配置服务器证书

StorageGRID 11.8

NetApp
May 10, 2024

目录

配置服务器证书

支持的服务器证书类型

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

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

有关StorageGRID如何保护客户端连接的详细信息、请参见 "S3和Swift客户端的安全性"。

配置管理接口证书

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

关于此任务

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

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

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

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

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

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

添加自定义管理接口证书

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

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。

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

上传证书

上传所需的服务器证书文件。

a. 选择 * 上传证书 * 。

b. 上传所需的服务器证书文件：

- * 服务器证书 * ： 自定义服务器证书文件（ PEM 编码）。
- 证书专用密钥:自定义服务器证书专用密钥文件 (`.key`）。

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

- * CA bundle* ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

c. 展开 * 证书详细信息 * 以查看您上传的每个证书的元数据。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。

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

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

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

d. 选择 * 保存 * 。+ 自定义管理接口证书将用于与Grid Manager、租户管理器、Grid Manager API或租户管理器API的所有后续新连接。

生成证书

生成服务器证书文件。

> 生产环境的最佳实践是使用由外部证书颁发机构签名的自定义管理接口证书。

a. 选择 * 生成证书 * 。

b. 指定证书信息：

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

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

c. 选择 * 生成 * 。

d. 选择*证书详细信息*以查看生成的证书的元数据。

- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 保存 * 。+ 自定义管理接口证书将用于与Grid Manager、租户管理器、Grid Manager API或租户管理器API的所有后续新连接。

5. 刷新页面以确保 Web 浏览器已更新。

> 上传或生成新证书后，请留出最多一天的时间来清除任何相关证书到期警报。

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

还原默认管理接口证书

您可以使用网格管理器和租户管理器连接的默认管理接口证书还原到。

步骤

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

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

4. 刷新页面以确保 Web 浏览器已更新。

使用脚本生成新的自签名管理接口证书

如果需要严格验证主机名，可以使用脚本生成管理接口证书。

开始之前

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

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

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

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

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

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

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

   在您的选择中包括开始和结束标记。

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

下载或复制管理接口证书

您可以保存或复制管理接口证书内容，以便在其他位置使用。

步骤

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

下载证书文件或 **CA** 包

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

a. 选择 * 下载证书 * 或 * 下载 CA 捆绑包 * 。

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

b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

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

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

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

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

   例如： `storagegrid_certificate.pem`

配置 S3 和 Swift API 证书

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

关于此任务

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

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

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

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

您可以上传或生成自定义 S3 和 Swift API 证书。

添加自定义 S3 和 Swift API 证书

步骤

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

上传证书

上传所需的服务器证书文件。

a. 选择 * 上传证书 * 。

b. 上传所需的服务器证书文件：

   - * 服务器证书 * ： 自定义服务器证书文件（ PEM 编码）。
   - 证书专用密钥:自定义服务器证书专用密钥文件 (`.key`）。

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

   - * CA bundle* ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

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

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

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

     例如： `storagegrid_certificate.pem`

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

d. 选择 * 保存 * 。

   自定义服务器证书用于后续的新 S3 和 Swift 客户端连接。

生成证书

生成服务器证书文件。

a. 选择 * 生成证书 * 。

b. 指定证书信息：

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

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

c. 选择 * 生成 * 。

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

- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 保存 * 。

自定义服务器证书用于后续的新 S3 和 Swift 客户端连接。

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

   上传或生成新证书后，请留出最多一天的时间来清除任何相关证书到期警报。

6. 刷新页面以确保 Web 浏览器已更新。

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

还原默认 S3 和 Swift API 证书

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

步骤

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

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

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

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

5. 刷新页面以确保 Web 浏览器已更新。

下载或复制 S3 和 Swift API 证书

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

步骤

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

   下载证书文件或 **CA** 包

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

   a. 选择 * 下载证书 * 或 * 下载 CA 捆绑包 * 。

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

   b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

      例如： `storagegrid_certificate.pem`

   复制证书或 **CA** 捆绑包 **PEM**

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

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

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

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

      例如： `storagegrid_certificate.pem`

相关信息

- "使用S3 REST API"
- "使用Swift REST API"

- "配置S3端点域名"

复制网格 CA 证书

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

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

关于此任务

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

步骤

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

   下载证书文件

   下载证书 `.pem` 文件

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

      例如： `storagegrid_certificate.pem`

   复制证书 **PEM**

   复制证书文本以粘贴到其他位置。

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

      例如： `storagegrid_certificate.pem`

为 FabricPool 配置 StorageGRID 证书

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

开始之前

- 您已拥有 "特定访问权限"。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。

关于此任务

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

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

步骤

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

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

3. 在 ONTAP 中将 StorageGRID 附加为云层。

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

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