管理证书

StorageGRID software

NetApp
July 23, 2026

目录

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。

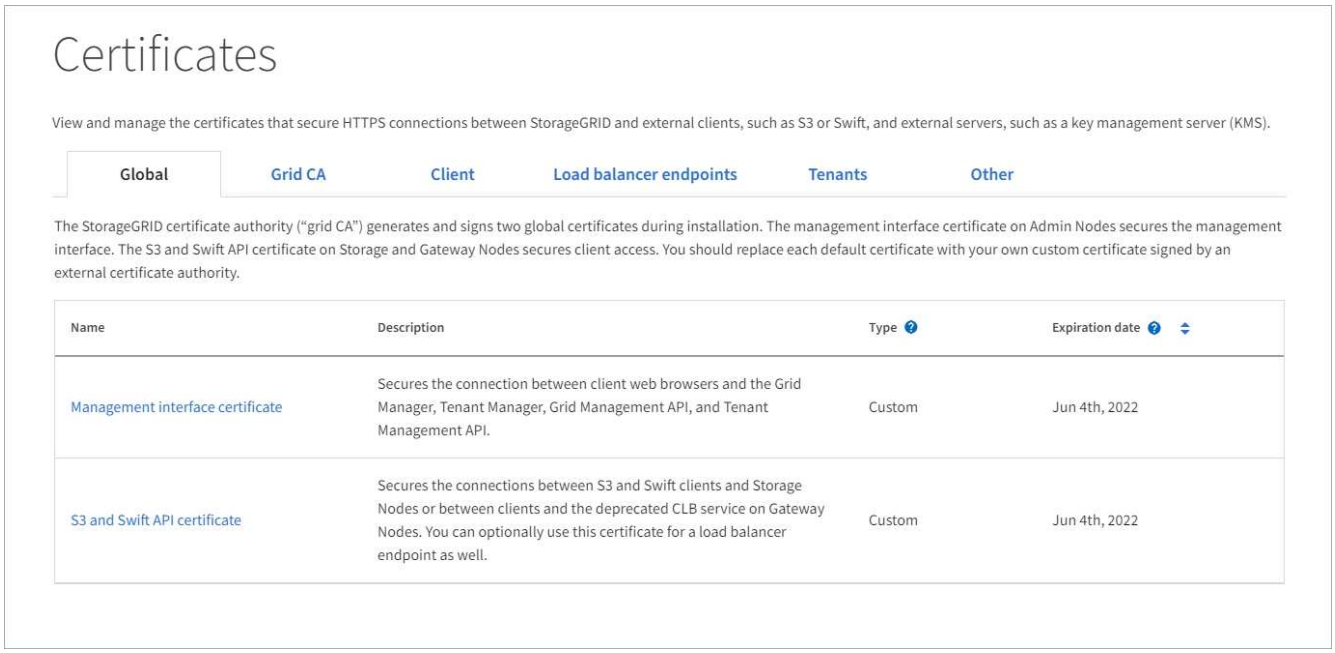
服务器和客户端证书类型的变体以多种方式实现。在配置系统之前，您应该准备好特定 StorageGRID 配置所需的所有证书。

${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。