配置安全设置

StorageGRID software

NetApp
July 23, 2026

目录

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**。

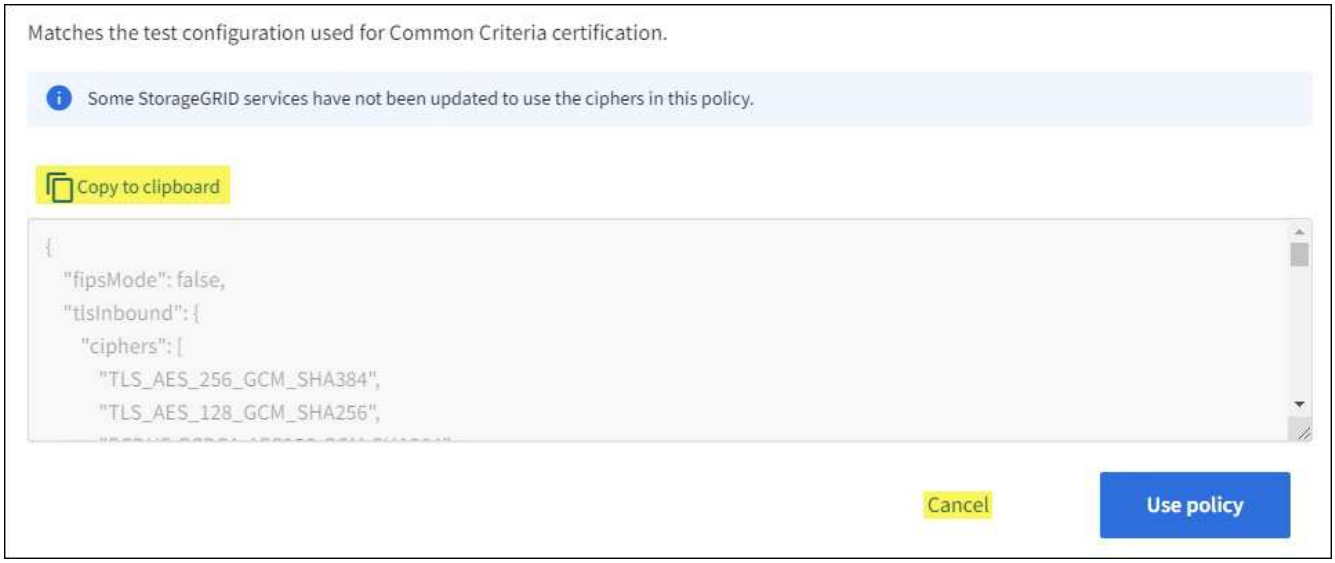
   策略磁贴上的*当前策略*旁边会显示一个绿色复选标记。

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**。