管理安全
StorageGRID software

NetApp
July 23, 2026

目录

管理安全

管理 StorageGRID 中的安全性

您可以从 Grid Manager 配置各种安全设置，以帮助保护您的 StorageGRID 系统。

管理加密

StorageGRID 提供多种加密数据的选项。您应该 "查看可用的加密方法" 以确定哪些选项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"可以保护 StorageGRID 数据，即使设备已从数据中心移除。设备卷加密后，除非节点可以与 KMS 通信，否则您无法访问设备上的任何数据。

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

管理代理服务器设置

如果使用的是 S3 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 "存储代理服务器"。如果使用 HTTPS 或 HTTP 发送 AutoSupport 软件包，则可以在管理节点和技术支持之间配置 "管理员代理服务器"。

控制防火墙

为了提高系统的安全性，您可以通过在 "外部防火墙" 上打开或关闭特定端口来控制对 StorageGRID 管理节点的访问。您还可以通过配置其 "内部防火墙" 来控制对每个节点的网络访问。您可以阻止对所有端口的访问，部署所需的端口除外。

查看 StorageGRID 加密方法

StorageGRID 提供多种加密数据的选项。您应查看可用的方法，以确定哪些方法符合您的数据保护要求。

下表提供了 StorageGRID 中可用加密方法的概要摘要。

加密选项	工作原理	适用于
Grid Manager 中的密钥管理服务器 (KMS)	您"配置密钥管理服务器"用于 StorageGRID 站点和 "为设备启用节点加密"。然后，设备节点连接到 KMS 以请求密钥加密密钥 (KEK)。此密钥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。设备上的所有数据都会受到保护，以防止物理丢失或从数据中心移除。 注意：仅存储节点和服务设备支持使用 KMS 管理加密密钥。
StorageGRID 设备安装程序中的驱动器加密页面	如果设备包含支持硬件加密的驱动器，您可以在安装过程中设置驱动器密码。当您设置驱动器密码时，任何人都无法从已从系统中删除的驱动器中恢复有效数据，除非他们知道密码。在开始安装之前，请转到 **Configure Hardware** > **Drive Encryption** ，以设置适用于节点中所有 StorageGRID 管理的自加密驱动器的驱动器密码。	包含自加密驱动器的设备。安全驱动器上的所有数据都会受到保护，以防止物理丢失或从数据中心移除。 驱动器加密不适用于 SANtricity 管理的驱动器。如果您有带有自加密驱动器和 SANtricity 控制器的存储设备，则可以在 SANtricity 中启用驱动器安全性。
SANtricity System Manager 中的驱动器安全性	如果您的 StorageGRID 设备启用了驱动器安全功能，您可以使用 "SANtricity System Manager"来创建和管理安全密钥。访问安全驱动器上的数据需要此密钥。	具有全磁盘加密 (FDE) 驱动器或自加密驱动器的存储设备。安全驱动器上的所有数据都受到保护，以防止物理丢失或从数据中心中移除。不能与某些存储设备或任何服务设备一起使用。
存储对象加密	您在 Grid Manager 中启用 "存储对象加密" 选项。启用后，任何未在存储桶级别或对象级别进行加密的新对象都将在摄入期间进行加密。	${post_edited_translations.segment} 现有的已存储对象不会被加密。对象元数据和其他敏感数据不会被加密。
${post_edited_translations.segment}	您发出 PutBucketEncryption 请求以启用存储桶加密。任何未在对象级进行加密的新对象都会在摄入期间进行加密。	${post_edited_translations.segment} 必须为存储桶指定加密。现有的存储桶对象不会被加密。对象元数据和其他敏感数据不会被加密。 "${post_edited_translations.segment}"

加密选项	工作原理	适用于
S3 对象服务器端加密 (SSE)	您发出 S3 请求以存储对象并包含 `x-amz-server-side-encryption`请求标头。	${post_edited_translations.segment} 必须为对象指定加密。对象元数据和其他敏感数据未加密。 StorageGRID 管理密钥。 "${post_edited_translations.segment}"
使用客户提供的密钥（SSE-C）对 S3 对象进行服务器端加密	${post_edited_translations.segment} • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	${post_edited_translations.segment} 必须为对象指定加密。对象元数据和其他敏感数据未加密。 ${post_edited_translations.segment} "${post_edited_translations.segment}"
${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment} 外部加密方法可对加密算法和密钥进行更严格的控制。可以与列出的其他方法相结合。
StorageGRID 外部的对象加密	在将对象数据和元数据摄入 StorageGRID 之前，您可以使用 StorageGRID 外部的加密方法对其进行加密。	仅对象数据和元数据（系统配置数据未加密）。 外部加密方法可对加密算法和密钥进行更严格的控制。可以与列出的其他方法相结合。 "Amazon Simple Storage Service - 用户指南：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，一次可以使用多个加密方法。例如：

- 您可以使用 KMS 保护设备节点，也可以使用 SANtricity System Manager 中的驱动器安全功能对同一设备中自加密驱动器上的数据进行"双重加密"。

- 您可以使用 KMS 来保护设备节点上的数据，也可以使用存储对象加密选项在接收所有对象时对其进行加密。

如果只有一小部分对象需要加密，请考虑在存储桶或单个对象级别控制加密。启用多级加密会带来额外的性能成本。

相关信息

"了解 FIPS 认证加密选项"

管理证书

管理 **StorageGRID** 中的安全证书

安全证书是用于在 StorageGRID 组件之间以及 StorageGRID 组件和外部系统之间创建安全、可信连接的小型数据文件。

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，向其客户端验证服务器的身份并为数据提供安全通信路径。服务器和客户端各有一个证书副本。
- *客户端证书*向服务器验证客户端或用户身份，提供比仅使用密码更安全的身份验证。客户端证书不加密数据。

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

StorageGRID 用作某些连接（如负载平衡器端点）的服务器，或用作其他连接（如 CloudMirror 复制服务）的客户端。

默认网格 **CA** 证书

StorageGRID 具有内置证书颁发机构 (CA)，可在系统安装期间生成内部网格 CA 证书。默认情况下，网格 CA 证书用于保护内部 StorageGRID 流量。外部证书颁发机构 (CA) 可以颁发完全符合组织信息安全策略的自定义证书。

在非生产环境中使用 Grid CA 证书。对于生产环境，请使用由外部证书颁发机构签名的自定义证书。支持无证书的非安全连接，但不推荐使用。

- ${post_edited_translations.segment}
- 所有自定义证书都必须符合 "${post_edited_translations.segment}"。
- ${post_edited_translations.segment}

> StorageGRID 还包含在所有网格上均相同的操作系统 CA 证书。在生产环境中，请确保指定由外部证书颁发机构签名的自定义证书，以代替操作系统 CA 证书。

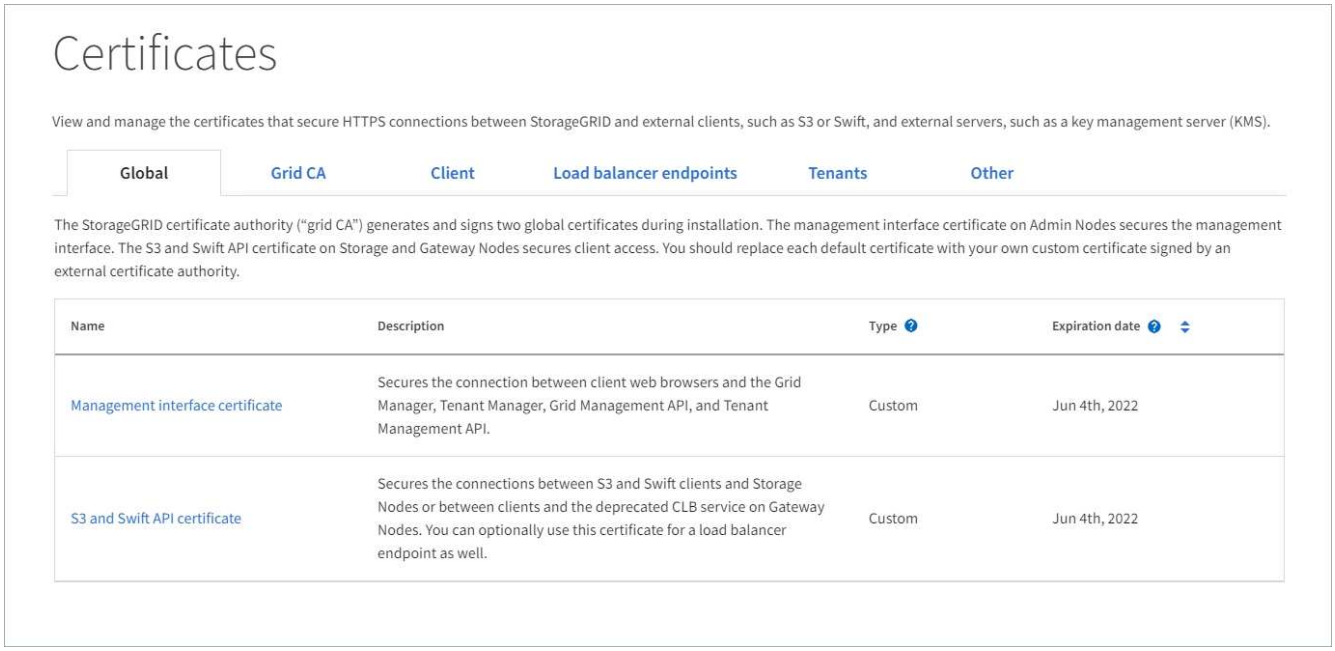
服务器和客户端证书类型的变体以多种方式实现。在配置系统之前，您应该准备好特定 StorageGRID 配置所需的所有证书。

