



# 配置服务器证书

## StorageGRID 11.5

NetApp  
April 11, 2024

# 目录

配置服务器证书 .....	1
支持的自定义服务器证书类型 .....	1
负载均衡器端点的证书 .....	1
为网格管理器和租户管理器配置自定义服务器证书 .....	1
还原网格管理器和租户管理器的默认服务器证书 .....	2
配置自定义服务器证书以连接到存储节点或CLB服务 .....	3
还原S3和Swift REST API端点的默认服务器证书 .....	4
复制StorageGRID 系统的CA证书 .....	4
为FabricPool 配置StorageGRID 证书 .....	5
为管理接口生成自签名服务器证书 .....	6

# 配置服务器证书

您可以自定义StorageGRID 系统使用的服务器证书。

StorageGRID 系统将安全证书用于多种不同的用途：

- 管理接口服务器证书：用于保护对网格管理器、租户管理器、网格管理API和租户管理API的访问。
- 存储API服务器证书：用于保护对存储节点和网关节点的访问、API客户端应用程序使用这些节点上传和下载对象数据。

您可以使用在安装期间创建的默认证书、也可以将其中一种或两种默认类型的证书替换为您自己的自定义证书。

## 支持的自定义服务器证书类型

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

有关StorageGRID 如何为REST API保护客户端连接的详细信息、请参见S3或Swift实施指南。

## 负载均衡器端点的证书

StorageGRID 单独管理用于负载均衡器端点的证书。要配置负载均衡器证书、请参见有关配置负载均衡器端点的说明。

相关信息

["使用 S3"](#)

["使用 Swift"](#)

["配置负载均衡器端点"](#)

## 为网格管理器和租户管理器配置自定义服务器证书

您可以将默认 StorageGRID 服务器证书替换为一个自定义服务器证书，该证书允许用户访问网格管理器和租户管理器，而不会遇到安全警告。

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服务器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服务器证书、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浏览器中安装根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过期时、系统会触发\*管理接口的服务器证书到期\*警报和原有的管理接口证书到期(Management Interface Certificate Expiration、MCEP)警报。根据需要、您可以选择\*支持\*>\*工具\*>\*网络拓扑\*来查看当前服务证书到期前的天数。然后、选择\*主管理节点\_\*>\*. CMN\*>\*资源\*。



如果您要使用域名而非 IP 地址访问网络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服务器证书将过期。
- 您可以从自定义管理接口服务器证书还原到默认服务器证书。

## 步骤

1. 选择\*配置\*>\*网络设置\*>\*服务器证书\*。
2. 在管理接口服务器证书部分中、单击\*安装自定义证书\*。
3. 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 (.crt) 。
  - 服务器证书专用密钥：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。

4. 单击 \* 保存 \*。

自定义服务器证书将用于所有后续的新客户端连接。

选择一个选项卡以显示有关已上传的默认StorageGRID 服务器证书或CA签名证书的详细信息。



上传新证书后、请留出最多一天的时间来清除任何相关证书到期警报(或旧警报)。

5. 刷新页面以确保 Web 浏览器已更新。

## 还原网络管理器和租户管理器的默认服务器证书

您可以还原为使用网络管理器和租户管理器的默认服务器证书。

### 步骤

1. 选择\*配置\*>\*网络设置\*>\*服务器证书\*。
2. 在管理接口服务器证书部分中、单击\*使用默认证书\*。
3. 单击确认对话框中的 \* 确定 \*。

还原默认服务器证书时、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。默认服务器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。

## 配置自定义服务器证书以连接到存储节点或CLB服务

您可以替换用于通过S3或Swift客户端连接到存储节点或网关节点上的CLB服务(已弃用)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、用户可能还需要在用于访问系统的S3或Swift API客户端中安装根CA证书、具体取决于所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、在根服务器证书即将过期时、系统会触发\*存储API端点服务器证书到期\*警报和原有的存储API服务端点证书到期(SCEP)警报。根据需要、您可以选择\*支持工具\*网格拓扑\*来查看当前服务证书到期前的天数。然后、选择\*主管理节点\_ CMN资源。

只有当客户端在网关节点上使用已弃用的CLB服务连接到StorageGRID 或直接连接到存储节点时、才会使用自定义证书。在管理节点或网关节点上使用负载均衡器服务连接到StorageGRID 的S3或Swift客户端使用为负载均衡器端点配置的证书。



负载均衡器端点的\*负载均衡器端点证书到期\*警报将触发、该端点不久将过期。

步骤

1. 选择\*配置\*>\*网络设置\*>\*服务器证书\*。
2. 在对象存储API服务端点服务器证书部分中、单击\*安装自定义证书\*。
3. 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 (.crt) 。
  - 服务器证书专用密钥：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。
4. 单击 \* 保存 \*。

自定义服务器证书用于所有后续新的API客户端连接。

选择一个选项卡以显示有关已上传的默认StorageGRID 服务器证书或CA签名证书的详细信息。



上传新证书后、请留出最多一天的时间来清除任何相关证书到期警报(或旧警报)。

5. 刷新页面以确保 Web 浏览器已更新。

相关信息

["使用 S3"](#)

["使用 Swift"](#)

["配置S3 API端点域名"](#)

## 还原S3和Swift REST API端点的默认服务器证书

您可以还原为对S3和Swift REST API端点使用默认服务器证书。

步骤

1. 选择\*配置\*>\*网络设置\*>\*服务器证书\*。
2. 在对象存储API服务端点服务器证书部分中、单击\*使用默认证书\*。
3. 单击确认对话框中的 \* 确定 \*。

还原对象存储API端点的默认服务器证书时、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。默认服务器证书将用于所有后续的新API客户端连接。

4. 刷新页面以确保 Web 浏览器已更新。

## 复制StorageGRID 系统的CA证书

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

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须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\*>\*网络设置\*>\*服务器证书\*。
2. 在\*内部CA证书\*部分中、选择所有证书文本。

您必须包括 -----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE----- 您选择的内容。

## Internal CA Certificate

StorageGRID uses an internal Certificate Authority (CA) to secure internal traffic. This certificate does not change if you upload your own certificates.

