管理证书
StorageGRID

NetApp
April 10, 2024

目录

管理证书

关于安全证书

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。此外，还支持无证书的不安全连接，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 系统强化准则 服务器证书。
- StorageGRID 支持将 CA 中的证书捆绑到一个文件中（称为 CA 证书包）。

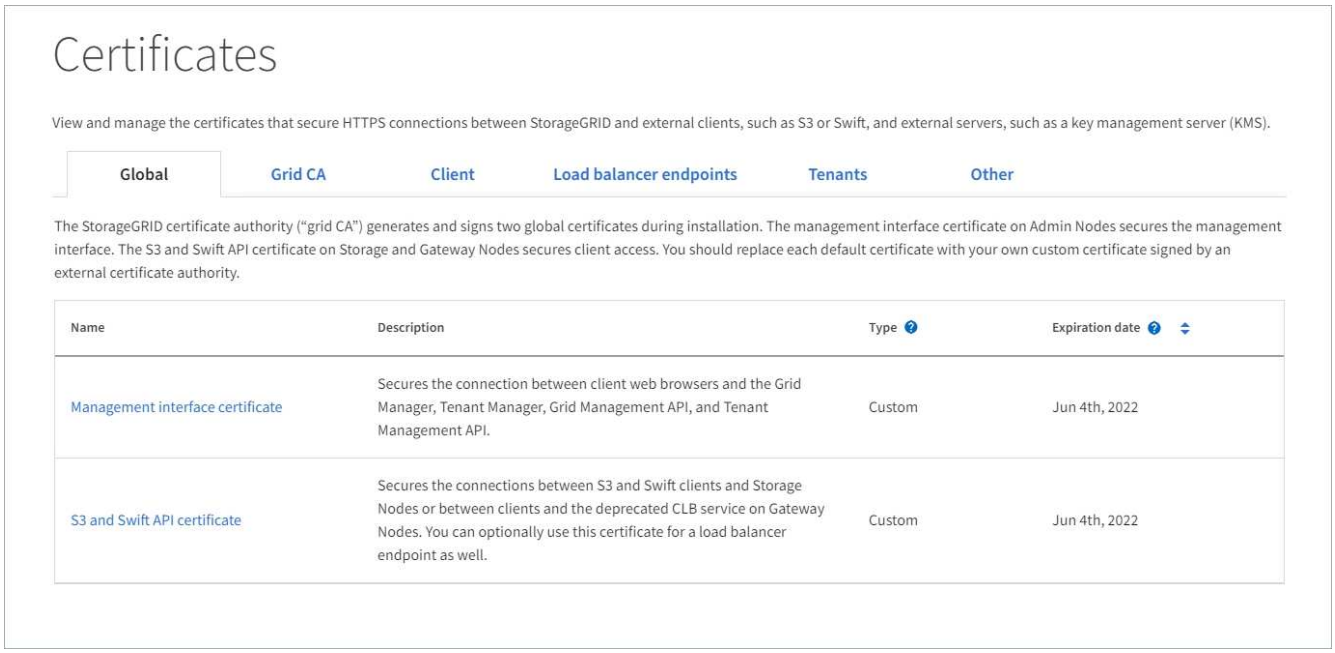
> StorageGRID 还包括在所有网格上相同的操作系统 CA 证书。在生产环境中，请确保指定一个由外部证书颁发机构签名的自定义证书，以替代操作系统 CA 证书。

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。

1. 在 Grid Manager 中，选择 * 配置 * > * 安全性 * > * 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。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， CLB 服务（已弃用）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上载或生成的，用于保护 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

- 选择一个端点名称以打开一个浏览器选项卡，其中包含有关负载平衡器端点的信息，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：

- 身份联合证书
- 云存储池证书
- 密钥管理服务器（ KMS ）证书
- 单点登录证书
- 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

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

- 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
- 为 S3， C2S S3 或 Azure 指定云存储池证书
- 手动为依赖方信任指定 SSO 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

安全证书详细信息

下面介绍了每种类型的安全证书，并提供了指向包含实施说明的文章的链接。

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	对与存储节点，网关节点上已弃用的连接负载平衡器（CLB）服务以及负载平衡器端点（可选）的安全 S3 或 Swift 客户端连接进行身份验证。	• 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传或生成单独的证书。 • 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

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

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

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

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 ）

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

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

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。

有关 StorageGRID 如何为 REST API 保护客户端连接的详细信息，请参见 使用 S3 或 使用 Swift。

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。

> 为了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 ` .pem` 保存文件。

   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：
   - * 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 * ： 证书所有者的 X.509 主题或可分辨名称（ DN ）。
   - * 有效天数 * ： 创建证书后的天数到期。
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 ` .pem` 保存文件。