${post_edited_translations.segment}

您可以在单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. 从 Grid Manager 中，选择 配置 > 安全 > 证书。



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。如果您拥有 "适当的权限"，则可以访问该选项卡。

   - 全局：保护网络浏览器和外部 API 客户端对 StorageGRID 的访问。
   - **Grid CA**：保护内部 StorageGRID 流量。
   - 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：保护 S3 客户端和 StorageGRID 负载平衡器之间的连接。
   - 租户：保护到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。

   下面将介绍每个选项卡，并链接到其他证书详细信息。

全局

全局证书可确保从 Web 浏览器和外部 S3 API 客户端安全地访问 StorageGRID。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]：保护客户端 Web 浏览器与 StorageGRID 管理界面的连接。
- <<${post_edited_translations.segment}>>：保护客户端 API 与存储节点、管理节点和网关节点的连接，S3 客户端应用程序使用这些节点上传和下载对象数据。

有关已安装的全局证书的信息包括：

- ${post_edited_translations.segment}
- 说明
- 类型：自定义或默认。+ 您应始终使用自定义证书来提高网格安全性。
- **Expiration date**：如果使用默认证书，则不会显示到期日期。

您可以轻松实现以下目标：

- 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：
  - "替换默认 StorageGRID 生成的管理接口证书" 用于 Grid Manager 和 Tenant Manager 连接。
  - "${post_edited_translations.segment}" 用于 Storage Node 和负载均衡器端点（可选）连接。
- "还原默认管理接口证书"。
- "还原默认 S3 API 证书"。
- "${post_edited_translations.segment}"。
- 复制或下载 "${post_edited_translations.segment}" 或 "${post_edited_translations.segment}"。

${post_edited_translations.segment}

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

证书信息包括证书过期日期和证书内容。

您可以 "复制或下载网格 CA 证书"，但无法进行修改。

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。

${post_edited_translations.segment}

您可以轻松实现以下目标：

- "${post_edited_translations.segment}"
- ${post_edited_translations.segment}
  - "${post_edited_translations.segment}"

- "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"${post_edited_translations.segment}"、"挂载"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*一次删除它们。

负载平衡器端点

负载平衡器端点证书 保护 S3 客户端与网关节点和管理节点上的 StorageGRID 负载均衡器服务之间的连接安全。

负载均衡器端点表为每个配置的负载均衡器端点包含一行，并指示该端点使用的是全局 S3 API 证书还是自定义负载均衡器端点证书。还会显示每个证书的过期日期。

对端点证书的更改可能需要长达 15 分钟才能应用于所有节点。

您可以轻松实现以下目标：

- "${post_edited_translations.segment}"，包括其证书详细信息。
- "为 FabricPool 指定负载均衡器端点证书。"
- "${post_edited_translations.segment}" 而不是生成新的负载均衡器端点证书。

租户

租户可以使用${post_edited_translations.segment}或平台服务端点证书来保护其与 StorageGRID 的连接。

${post_edited_translations.segment}

您可以轻松实现以下目标：

- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"

其他

StorageGRID 使用其他安全证书来满足特定用途。这些证书按其功能名称列出。其他安全证书包括：

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 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到期日期（如适用）。选择函数名称将打开一个浏览器选项卡，您可以在其中查看和编辑证书详细信息。

只有在具有 "适当的权限" 的情况下，才能查看和访问其他证书的信息。

您可以轻松实现以下目标：

- "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"
- "为外部 syslog 服务器使用证书"
- "轮换网格联合连接证书"
- "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

下面将介绍每种类型的安全证书，并提供指向实现说明的链接。

管理接口证书

证书类型	问题描述	导航位置	详细信息
服务器	验证客户端 Web 浏览器与 StorageGRID 管理界面之间的连接，允许用户在不出现安全警告的情况下访问 Grid Manager 和 Tenant Manager。 此证书还验证 Grid Management API 和 Tenant Management API 连接。 您可以使用在安装过程中创建的默认证书，也可以上传自定义证书。	配置 > 安全 > 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"

${post_edited_translations.segment}

证书类型	问题描述	导航位置	详细信息
服务器	验证到存储节点和负载均衡器端点的安全 S3 客户端连接（可选）。	配置 > 安全 > 证书，选择*全局*选项卡，然后选择 **S3 API certificate**	"配置 S3 API 证书"

网格**CA**证书

请参阅默认网格 CA 证书说明。

管理员客户端证书

证书类型	问题描述	导航位置	详细信息
客户端	安装在每个客户端上，允许 StorageGRID 对外部客户端访问进行身份验证。 • 允许授权外部客户端访问 StorageGRID Prometheus 数据库。 • 允许使用外部工具安全监控 StorageGRID。	配置 > 安全 > 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	问题描述	导航位置	详细信息
服务器	验证 S3 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。配置负载平衡器端点时，可以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。 您还可以使用全局 <<${post_edited_translations.segment}>> 证书的自定义版本来验证与负载平衡器服务的连接。如果全局证书用于验证负载平衡器连接，则无需为每个负载平衡器端点上传或生成单独的证书。 注意： 用于负载均衡器身份验证的证书是正常 StorageGRID 操作期间最常用的证书。	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	问题描述	导航位置	详细信息
服务器	验证从 StorageGRID 云存储池到外部存储位置（如 S3 Glacier 或 Microsoft Azure Blob 存储）的连接。每种云提供商类型需要不同的证书。	**ILM** > 存储池	"创建云存储池"

电子邮件警报通知证书

证书类型	问题描述	导航位置	详细信息
服务器和客户端	验证 SMTP 电子邮件服务器与用于警报通知的 StorageGRID 之间的连接。 • 如果与 SMTP 服务器的通信需要传输层安全性 (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。	告警 > 电子邮件设置	"为警报设置电子邮件通知"

外部 **syslog** 服务器证书

证书类型	问题描述	导航位置	详细信息
服务器	验证外部 syslog 服务器与 StorageGRID 之间的 TLS 或 RELP/TLS 连接，该服务器用于记录 StorageGRID 中的事件。 注意： TCP、RELP/TCP 和 UDP 连接到外部 syslog 服务器不需要外部 syslog 服务器证书。	配置 > 监控 > 审核和 **syslog** 服务器	"使用外部 syslog 服务器"

网格联盟连接证书

证书类型	问题描述	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	• "创建网格联盟连接" • "轮换连接证书"

身份联合证书

证书类型	问题描述	导航位置	详细信息
服务器	验证 StorageGRID 与外部身份提供程序（如 Active Directory、OpenLDAP 或 Oracle Directory Server）之间的连接。用于身份联合，允许管理员组和用户由外部系统管理。	配置 > 访问控制 > 身份联合	"${post_edited_translations.segment}"

密钥管理服务器**(KMS)**证书

证书类型	问题描述	导航位置	详细信息
服务器和客户端	验证 StorageGRID 与外部密钥管理服务器 (KMS) 之间的连接，该服务器为 StorageGRID 设备节点提供加密密钥。	配置 > 安全 > 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	问题描述	导航位置	详细信息
服务器	验证从 StorageGRID 平台服务到 S3 存储资源的连接。	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	问题描述	导航位置	详细信息
服务器	验证身份联合服务（如 Active Directory Federation Services (AD FS)）与用于单点登录 (SSO) 请求的 StorageGRID 之间的连接。	配置 > 访问控制 > 单点登录	"${post_edited_translations.segment}"

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. 您可以配置负载平衡器端点，并在 StorageGRID 中上传或生成服务器证书。
2. 您可以配置与负载均衡器端点的 S3 客户端连接，并将相同的证书上传到客户端。
3. 当客户端想要保存或检索数据时，它使用 HTTPS 连接到负载均衡器端点。

4. StorageGRID 使用包含公钥的服务器证书以及基于私钥的签名进行响应。
5. 客户端将服务器签名与其证书副本上的签名进行比较。如果签名匹配，则客户端使用相同的公钥启动会话。
6. 客户端将对象数据发送至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. 使用外部密钥管理服务器软件，可以将 StorageGRID 配置为 KMS 客户端，并获取 CA 签名的服务器证书、公共客户端证书和客户端证书的私钥。
2. 使用 Grid Manager，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私钥。
3. 当 StorageGRID 节点需要加密密钥时，它会向 KMS 服务器发出请求，其中包括来自证书的数据和基于私钥的签名。
4. KMS 服务器验证证书签名并决定它可以信任 StorageGRID。
5. ${post_edited_translations.segment}

StorageGRID 中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 密码需要 RSA 证书，而 ECDSA 密码需要 ECDSA 证书。请参阅"管理安全证书"。如果配置与服务器证书不兼容的自定义安全策略，则可以"暂时还原为默认安全策略"。

有关 StorageGRID 保护客户端连接的详细信息，请参见 "S3 客户端的安全性"。

在 StorageGRID 中配置管理界面证书

您可以将默认管理接口证书替换为单个自定义证书，该证书允许用户访问 Grid Manager 和 Tenant Manager，而不会遇到安全警告。您还可以还原为默认管理接口证书或生成新证书。

