网关节点仅在显式配置的端点上接受入站流量，则已定义负载平衡器端点。

> 更改客户端网络的配置时、如果未配置负载平衡器端点、现有客户端连接可能会失败。

关于此任务

StorageGRID 在每个节点上都有一个内部防火墙、可用于打开或关闭网格节点上的部分端口。您可以使用防火墙控制选项卡打开或关闭网格网络、管理网络和客户端网络上默认打开的端口。您还可以创建一个可访问关闭的网格端口的特权IP地址列表。如果您使用的是客户端网络、则可以指定节点是否信任客户端网络的入站流量、并且可以配置客户端网络上特定端口的访问。

将向网格外部的IP地址开放的端口数限制为仅限绝对必要的端口、可增强网格的安全性。您可以使用三个防火墙控制选项卡中每个选项卡上的设置来确保仅打开所需的端口。

有关使用防火墙控件的详细信息(包括示例)、请参见 "管理防火墙控制"。

有关外部防火墙和网络安全的详细信息、请参阅 "在外部防火墙处控制访问"。

访问防火墙控件

步骤

1. 选择*configuration*>*Security*>*Firewall control*。

   介绍了此页面上的三个选项卡 "管理防火墙控制"。

2. 选择任何选项卡以配置防火墙控件。

   您可以按任意顺序使用这些选项卡。您在一个选项卡上设置的配置不会限制在其他选项卡上可以执行的操作；但是、在一个选项卡上进行的配置更改可能会更改在其他选项卡上配置的端口的行为。

特权地址列表

您可以使用特权地址列表选项卡授予主机对默认关闭或通过管理外部访问选项卡上的设置关闭的端口的访问权限。

默认情况下、有权限的IP地址和子网不具有内部网格访问权限。此外、即使在"管理外部访问"选项卡中阻止了负载平衡器端点和在"特权地址列表"选项卡中打开的其他端口、也可以访问。

> 特权地址列表选项卡上的设置不能覆盖不可信客户端网络选项卡上的设置。

步骤

1. 在特权地址列表选项卡上、输入要授予对已关闭端口的访问权限的地址或IP子网。
2. (可选)选择*以CIDR表示法添加其他IP地址或子网*以添加其他有权限的客户端。

   > 向特权列表中添加尽可能少的地址。

3. (可选)选择*允许有权限的IP地址访问StorageGRID 内部端口*。请参见 "StorageGRID 内部端口"。

   > 此选项会删除对内部服务的一些保护。如果可能、请将其禁用。

4. 选择 * 保存 * 。

管理外部访问

在"管理外部访问"选项卡中关闭某个端口后、任何非网格IP地址都无法访问该端口、除非您将该IP地址添加到特权地址列表中。您只能关闭默认情况下处于打开状态的端口、并且只能打开已关闭的端口。

> "管理外部访问"选项卡上的设置无法覆盖"不可信客户端网络"选项卡上的设置。例如、如果节点不可信、则客户端网络上会阻止端口SSH/ 22、即使此端口在管理外部访问选项卡上打开也是如此。不可信客户端网络选项卡上的设置会覆盖客户端网络上已关闭的端口(例如443、8443、9443)。

步骤

1. 选择*管理外部访问*。此选项卡将显示一个表、其中包含网格中节点的所有外部端口(默认情况下可由非网格节点访问的端口)。
2. 使用以下选项配置要打开和关闭的端口：
   - 使用每个端口旁边的切换键打开或关闭选定端口。
   - 选择*打开所有显示的端口*以打开表中列出的所有端口。
   - 选择*关闭所有显示的端口*以关闭表中列出的所有端口。

   > 如果关闭网格管理器端口443或8443、则当前连接到被阻止端口的任何用户(包括您)将无法访问网格管理器、除非其IP地址已添加到特权地址列表中。

   > 使用表右侧的滚动条确保您已查看所有可用端口。使用搜索字段输入端口号以查找任何外部端口的设置。您可以输入部分端口号。例如，如果输入*2*，则会显示名称中包含字符串“2”的所有端口。

3. 选择 * 保存 *

不可信客户端网络

如果节点的客户端网络不可信、则该节点仅接受配置为负载平衡器端点的端口以及您在此选项卡上选择的其他端口(可选)上的入站流量。您还可以使用此选项卡为扩展中添加的新节点指定默认设置。

> 如果尚未配置负载平衡器端点，现有客户端连接可能会失败。

在*不可信客户端网络*选项卡上所做的配置更改将覆盖*管理外部访问*选项卡上的设置。

步骤

1. 选择*不可信客户端网络*。
2. 在设置新节点默认值部分中、指定在扩展操作步骤 中向网格添加新节点时的默认设置。
   - 可信(默认)：在扩展中添加节点时、其客户端网络是可信的。
   - * 不可信 * ：在扩展中添加节点时，其客户端网络不可信。

     您可以根据需要返回此选项卡来更改特定新节点的设置。

     > 此设置不会影响 StorageGRID 系统中的现有节点。

3. 使用以下选项选择仅允许在显式配置的负载平衡器端点或其他选定端口上进行客户端连接的节点：
   - 选择*在显示的节点上取消信任*，将表中显示的所有节点添加到不可信客户端网络列表中。
   - 选择*在显示的节点上信任*，从不可信客户端网络列表中删除表中显示的所有节点。
   - 使用每个端口旁边的切换功能将选定节点的客户端网络设置为可信或不可信。

     例如，您可以选择*Untrust on displayed N点*将所有节点添加到Untrusted Client Network列表中，然后使用单个节点旁边的切换将该单个节点添加到Trusted Client Network列表中。

> 使用表右侧的滚动条确保您已查看所有可用节点。使用搜索字段输入节点名称以查找任何节点的设置。您可以输入部分名称。例如，如果输入*GW*，则会显示名称中包含字符串"gw"的所有节点。

4. (可选)选择要在不可信客户端网络上打开的任何其他端口。这些端口可以提供对网格管理器和/或租户管理器的访问。

   例如、您可能希望使用此选项来确保可以在客户端网络上访问网格管理器进行维护。

   > 这些附加端口在客户端网络上处于打开状态、无论它们是否在管理外部访问选项卡中关闭。

5. 选择 * 保存 * 。

   此时将立即应用并实施新的防火墙设置。如果尚未配置负载平衡器端点，现有客户端连接可能会失败。