To export the internal CA certificate, copy all of the certificate text (starting with -----BEGIN CERTIFICATE and ending with END CERTIFICATE-----), and save it as a .pem file.

```
Subject DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT
Certificate: -----BEGIN CERTIFICATE-----
MIIEETjCCAzagAwIBAgIJAjMIM8F717AKQMA0GCSqGSIb3DQEBCwUAMHcxZzA3BGNV
BAYTA1VTMRMwEQYDVQKIExpDYWxpZm9ybm1hMRIwEAYDVQQHEw1TdW5ueXZhbG91
FDASBgNVBAoTC051dEFwCzBjbmMuMRswGQYDVQQLEExJOZXRhcHAgu3RvcmlFZnZlUz
SUQxMDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2M
MHcxZzA3BGNVBA1VTMRMwEQYDVQKIExpDYWxpZm9ybm1hMRIwEAYDVQQHEw1TdW
5ueXZhbG91FDASBgNVBAoTC051dEFwCzBjbmMuMRswGQYDVQQLEExJOZXRhcHAgu
U3RvcmlFZnZlUzSUQxMDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2MDE2M
ADCCAQoCggEBAN1ULKf8my5k7LFX1Kdn3Y29QpGf0QLr8+01Fx9RwPBo8akVMxkb
0RhOLbZIp8hI+v8FHS7057o1balMbNOeyjdgVywGxOZ+EqXoU5hEYKjx5Yj/wueo8
nK6fzrhRwKfLB0JKdPvgXJYCKntS5JPjx2dsd5Po1eq0Zt54pFkuMuqjGeqjY
s+2CSR1mN3kUAHORu20jHmVvo+P15K9dP+YUuwH9t3KccY95tINIhzLKBvSf2QQC
pzf6Xncg7ebd/B1kKmZbBwbaerscf+Q17w6z5kfVe4Qhx1CkR5YryHfAheIwMgu
A4790hstckFq34WkrsGatsWz6RXm1gQv8CAwEAAB3DCB2TAdBgNVHQ4EFgQU
fiTcKt2l0ccoen9s4BD0R5TLgYwgakGA1UdIw5BoTCBnoAUFiTCkT2l0ccoen9s
x4BD0R5TLgahE6R5MHcxZzA3BGNVBA1VTMRMwEQYDVQKIExpDYWxpZm9ybm1h
MRIwEAYDVQQHEw1TdW5ueXZhbG91FDASBgNVBAoTC051dEFwCzBjbmMuMRswGQY
VQLEExJOZXRhcHAgu3RvcmlFZnZlUzSUQxMDE2MDE2MDE2MDE2MDE2MDE2MDE2M
MAwGA1UdEwQFMAMBaf8wDQYJKoZIhvcNAQELBQADggEBANhsVJQaCs72UzQONjpu
cZKai1iUQr+S2h9RjfsY3jKwu7+SBh9A2Phgmu8p1gA1q55a7bE3+7Ye3TwstD1l
acB8B3Iuh1xvLpQ5QYDvRS7YtQ4cKaSwongy+yyxoU0MTzn6DFXGd4i4pr5+xS
/qccXWekopYzfUtK5wqfjRqUsdFc58djp+adDqI8F5m9ZXGvwydJgBuyUjwgdKw
109bWlH++AKcELR8cgg/B6RzoAGE4Km1BvVw+rJrxu0//NCU3u5KaGte862f+gG
I37X9GEzFtqnnhXvo2BZ/OLyGgYbgiksad1nFU3VAjK9iVGHHLpD6BQ8ZxQhYgc
aHh=
-----END CERTIFICATE-----
```

3. 右键单击选定文本、然后选择\*复制\*。
4. 将复制的证书粘贴到文本编辑器中。
5. 使用扩展名保存文件 .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，您可以在配置负载均衡器端点时生成或上传服务器证书。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须使用支持的浏览器登录到网络管理器。

关于此任务

创建负载均衡器端点时、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、请参见有关为FabricPool 配置StorageGRID 的说明。



网关节点上的单独连接负载均衡器（CLB）服务已弃用，不再建议用于 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 负载均衡器端点以供 FabricPool 使用。

创建HTTPS负载均衡器端点时、系统会提示您上传服务器证书、证书专用密钥和CA捆绑包。

3. 在 ONTAP 中将 StorageGRID 附加为云层。

指定负载均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。

#### 相关信息

["为 FabricPool 配置 StorageGRID"](#)

## 为管理接口生成自签名服务器证书

您可以使用脚本为需要严格主机名验证的管理API客户端生成自签名服务器证书。

#### 您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 Passwords.txt 文件

#### 关于此任务

在生产环境中、您应使用由已知证书颁发机构(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。

#### 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API客户端与StorageGRID 同步到同一时间源；否则、客户端可能会拒绝此证书。

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 365
```

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\*配置服务器证书管理接口服务器证书\*。

#### 7. 将管理API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。

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。