关于此任务

默认情况下，每个管理节点都会颁发由网格 CA 签名的证书。这些 CA 签名的证书可以替换为单个通用自定义管理接口证书和相应的私钥。

由于所有管理节点都使用单个自定义管理接口证书，因此如果客户端在连接到 Grid Manager 和 Tenant Manager 时需要验证主机名，则必须将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。

${post_edited_translations.segment}

为确保操作不会因服务器证书失效而中断，当此服务器证书即将过期时会触发*管理接口的服务器证书过期*警报。根据需要，您可以通过选择*配置* > 安全 > *证书*并在 Global 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。

如果使用域名而不是 IP 地址访问 Grid Manager 或 Tenant Manager，则浏览器将显示证书错误，如果发生以下任一情况，则无法选择绕过：

- 您的自定义管理界面证书已过期。
- 你 从自定义管理接口证书还原为默认服务器证书。

添加自定义管理接口证书

要添加自定义管理界面证书，您可以提供自己的证书或使用 Grid Manager 生成证书。

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择*管理界面证书*。
3. ${post_edited_translations.segment}
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：

   - ${post_edited_translations.segment}
   - 证书私钥：自定义服务器证书私钥文件 (`.key`）。

     EC 私钥必须为 224 位或更大。RSA 私钥必须为 2048 位或更大。

   - **CA bundle**：包含来自每个中间颁发证书颁发机构 (CA) 的证书的单个可选文件。该文件应包含以证书链顺序连接的每个 PEM 编码的 CA 证书文件。

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 捆绑包，则每个证书都会显示在自己的选项卡上。

   - 选择*下载证书*保存证书文件，或选择*下载 CA 捆绑包*保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

   例如： `storagegrid_certificate.pem`

   - ${post_edited_translations.segment}

d. 选择 * 保存 *。+ 自定义管理接口证书将用于随后与 Grid Manager、Tenant Manager、Grid Manager API 或 Tenant Manager API 的所有新连接。

生成证书

${post_edited_translations.segment}

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	问题描述
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 主题或标识名 (DN)。 如果在此字段中未输入任何值，则生成的证书将使用第一个域名或 IP 地址作为使用者通用名称 (CN)。

字段	问题描述
有效天数	创建后证书过期的天数。
添加密钥使用扩展	${post_edited_translations.segment} ${post_edited_translations.segment} ${post_edited_translations.segment}

c. 选择 **Generate**。

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 `.pem` 保存文件。

例如： `storagegrid_certificate.pem`

- 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。

e. 选择 * 保存 *。+ 自定义管理接口证书将用于随后与 Grid Manager、Tenant Manager、Grid Manager API 或 Tenant Manager API 的所有新连接。

5. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

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

${post_edited_translations.segment}

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择*管理界面证书*。
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，无法从系统中恢复。默认管理接口证书用于所有后续新客户端连接。

4. ${post_edited_translations.segment}

${post_edited_translations.segment}

如果需要严格的主机名验证，您可以使用脚本生成管理接口证书。

开始之前

- 您有 "特定访问权限"。
- 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. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 身份登录时，提示符将从 `$`更改为 `#`。
3. 使用新的自签名证书配置 StorageGRID。

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

   - 对于 `--domains`，请使用通配符来表示所有 Admin Node 的完全限定域名。例如，`*.ui.storagegrid.example.com` 使用 * 通配符来表示 `admin1.ui.storagegrid.example.com` 和 `admin2.ui.storagegrid.example.com`。
   - 将 以配置管理接口证书，该证书由 Grid Manager 和 Tenant Manager 使用。 `--type` 设置为 `management`
   - 默认情况下，生成的证书有效期为一年（365 天），并且必须在到期前重新创建。您可以使用 `--days`参数覆盖默认有效期。

     > 证书的有效期从运行 `make-certificate`时开始。您必须确保管理客户端与 StorageGRID 同步到相同的时间源；否则，客户端可能会拒绝证书。

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

     ${post_edited_translations.segment}
4. 选择并复制证书。

   在您的选择中包括 BEGIN 和 END 标记。
5. 从命令外壳中注销。 `$ exit`
6. 确认证书已配置：
   a. 访问 Grid Manager。

b. 选择*配置* > 安全 > 证书

c. 在*全局*选项卡上，选择*管理界面证书*。

7. 将管理客户端配置为使用您复制的公共证书。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供其他地方使用。

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择*管理界面证书*。
3. 选择 **Server** 或 **CA bundle** 选项卡，然后下载或复制证书。

${post_edited_translations.segment}

下载证书或 CA 捆绑包 `.pem`文件。如果您使用的是可选的 CA 捆绑包，则该捆绑包中的每个证书都会显示在各自的子选项卡上。

a. 选择*下载证书*或*下载 CA 捆绑包*。

如果要下载 CA 捆绑包，CA 捆绑包辅助选项卡中的所有证书都将作为单个文件下载。

b. 指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

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。如果使用可选的 CA 捆绑包，则捆绑包中的每个证书都显示在其自己的子选项卡上。

a. 选择 **Copy certificate PEM** 或 **Copy CA bundle PEM**。

如果要复制 CA 捆绑包，CA 捆绑包辅助选项卡中的所有证书将一起复制。

b. 将复制的证书粘贴到文本编辑器中。

c. 保存带有扩展名 `.pem`的文本文件。

例如： `storagegrid_certificate.pem`

在 StorageGRID 中配置 S3 API 证书

您可以替换或恢复用于 S3 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贵组织。

Swift 详细信息已从此版本的文档网站中删除。请参阅 "StorageGRID 11.8：配置 S3 和 Swift API 证书"。

关于此任务

默认情况下，每个存储节点都会颁发由网格 CA 签名的 X.509 服务器证书。这些 CA 签名的证书可以替换为单个通用自定义服务器证书和相应的私钥。

所有存储节点都使用单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，则必须将该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，您可能还需要在将用于访问系统的 S3 API 客户端中安装网格 CA 证书，具体取决于您使用的根证书颁发机构 (CA)。

为了确保操作不会因服务器证书失效而中断，当根服务器证书即将过期时，将触发 **S3 API** 全局服务器证书过期 警报。根据需要，您可以通过选择 配置 > 安全 > 证书，并在全局选项卡上查看 S3 API 证书的到期日期，来了解当前证书的到期时间。

您可以上传或生成自定义 S3 API 证书。

添加自定义 **S3 API** 证书

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择 **S3 API** 证书。
3. ${post_edited_translations.segment}
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：

   - ${post_edited_translations.segment}
   - 证书私钥：自定义服务器证书私钥文件 (`.key`）。

     EC 私钥必须为 224 位或更大。RSA 私钥必须为 2048 位或更大。

   - **CA bundle**：包含来自每个中间颁发证书颁发机构的证书的单个可选文件。文件应包含以证书链顺序连接的每个 PEM 编码的 CA 证书文件。

c. 选择证书详细信息以显示已上传的每个自定义 S3 API 证书的元数据和 PEM。如果您上传了可选的 CA 捆绑包，则每个证书都会显示在自己的选项卡上。

   - 选择*下载证书*保存证书文件，或选择*下载 CA 捆绑包*保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

   例如： `storagegrid_certificate.pem`

   - ${post_edited_translations.segment}

d. 选择 **Save**。

   自定义服务器证书用于后续新的 S3 客户端连接。

生成证书

${post_edited_translations.segment}

a. 选择*生成证书*。

b. 指定证书信息：

字段	问题描述
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 主题或标识名 (DN)。 如果在此字段中未输入任何值，则生成的证书将使用第一个域名或 IP 地址作为使用者通用名称 (CN)。
有效天数	创建后证书过期的天数。

字段	问题描述
添加密钥使用扩展	${post_edited_translations.segment} ${post_edited_translations.segment} ${post_edited_translations.segment}

c. 选择 **Generate**。

d. 选择*证书详细信息*以显示已生成的自定义 S3 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 `.pem` 保存文件。

例如： `storagegrid_certificate.pem`

- 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。

e. 选择 **Save**。

自定义服务器证书用于后续新的 S3 客户端连接。

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

${post_edited_translations.segment}

6. ${post_edited_translations.segment}
7. 添加自定义 S3 API 证书后，S3 API 证书页面会显示正在使用的自定义 S3 API 证书的详细信息。+ 您可以根据需要下载或复制证书 PEM。

还原默认 **S3 API** 证书

对于到存储节点的 S3 客户端连接，您可以还原为使用默认的 S3 API 证书。但是，不能对负载平衡器端点使用默认的 S3 API 证书。

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择 **S3 API** 证书。
3. 选择*使用默认证书*。

   还原全局 S3 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，无法从系统中恢复。默认 S3 API 证书将用于后续到存储节点的新 S3 客户端连接。

4. 选择 **OK** 确认警告并恢复默认 S3 API 证书。

   如果您具有根访问权限，并且自定义 S3 API 证书用于负载平衡器端点连接，则会显示无法再使用默认 S3 API 证书访问的负载平衡器端点列表。转到 "配置负载平衡器端点" 以编辑或删除受影响的端点。

5. ${post_edited_translations.segment}

下载或复制 **S3 API** 证书

您可以保存或复制 S3 API 证书内容以供其他地方使用。

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择 **S3 API** 证书。
3. 选择 **Server** 或 **CA bundle** 选项卡，然后下载或复制证书。