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，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。

您需要的内容

- 您具有特定的访问权限。
- 您已有 `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 `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 用户身份登录时，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 *wilder-admin-node-fqdn* -type management`

- 对于 ` 域` ，请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` 。
- 将 ` 键入` 设置为 `management` 以配置管理接口证书，网格管理器和租户管理器将使用该证书。
- 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` 参数覆盖默认有效期。

> 运行 `make-certificate` 时，证书的有效期开始。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。` $ 退出`
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 捆绑包 ` .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 ` .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. 保存扩展名为 ` .pem` 的文本文件。

   例如： `storagegRid_certificate.pem`

配置 **S3** 和 **Swift API** 证书

您可以替换或还原用于通过 S3 或 Swift 客户端连接到存储节点，网关节点上已弃用的连接负载平衡器（ CLB ）服务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 ）。

> 为了确保操作不会因服务器证书失败而中断，根服务器证书即将过期时会触发 * 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 ` .pem` 保存文件。

   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：
   - * 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 * ： 证书所有者的 X.509 主题或可分辨名称（ DN ）。
   - * 有效天数 * ： 创建证书后的天数到期。
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 ` .pem` 保存文件。

   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

对于 S3 和 Swift 客户端与存储节点的连接以及网关节点上已弃用的 CLB 服务，您可以还原为使用默认 S3 和 Swift API 证书。但是，您不能对负载平衡器端点使用默认 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，无法从系统中恢复。默认的 S3 和 Swift API 证书将用于以后与存储节点以及网关节点上已弃用的 CLB 服务建立的新 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 捆绑包 ` .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 ` .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. 保存扩展名为 ` .pem` 的文本文件。

   例如： `storagegRid_certificate.pem`

相关信息

- 使用 S3
- 使用 Swift
- 配置 S3 API 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。

您需要的内容

- 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 * 证书 PEM* 部分中，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 * 复制证书 PEM* 。
b. 将复制的证书粘贴到文本编辑器中。
c. 保存扩展名为 ` .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，您可以在配置负载平衡器端点时生成或上传服务器证书。

您需要的内容

- 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。

> 网关节点上的单独连接负载平衡器（ CLB ）服务已弃用，不建议用于 FabricPool 。

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。

请参见有关的信息 常规安全证书用途 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败而中断，当此服务器证书即将到期时，系统将触发 " 证书 " 页面上配置的 * 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。

您需要的内容

- 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

按照适用于您的场景的操作步骤 添加客户端证书：

- [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. 输入一个证书名称、该名称至少包含1个字符、但不超过32个字符。
4. 要使用外部监控工具访问 Prometheus 指标，请选择 * 允许 Prometheus* 。
5. 在*证书类型*部分中、上传管理接口证书`.pem`文件。
   a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
   b. 上传管理接口证书文件(`.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。
6. 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。
   f. 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。

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. 输入一个证书名称、该名称至少包含1个字符、但不超过32个字符。
5. 要使用外部监控工具访问 Prometheus 指标，请选择 * 允许 Prometheus* 。
6. 在*证书类型*部分中、上传客户端证书、私钥和CA捆绑包`.pem` files：
   a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
   b. 上传客户端证书、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 * 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. 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。
   f. 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。

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. 输入一个证书名称、该名称至少包含1个字符、但不超过32个字符。
4. 要使用外部监控工具访问 Prometheus 指标，请选择 * 允许 Prometheus* 。
5. 在*证书类型*部分中、选择*生成证书*。
6. 指定证书信息：
   - 域名：要包含在证书中的管理节点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管理节点IP地址。
   - * 主题 * ： 证书所有者的 X.509 主题或可分辨名称（ DN ）。
7. 选择 * 生成 * 。
8. 【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 ` .pem` 保存文件。

   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。

9. 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。

10. 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。
11. 选择*管理接口证书*。
12. 选择 * 使用自定义证书 * 。
13. 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。

14. 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：+
       - 管理接口客户端证书同时提供给"**CA**证书"和"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。

    f. 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. 输入一个证书名称、该名称至少包含1个字符、但不超过32个字符。
5. 要使用外部监控工具访问 Prometheus 指标，请选择 * 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 ` .pem` 保存文件。

   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：
   - * 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 * ： 证书所有者的 X.509 主题或可分辨名称（ DN ）。
   - * 有效天数 * ： 创建证书后的天数到期。
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 ` .pem` 保存文件。

   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 ` .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 * 复制证书 PEM* 。
b. 将复制的证书粘贴到文本编辑器中。
c. 保存扩展名为 ` .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，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。