${post_edited_translations.segment}

下载证书或 CA 捆绑包 `.pem`文件。如果您使用的是可选的 CA 捆绑包，则该捆绑包中的每个证书都会显示在各自的子选项卡上。

a. 选择*下载证书*或*下载 CA 捆绑包*。

   如果要下载 CA 捆绑包，CA 捆绑包辅助选项卡中的所有证书都将作为单个文件下载。

b. 指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

   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。如果使用可选的 CA 捆绑包，则捆绑包中的每个证书都显示在其自己的子选项卡上。

a. 选择 **Copy certificate PEM** 或 **Copy CA bundle PEM**。

   如果要复制 CA 捆绑包，CA 捆绑包辅助选项卡中的所有证书将一起复制。

b. 将复制的证书粘贴到文本编辑器中。

c. 保存带有扩展名 `.pem`的文本文件。

   例如： `storagegrid_certificate.pem`

相关信息

- "使用 S3 REST API"
- "配置 S3 端点域名"

复制 **StorageGRID** 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，此证书不会更改。

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 "特定访问权限"。

关于此任务

如果已配置自定义服务器证书，则客户端应用程序应使用自定义服务器证书验证服务器。它们不应从 StorageGRID 系统中复制 CA 证书。

步骤

1. 选择 **Configuration** > **Security** > **Certificates**，然后选择 **Grid 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 `.pem` 保存文件。

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 **Copy certificate PEM**。

b. 将复制的证书粘贴到文本编辑器中。

c. 保存带有扩展名 `.pem`的文本文件。

例如： `storagegrid_certificate.pem`

为 FabricPool 配置 StorageGRID 证书

对于执行严格主机名验证且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，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

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

关于此任务

创建负载平衡器端点时，可以生成自签名服务器证书或上载由已知证书颁发机构 (CA) 签名的证书。在生产环境中，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，因为它们能够更好地防御中间人攻击。

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程序，请参见 "为 FabricPool 配置 StorageGRID"。

步骤

1. 可选操作：配置供 FabricPool 使用的高可用性 (HA) 组。
2. 创建供 FabricPool 使用的 S3 负载平衡器端点。

   当您创建 HTTPS 负载均衡器端点时，系统会提示您上传服务器证书、证书私钥和可选的 CA 捆绑包。

3. 在 ONTAP 中将 StorageGRID 附加为云层。

   指定上传的 CA 证书中使用的负载均衡器端点端口和完全限定域名。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 证书由根 CA 直接颁发，则必须提供根 CA 证书。

在 **StorageGRID** 中配置客户端证书

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

如果需要使用外部监控工具访问 StorageGRID，您必须使用 Grid Manager 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"。

为了确保操作不会因服务器证书失效而中断，当此服务器证书即将过期时，会触发*证书页面上配置的客户端证书过期*警报。根据需要，您可以通过选择*配置* > 安全 > *证书*并在客户端选项卡上查看客户端证书的到期日期来了解当前证书的过期时间。

如果使用密钥管理服务器 (KMS) 保护特殊配置的设备节点上的数据，请参阅有关 "上传 KMS 客户端证书" 的具体信息。

开始之前

- ${post_edited_translations.segment}
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 要配置客户端证书：
  - 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，则具有用于配置管理接口证书的 CA、客户端证书和私钥。
  - 要上传自己的证书，证书的私钥需在本地计算机上可用。
  - 私钥必须在创建时保存或记录。如果您没有原始私钥，则必须创建一个新私钥。
- 要编辑客户端证书：
  - 您拥有管理节点的 IP 地址或域名。
  - 要上传自己的证书或新证书，私钥、客户端证书和 CA（如果使用）需在本地计算机上可用。

添加客户端证书

要添加客户端证书，请使用以下过程之一：

- [管理接口证书已配置]
- CA 颁发的客户端证书
- 从 Grid Manager 生成的证书

管理接口证书已配置

如果已使用客户提供的 CA、客户端证书和私钥配置管理接口证书，请使用此过程添加客户端证书。

步骤

1. 在 Grid Manager 中，选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。
2. 选择 **Add**。
3. 请输入证书名称。
4. 要使用外部监控工具访问 Prometheus 指标，请选择 **Allow prometheus**。
5. 选择 **Continue**。
6. 对于*附加证书*步骤，上传管理接口证书。
   a. 选择*上传证书*。
   b. 选择*Browse*，然后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 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。
   c. 选择 **Create** 将证书保存到 Grid Manager 中。

      新证书将显示在"客户端"选项卡上。
7. 配置外部监控工具，例如 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私钥的 Prometheus 添加客户端证书，请使用此过程添加管理员客户端证书。

步骤

1. 执行"配置管理接口证书"中的步骤。
2. 在 Grid Manager 中，选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。
3. 选择 **Add**。
4. 请输入证书名称。
5. 要使用外部监控工具访问 Prometheus 指标，请选择 **Allow prometheus**。
6. 选择 **Continue**。
7. 对于*附加证书*步骤，上传客户端证书、私钥和 CA 捆绑包文件：

a. 选择*上传证书*。

b. 选择*Browse*，然后选择客户端证书、私钥和 CA 捆绑包文件(`.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 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。

c. 选择 **Create** 将证书保存到 Grid Manager 中。

新证书显示在"客户端"选项卡上。

8. 配置外部监控工具，例如 Grafana。

从 **Grid Manager** 生成的证书

如果未配置管理接口证书，并且您计划为使用 Grid Manager 中生成证书功能的 Prometheus 添加客户端证书，请使用此过程添加管理员客户端证书。

步骤

1. 在 Grid Manager 中，选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。
2. 选择 **Add**。
3. 请输入证书名称。
4. 要使用外部监控工具访问 Prometheus 指标，请选择 **Allow prometheus**。
5. 选择 **Continue**。
6. 对于*附加证书*步骤，选择*生成证书*。
7. 指定证书信息：

- 主题（可选）：证书所有者的 X.509 主题或标识名（DN）。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

8. 选择 **Generate**。
9. ${post_edited_translations.segment}

关闭对话框后，您将无法查看证书私钥。请将密钥复制或下载到安全位置。

- 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。
- 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 `.pem` 保存文件。

例如： `storagegrid_certificate.pem`

- 选择*复制私钥*以复制证书私钥，以便粘贴到其他位置。
- 选择*下载专用密钥*将专用密钥另存为文件。

  ${post_edited_translations.segment}

10. 选择 **Create** 将证书保存到 Grid Manager 中。

    新证书将显示在"客户端"选项卡上。

11. ${post_edited_translations.segment}
12. ${post_edited_translations.segment}
13. ${post_edited_translations.segment}
14. 从 ${post_edited_translations.segment} 步骤中上传 certificate.pem 和 private_key.pem 文件。无需上传 CA 捆绑包。
    a. ${post_edited_translations.segment}
    b. 上传每个证书文件 (`.pem`)。
    c. 选择*保存*将证书保存到 Grid Manager 中。

       新证书将显示在管理接口证书页面上。

15. 配置外部监控工具，例如 Grafana。

配置外部监控工具

步骤

1. ${post_edited_translations.segment}
   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. ${post_edited_translations.segment}
   d. 在 TLS/SSL 身份验证详细信息下，复制并粘贴：
      - 管理接口 CA 证书至 **CA Cert**
      - ${post_edited_translations.segment}
      - ${post_edited_translations.segment}
   e. **ServerName**：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 "监控 StorageGRID 的说明"。

${post_edited_translations.segment}

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 访问权限，或者在当前证书过期时上传新证书。

步骤

1. 选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。

   证书过期日期和 Prometheus 访问权限列在表中。如果证书即将过期或已过期，表中会显示一条消息，并触发警报。

2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. 请输入证书名称。
5. 要使用外部监控工具访问 Prometheus 指标，请选择 **Allow prometheus**。
6. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

附加新客户端证书

您可以在当前证书过期时上传新证书。

步骤

1. 选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。

   证书过期日期和 Prometheus 访问权限列在表中。如果证书即将过期或已过期，表中会显示一条消息，并触发警报。

2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

上传证书

复制证书文本以粘贴到其他位置。

a. ${post_edited_translations.segment}

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 `.pem` 保存文件。

   例如： `storagegrid_certificate.pem`

   - 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。

c. 选择 **Create** 将证书保存到 Grid Manager 中。

   ${post_edited_translations.segment}

生成证书

生成证书文本以粘贴到其他位置。

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 主题或标识名（DN）。
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

     ${post_edited_translations.segment}

c. 选择 **Generate**。

d. 选择*客户端证书详细信息*以显示证书元数据和证书 PEM。

   关闭对话框后，您将无法查看证书私钥。请将密钥复制或下载到安全位置。

   - 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。
   - 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 `.pem` 保存文件。

   例如： `storagegrid_certificate.pem`

   - 选择*复制私钥*以复制证书私钥，以便粘贴到其他位置。

- 选择*下载专用密钥*将专用密钥另存为文件。

  ${post_edited_translations.segment}

e. 选择 **Create** 将证书保存到 Grid Manager 中。

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地方使用。

步骤

1. 选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 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 `.pem` 保存文件。

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 **Copy certificate PEM**。
b. 将复制的证书粘贴到文本编辑器中。
c. 保存带有扩展名 `.pem`的文本文件。

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，则可以将其删除。

步骤

1. 选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

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新的客户端证书才能访问 StorageGRID Prometheus 数据库。

配置安全设置

在 **StorageGRID** 中管理 **TLS** 和 **SSH** 策略

TLS 和 SSH 策略确定使用哪些协议和密码与客户端应用程序建立安全的 TLS 连接，以及与内部 StorageGRID 服务建立安全的 SSH 连接。

安全策略控制 TLS 和 SSH 如何加密传输中的数据。通常，使用 Modern compatibility（默认）策略，除非您的系统需要符合 Common Criteria 标准，或者您需要使用其他密码。

某些 StorageGRID 服务尚未更新为使用这些策略中的密码。

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 "root 访问权限"。

选择安全策略

步骤

1. 选择*配置* > 安全 > 安全设置。

   TLS and SSH policies 选项卡显示可用策略。当前有效的策略在策略图块上以绿色复选标记标注。

2. 查看选项卡以了解可用的策略。

现代兼容性（默认）

如果您需要强加密且没有特殊要求，请使用默认策略。此策略与大多数 TLS 和 SSH 客户端兼容。

旧版兼容性

如果您需要旧版客户端的其他兼容性选项，请使用旧版兼容性策略。此策略中的其他选项可能会使其安全性低于新式兼容性策略。

通用标准

如果您需要Common Criteria认证，请使用Common Criteria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 (NCSM) 3.0.8 或 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模块进行与负载均衡器端点、租户管理器和网格管理器的外部客户端连接，请使用 FIPS 严格策略。使用此策略可能会降低性能。

NCSM 3.0.8 和 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模块用于以下操作：

- NCSM
  - 以下服务之间的 TLS 连接：ADC、AMS、CMN、DDS、LDR、SSM、NMS、mgmt-api、nginx、nginx-gw 和 cache-svc
  - 客户端与 nginx-gw 服务（负载均衡器端点）之间的 TLS 连接
  - 客户端与 LDR 服务之间的 TLS 连接
  - SSE-S3、SSE-C 和存储对象加密设置的对象内容加密
  - SSH 连接

  有关详细信息，请参见 NIST Cryptographic Algorithm Validation Program "证书 #4838"。
- NetApp StorageGRID 内核加密 API 模块

  NetApp StorageGRID 内核加密 API 模块仅存在于 VM 和 StorageGRID 设备平台上。
  - 熵收集
  - 节点加密

  有关详细信息，请参见 NIST Cryptographic Algorithm Validation Program "证书 #A6242 至 #A6257"和 "熵证书 #E223"。

注意：选择此策略后，"执行滚动重启"所有节点都要激活 NCSM。使用 维护 > 滚动重启 来启动和监控重启。

自定义

如果需要应用自己的密码，请创建自定义策略。

或者，如果您的 StorageGRID 具有 FIPS 140 加密要求，则启用 FIPS 模式功能以使用 NCSM 3.0.8 和 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模块：

a. 将 `fipsMode`参数设置为 `true`。

b. 出现提示时，"执行滚动重启"让所有节点激活加密模块。使用 **Maintenance** > **Rolling reboot** 启动和监控重启。

c. 选择 **Support** > **Diagnostics** 以查看活动的 FIPS 模块版本。

3. 要查看每个策略的密码、协议和算法的详细信息，请选择 **View details**。
4. 要更改当前策略，请选择 **Use policy**。

   策略磁贴上的*当前策略*旁边会显示一个绿色复选标记。

创建自定义安全策略

如果需要应用自己的密码，则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图块中，选择*查看详细信息*。
2. 选择*复制到剪贴板*，然后选择*取消*。

3. 在*自定义策略*图块中，选择*配置和使用*。
4. 粘贴您复制的 JSON 并进行所需的更改。
5. 选择*使用策略*。

   自定义策略磁贴上的*当前策略*旁边会显示一个绿色复选标记。

6. （可选）选择*编辑配置*以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，且配置的 TLS 策略与 "已配置的服务器证书" 不兼容，则可能无法登录到 Grid Manager。

您可以暂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 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 身份登录时，提示符将从 `$`更改为 `#`。

2. 运行以下命令：

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

3. 在 Web 浏览器中，访问同一管理节点上的 Grid Manager。
4. 请按照 选择安全策略 中的步骤重新配置策略。

配置 StorageGRID 网络和对象安全性

您可以配置网络和对象安全性，以加密存储的对象，防止某些 S3 请求，或允许客户端连接到 Storage Nodes 时使用 HTTP 而不是 HTTPS。

存储对象加密

存储对象加密可对通过 S3 摄取的所有对象数据进行加密。默认情况下，存储的对象不会加密，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，所有新摄取的对象都将被加密，但不会对现有存储的对象进行任何更改。如果禁用加密，当前已加密的对象将保持加密状态，但新摄取的对象将不会被加密。

存储对象加密设置仅适用于未通过存储桶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"。

防止客户端修改

防止客户端修改是系统范围内的设置。当选择*防止客户端修改*选项时，以下请求将被拒绝。

S3 REST API

- DeleteBucket 请求
- 任何修改现有对象数据、用户定义元数据或 S3 对象标记的请求

为存储节点连接启用 HTTP

默认情况下，客户端应用程序使用 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 客户端需要直接与存储节点建立 HTTP 连接时，才对存储节点连接使用 HTTP。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，不需要使用此选项（因为您可以"配置每个负载均衡器端点"使用

HTTP 或 HTTPS）。

请参阅"摘要：客户端连接的 IP 地址和端口"以了解 S3 客户端在使用 HTTP 或 HTTPS 连接到 Storage Nodes 时使用的端口。

选择选项

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- ${post_edited_translations.segment}

步骤

1. 选择*配置* > 安全 > 安全设置。
2. 选择*网络和对象*选项卡。
3. 对于存储对象加密，如果您不希望对存储对象进行加密，请使用 **None**（默认）设置，或选择 **AES-128** 或 **AES-256** 对存储对象进行加密。
4. 如果要阻止 S3 客户端发出特定请求，可以选择*防止客户端修改*。

   如果更改此设置，应用新设置大约需要一分钟。配置的值将被缓存以提升性能和扩展能力。

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

   ${post_edited_translations.segment}

6. 选择 **Save**。

更改 StorageGRID 接口安全设置

通过界面安全设置，可以控制用户在超过指定时间内处于非活动状态时是否自动注销，以及 API 错误响应中是否包含堆栈跟踪。

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 "root 访问权限"。

关于此任务

*安全设置*页面包括*浏览器非活动超时*和*管理 API 堆栈跟踪*设置。

浏览器非活动超时

指示在用户注销之前，用户的浏览器可以处于非活动状态的时间长度。默认时间为 15 分钟。

浏览器非活动超时也受以下因素控制：

- 一个单独的、不可配置的 StorageGRID 计时器，用于系统安全。每个用户的身份验证令牌在用户登录后 16 小时过期。当用户的身份验证过期时，即使浏览器非活动超时已禁用或尚未达到浏览器超时的值，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，假设已为 StorageGRID 启用单点登录 (SSO)。

  如果启用了 SSO 并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。请参阅 "SSO 的工作原理"。

管理 **API** 堆栈跟踪

控制是否在 Grid Manager 和 Tenant Manager API 错误响应中返回堆栈跟踪。

此选项默认处于禁用状态，但您可能希望为测试环境启用此功能。一般来说，您应在生产环境中禁用堆栈跟踪，以避免在发生 API 错误时泄露内部软件详细信息。

步骤

1. 选择*配置* > 安全 > 安全设置。
2. 选择*界面*选项卡。
3. 要更改浏览器非活动超时的设置，请执行以下操作：
   a. 展开折叠面板。
   b. 要更改超时时间段，请指定一个介于 60 秒和 7 天之间的值。默认超时时间为 15 分钟。
   c. 要禁用此功能，请取消选中该复选框。
   d. 选择 **Save**。

      此新设置不会影响当前登录的用户。要使新的超时设置生效，用户必须重新登录或刷新浏览器。
4. 要更改 Management API 堆栈跟踪的设置，请执行以下操作：
   a. 展开折叠面板。
   b. 选中复选框以在 Grid Manager 和 Tenant Manager API 错误响应中返回堆栈跟踪。

      在生产环境中禁用堆栈跟踪，以避免在发生 API 错误时泄露内部软件详细信息。

   c. 选择 **Save**。

在 StorageGRID 中管理外部 SSH 访问

通过阻止或允许外部访问，管理进入网格的入站流量的 SSH 访问。管理 SSH 外部访问不会对网格中节点之间的流量产生影响。

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 "root 访问权限"。

关于此任务

为增强系统安全性，默认情况下会阻止外部 SSH 访问。如果需要执行需要入站 SSH 访问的任务，例如故障排除，请暂时允许外部访问。完成任务后，请阻止外部访问。

步骤

1. 选择*配置* > 安全 > 安全设置。
2. 选择 **Block SSH** 选项卡。
3. 使用*阻止入站SSH访问*选项来管理外部SSH访问：
   a. 选中复选框以阻止访问（默认）。
   b. 取消选中该复选框以允许访问。

   需要访问服务笔记本电脑和所有其他网格节点之间的端口 22。完成维护任务后，请删除端口 22 的访问权限。

4. 选择 **Save**。

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)"。

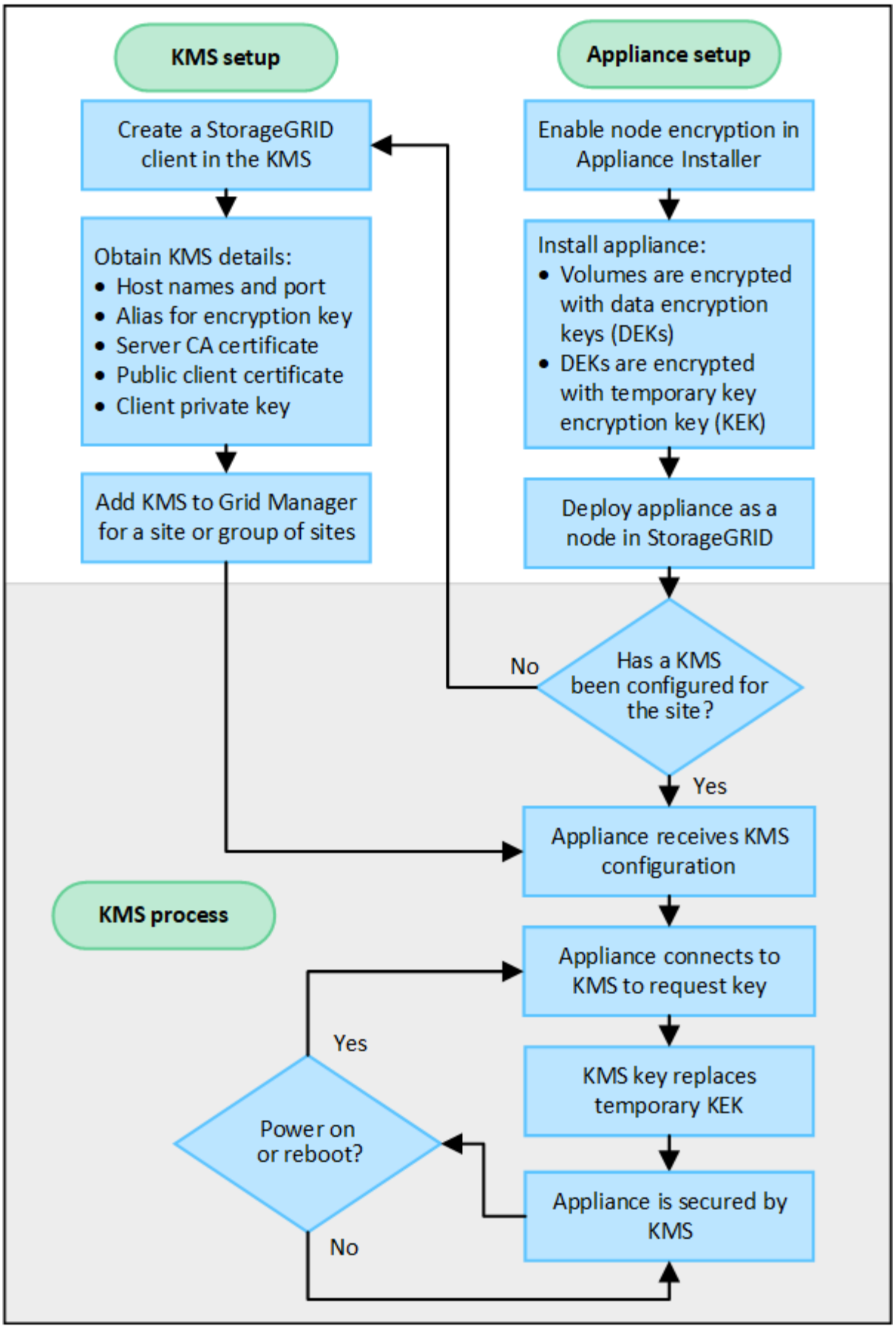
您可以使用一个或多个密钥管理服务器来管理在安装期间启用了 节点加密 设置的任何 StorageGRID 设备节点的节点加密密钥。将密钥管理服务器与这些设备节点结合使用，即使设备从数据中心移出，也可以保护您的数据。在对设备卷进行加密后，除非节点可以与 KMS 进行通信，否则您将无法访问该设备上的任何数据。

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。

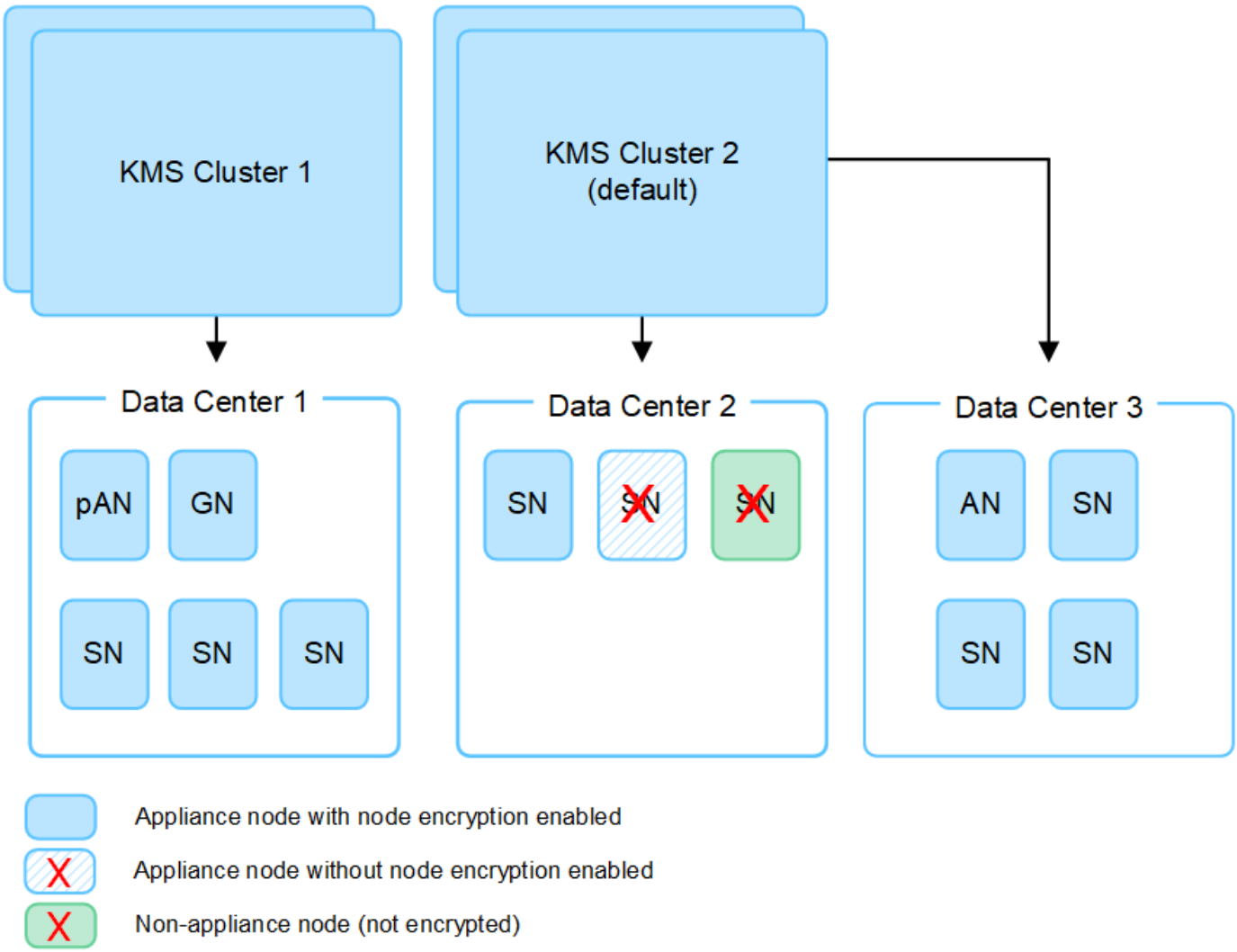
我需要多少密钥管理服务器?

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。

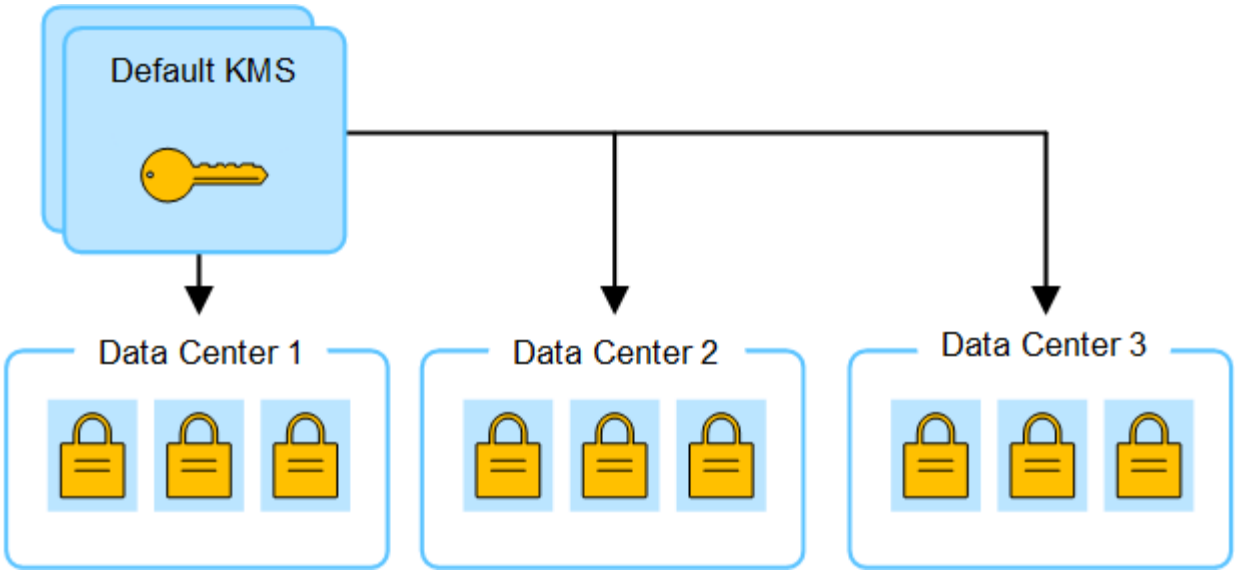
更改 **StorageGRID** 站点 **KMS** 的注意事项

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。

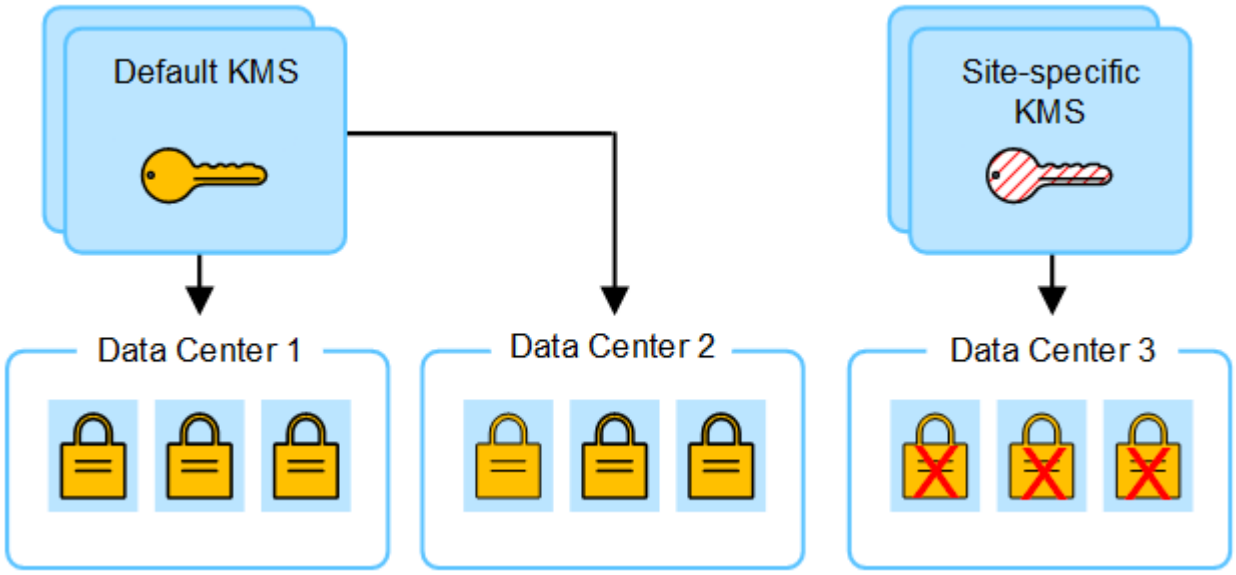
如果您更改了用于某个站点的 KMS，则必须确保可以使用存储在新 KMS 上的密钥对该站点上先前加密的设备节点进行解密。在某些情况下，您可能需要将当前版本的加密密钥从原始 KMS 复制到新 KMS。您必须确保 KMS 具有正确的密钥，以便对该站点上加密的设备节点进行解密。

例如：

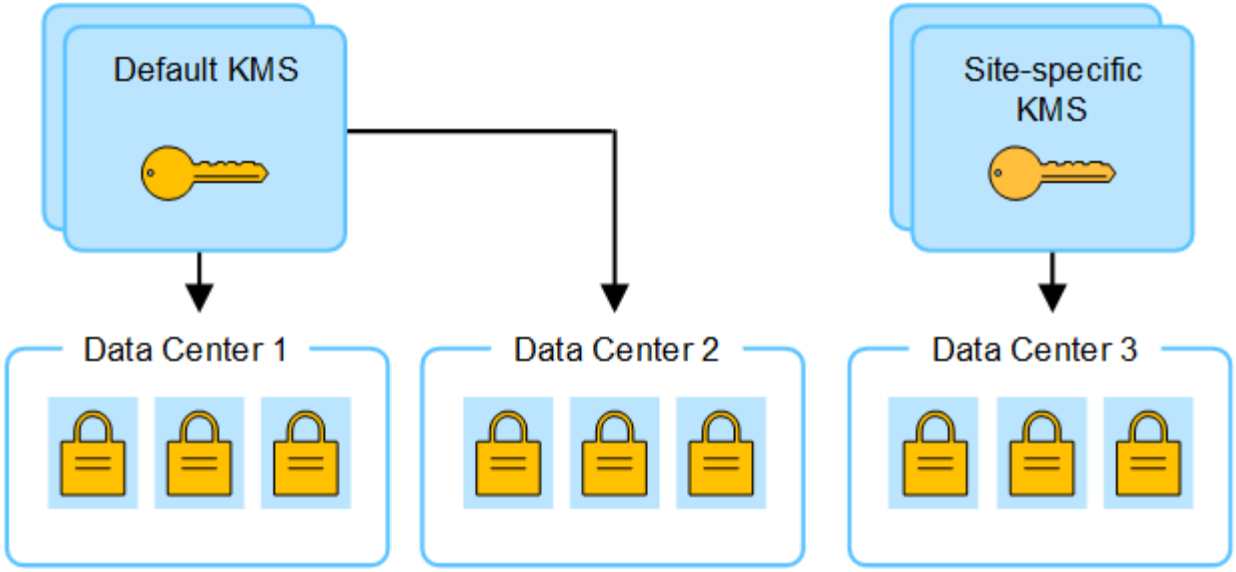
1. ${post_edited_translations.segment}
2. 保存 KMS 时，所有启用了 节点加密 设置的设备节点都会连接到 KMS 并请求加密密钥。此密钥用于加密所有站点上的设备节点。必须使用同一密钥对这些设备进行解密。



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。 "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} 2. ${post_edited_translations.segment} "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 Grid Manager，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)"

${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。 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。 • 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 **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。 ${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} 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。 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）。*

字段	问题描述
主机名称	KMS 的完全限定域名或 IP 地址。 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。 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。
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	问题描述
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。 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。 *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。 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。 *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} 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。

管理代理服务器设置

配置 StorageGRID 存储代理

如果使用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，以允许平台服务消息发送到外部端点，例如 Internet 上的端点。

> 配置的存储代理设置不适用于 Kafka 平台服务端点。

开始之前

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

关于此任务

您可以配置单个存储代理的设置。

步骤

1. 选择*配置* > 安全 > 代理设置。
2. 在*存储*选项卡上，选中*启用存储代理*复选框。
3. 选择存储代理的协议。
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。

   将此字段留空以使用协议的默认端口：HTTP 为 80，SOCKS5 为 1080。

6. 选择 **Save**。

   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。

   > 代理服务器更改最多可能需要 10 分钟才能生效。

7. 请检查代理服务器的设置，以确保来自 StorageGRID 的平台服务相关消息不会被阻止。
8. 如果需要禁用存储代理，请清除复选框，然后选择*保存*。

在 StorageGRID 中配置管理代理设置

如果使用 HTTP 或 HTTPS 发送 AutoSupport 软件包，则可以在管理节点和技术支持之间配置非透明代理服务器（AutoSupport）。

有关 AutoSupport 的详细信息，请参见 "配置 AutoSupport"。

开始之前

- 您有 "特定访问权限"。

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。

关于此任务

您可以配置单个管理代理的设置。

步骤

1. 选择*配置* > 安全 > 代理设置。

   此时将显示"代理服务器设置"页面。默认情况下，在选项卡菜单中选择"存储"。

2. 选择 **Admin** 选项卡。
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. 请输入用于连接到代理服务器的端口。
6. （可选）输入代理服务器的用户名和密码。

   如果您的代理服务器不需要用户名或密码，请将这些字段留空。

7. 选择以下选项之一：

   - 如果要保护与管理代理的连接，请选择*验证代理证书*。上传 CA 捆绑包以验证管理代理服务器提供的 SSL 证书的真实性。

     AutoSupport on Demand、通过 StorageGRID 的 E-Series AutoSupport 以及 StorageGRID 升级页面上的更新路径确定，在验证代理证书后将无法正常工作。

   上传 CA 捆绑包后，将显示其元数据。

   - 如果在与管理员代理服务器通信时不想验证证书，请选择*Do not verify proxy certificate*。

8. 选择 **Save**。

   保存管理员代理后，将配置管理节点与技术支持之间的代理服务器。

   代理服务器更改最多可能需要 10 分钟才能生效。

9. 如果您需要禁用管理员代理，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 **StorageGRID** 访问

您可以在外部防火墙上打开或关闭特定端口。

您可以通过在外部防火墙上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，除了使用其他方法来控制系统访问之外，您可能还希望阻止租户在防火墙处连接到 Grid Manager。

如果要配置 StorageGRID 内部防火墙，请参见 "配置内部防火墙"。

端口	问题描述	如果端口打开.....
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 Grid Manager、Grid Management API、Tenant Manager 和 Tenant Management API。 注意： 端口 443 也用于一些内部流量。
8443	管理节点上的受限 Grid Manager 端口	• 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 Tenant Manager 或 Tenant Management API。 • 对内部内容的请求将被拒绝。
9443	管理节点上的受限租户管理器端口	• 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 Grid Manager 或网格管理 API。 • 对内部内容的请求将被拒绝。

单点登录 (SSO) 在受限 Grid Manager 或 Tenant Manager 端口上不可用。如果希望用户使用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 StorageGRID 中的内部防火墙控制

StorageGRID 在每个节点上包含一个内部防火墙，通过控制对节点的网络访问来增强网格的安全性。使用防火墙可阻止所有端口上的网络访问，特定网格部署所必需的端口除外。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可自定义网格所需的访问权限。

- 特权地址列表：使用此选项卡可允许选定访问已关闭的端口。您可以添加 CIDR 表示法的 IP 地址或子网，这些地址或子网可以访问使用"管理外部访问"选项卡关闭的端口。
- 管理外部访问：使用此选项卡可关闭默认打开的端口，或重新打开先前已关闭的端口。
- 不受信任的客户端网络：使用此选项卡可指定节点是否信任来自客户端网络的入站流量。

  此选项卡上的设置将覆盖"管理外部访问"选项卡中的设置。

  - 具有不受信任客户端网络的节点将仅接受在该节点上配置的负载均衡器端点端口上的连接（全局、节点接口和节点类型绑定端点）。

- 无论 Manage external networks 选项卡上的设置如何，在不受信任的客户端网络上，负载均衡器端点端口_是唯一开放的端口_。
- 受信任时，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。

> 您在一个选项卡上进行的设置可能会影响您在另一个选项卡上进行的访问更改。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，请参见 "控制外部防火墙的访问"。

${post_edited_translations.segment}

“特权地址列表”选项卡使您能够注册一个或多个被授予访问已关闭网格端口权限的 IP 地址。“管理外部访问”选项卡使您能够关闭对选定外部端口或所有打开的外部端口的外部访问（外部端口是默认情况下非网格节点可访问的端口）。这两个选项卡通常可以结合使用，以自定义允许网格访问的精确网络访问权限。

> ${post_edited_translations.segment}

示例 **1**：使用跳板机执行维护任务

假设您要使用跳板机（经过安全加固的主机）进行网络管理。您可以使用以下常规步骤：

1. ${post_edited_translations.segment}
2. 使用"管理外部访问"选项卡可阻止所有端口。

> 在阻止端口 443 和 8443 之前，请先添加特权 IP 地址。当前连接到被阻止端口的任何用户（包括您）都将失去对 Grid Manager 的访问权限，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将对除跳转主机之外的所有主机被阻止。然后，您可以使用跳转主机更安全地对网格执行维护任务。

示例 **2**：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。您可以使用以下常规步骤：

1. 使用"特权地址列表"选项卡，仅向需要访问该服务的主机授予访问权限。
2. 使用"管理外部访问"选项卡可阻止所有端口。

> 在阻止访问分配给 Grid Manager 和 Tenant Manager 的任何端口（预设端口为 443 和 8443）之前，请先添加特权 IP 地址。当前连接到被阻止端口的任何用户（包括您）都将失去对 Grid Manager 的访问权限，除非其 IP 地址已添加到特权地址列表中。

保存配置后，特权地址列表中的主机可以使用该敏感端口及其上的服务。无论请求来自哪个接口，所有其他主机均被拒绝访问该服务。

示例 **3**：禁用对未使用服务的访问

在网络级别，您可以禁用某些不打算使用的服务。例如，要阻止 HTTP S3 客户端流量，您可以使用"管理外部访问"选项卡上的切换来阻止端口 18084。

不受信任的客户端网络选项卡

如果使用客户端网络，则可以通过仅接受显式配置的端点上的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为_trusted_。也就是说，默认情况下，StorageGRID 信任所有 "可用外部端口" 上每个网格节点的入站连接。

您可以通过指定每个节点上的客户端网络_不可信_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受信任，则该节点仅接受明确配置为负载平衡器端点的端口上的入站连接。请参阅"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 请求之外的所有入站流量。您将执行以下一般步骤：

1. 在"负载平衡器端点"页面中，通过端口 443 上的 HTTPS 为 S3 配置负载平衡器端点。
2. 在防火墙控制页面中，选择"不受信任"以指定网关节点上的客户端网络不受信任。

保存配置后，除端口 443 上的 HTTPS S3 请求和 ICMP echo (ping) 请求外，网关节点客户端网络上的所有入站流量都将被丢弃。

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该存储节点的任何入站连接。您将执行以下常规步骤：

- 在防火墙控制页面的"不受信任的客户端网络"选项卡中，指示存储节点上的客户端网络不受信任。

保存配置后，存储节点不再接受客户端网络上的任何传入流量，但它继续允许向已配置的平台服务目标发出出站请求。

示例 **3**：将对 **Grid Manager** 的访问限制为子网

假设您只想允许 Grid Manager 访问特定子网。您将执行以下步骤：

1. 将管理节点的客户端网络附加到子网。
2. 使用"不受信任的客户端网络"选项卡将客户端网络配置为不受信任。
3. 在创建管理接口负载均衡器端点时，输入端口并选择该端口将访问的管理接口。
4. 对于不受信任的客户端网络，选择*是*。
5. 使用管理外部访问选项卡可阻止所有外部端口（为该子网外的主机设置或不设置特权 IP 地址）。

保存配置后，只有您指定的子网上的主机才能访问 Grid Manager。所有其他主机均被屏蔽。

配置 StorageGRID 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

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。
- 您已查看 "管理防火墙控件" 和 "网络连接准则" 中的信息。
- 如果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，如果未配置负载均衡器端点，则现有客户端连接可能会失败。

关于此任务

StorageGRID 在每个节点上包含一个内部防火墙，使您能够打开或关闭网格节点上的某些端口。您可以使用防火墙控制选项卡打开或关闭默认情况下在网格网络、管理网络和客户端网络上打开的端口。您还可以创建可访问已关闭网格端口的特权 IP 地址列表。如果使用客户端网络，则可以指定节点是否信任来自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权限。

将对网格外部 IP 地址开放的端口数量限制为仅绝对必要的端口，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，以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 "管理防火墙控件"。

有关外部防火墙和网络安全的详细信息，请参见 "控制外部防火墙的访问"。

访问防火墙控件

步骤

1. 选择*配置* > 安全 > 防火墙控制。

   本页上的三个选项卡如 "管理防火墙控件" 中所述。

2. 选择任意选项卡以配置防火墙控件。

   您可以按任何顺序使用这些选项卡。您在一个选项卡上设置的配置不限制您可以在其他选项卡上执行的操作；但是，您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，特权 IP 地址和子网没有内部网格访问权限。此外，即使在"管理外部访问"选项卡中被阻止，也可以访问在"特权地址列表"选项卡中打开的负载均衡器端点和其他端口。

> "特权地址列表"选项卡上的设置无法覆盖"不受信任的客户端网络"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 **Add another IP address or subnet in CIDR notation** 以添加其他特权客户端。

   将尽可能少的地址添加到特权列表。

3. 可选，选择*允许特权 IP 地址访问 StorageGRID 内部端口*。请参阅 "StorageGRID 内部端口"。

   此选项将删除对内部服务的一些保护。如有可能，请将其停用。

4. 选择 **Save**。

管理外部访问

在"管理外部访问"选项卡中关闭端口时，除非您将 IP 地址添加到特权地址列表，否则任何非网格 IP 地址都无法访问该端口。您只能关闭默认情况下处于打开状态的端口，也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"不受信任的客户端网络"选项卡上的设置。例如，如果节点不受信任，端口 SSH/22 在客户端网络上被阻止，即使它在"管理外部访问"选项卡上已打开。"不受信任的客户端网络"选项卡上的设置将覆盖客户端网络上的封闭端口（如 443、8443、9443）。

步骤

1. 选择*管理外部访问权限*。该选项卡显示一个表格，其中包含网格中节点的所有外部端口（默认情况下非网格节点可访问的端口）。
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开关打开或关闭选定端口。
   - 选择*Open all displayed ports*以打开表格中列出的所有端口。
   - 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 Grid Manager 端口 443 或 8443，则当前连接到受阻端口的任何用户（包括您）都将失去对 Grid Manager 的访问权限，除非其 IP 地址已添加到特权地址列表中。

   使用表格右侧的滚动条，确保您已查看所有可用端口。使用搜索字段通过输入端口号来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 **Save**

不受信任的客户端网络

如果节点的客户端网络不受信任，则该节点仅接受配置为负载平衡器端点的端口上的入站流量，以及您在此选项卡上选择的其他端口（可选）。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。

如果未配置负载均衡器端点，则现有客户端连接可能会失败。

您在*不受信任的客户端网络*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*不受信任的客户端网络*。
2. 在设置新节点默认值部分，指定在扩展过程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。
   - 不受信任：在扩展中添加节点时，其客户端网络不受信任。

   根据需要，您可以返回此选项卡以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. 使用以下选项选择应仅在显式配置的负载平衡器端点或其他选定端口上允许客户端连接的节点：

   - 选择*显示的节点不受信任*，将表中显示的所有节点添加到不受信任的客户端网络列表中。
   - 选择*Trust on displayed nodes*，从不受信任的客户端网络列表中删除表中显示的所有节点。
   - 使用每个节点旁边的切换开关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*对显示的节点不信任*将所有节点添加到不受信任的客户端网络列表中，然后使用单个节点旁边的切换开关将该单个节点添加到受信任的客户端网络列表中。

   使用表格右侧的滚动条，确保您已查看所有可用节点。使用搜索字段通过输入节点名称来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. 选择 **Save**。

新的防火墙设置将立即应用和实施。如果未配置负载均衡器端点，现有客户端连接可能会失败。