配置安全设置
StorageGRID 11.8

NetApp
March 19, 2024

目录

配置安全设置

管理TLS和SSH策略

TLS和SSH策略用于确定使用哪些协议和加密方法与客户端应用程序建立安全TLS连接、以及与内部StorageGRID 服务建立安全SSH连接。

此安全策略控制TLS和SSH如何对移动数据进行加密。通常、请使用现代兼容性(默认)策略、除非您的系统需要符合通用标准或您需要使用其他密钥。

某些StorageGRID 服务尚未更新、无法在这些策略中使用这些加密方法。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "root访问权限"。

选择一个安全策略

步骤

1. 选择*configuration*>*Security*>*Security settings。

   TLS和SSH策略*选项卡显示可用策略。当前活动的策略会在策略磁贴上标记为绿色复选标记。

2. 查看图块、了解可用策略。

策略	Description
现代兼容性(默认)	如果需要强加密、则使用默认策略、除非您有特殊要求。此策略与大多数TLS和SSH客户端兼容。
传统兼容性	如果需要为旧客户端提供其他兼容性选项、请使用此策略。此策略中的其他选项可能会使其不如现代兼容性策略安全。
通用标准	如果您需要通用标准认证、请使用此策略。

策略	Description
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3.0.8将外部客户端连接到负载平衡器端点、租户管理器和网格管理器、请使用此策略。使用此策略可能会降低性能。 注意：选择此策略后，所有节点都必须为 "已滚动重新启动" 激活NetApp加密安全模块。使用*Maintenance (维护)*>*rolling reboot (滚动重新启动)*启动并监控重新启动。
自定义	如果需要应用您自己的用户名或用户名、请创建自定义策略。

3. 要查看有关每个策略的加密、协议和算法的详细信息，请选择*查看详细信息*。
4. 要更改当前策略，请选择*使用策略*。

   策略磁贴上的*current policy*旁边会出现一个绿色复选标记。

创建自定义安全策略

如果需要应用自己的用户名、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的磁贴中，选择*查看详细信息*。
2. 选择*复制到剪贴板*，然后选择*取消*。

3. 从“自定义策略”磁贴中，选择“配置和使用”。
4. 粘贴您复制的JSON并进行所需的任何更改。
5. 选择*使用策略*。

   自定义策略磁贴上的*当前策略*旁边会出现一个绿色复选标记。

6. (可选)选择*Edit configuration*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、并且配置的TLS策略与不兼容、则可能无法登录到网格管理器 "已配置服务器证书"。

您可以临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 `#`。
2. 运行以下命令：

   ```
   restore-default-cipher-configurations
   ```
3. 从 Web 浏览器访问同一管理节点上的网格管理器。
4. 按照中的步骤进行操作 选择一个安全策略 以重新配置策略。

配置网络和对象安全性

您可以将网络和对象安全性配置为对存储的对象进行加密、防止某些S3和Swift请求、或者允许客户端连接到存储节点时使用HTTP而不是HTTPS。

存储对象加密

通过存储对象加密、可以在通过S3读取所有对象数据时对这些数据进行加密。默认情况下、存储的对象不会进行加密、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，所有新载入的对象都将被加密，但不会对现有存储的对象进行任何更改。如果禁用加密、则当前加密的对象仍会保持加密状态、但不会对新加装的对象进行加密。

存储的对象加密设置仅适用于尚未通过存储分段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"。

防止修改客户端

防止客户端修改是一项系统范围的设置。如果选择了*prevent client修改*选项，则会拒绝以下请求。

S3 REST API

- DeleteBuckets请求
- 修改现有对象数据，用户定义的元数据或 S3 对象标记的任何请求

Swift REST API

- 删除容器请求
- 修改任何现有对象的请求。例如，以下操作被拒绝： PUT 覆盖，删除，元数据更新等。

为存储节点连接启用HTTP

默认情况下、客户端应用程序会使用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和Swift客户端需要直接与存储节点建立HTTP连接时、才使用HTTP进行存储节点连接。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、您无需使用此选项(因为您可以 "配置每个负载平衡器端点" 以使用HTTP或HTTPS)。

请参见 "摘要：客户端连接的 IP 地址和端口" 了解S3和Swift客户端在使用HTTP或HTTPS连接到存储节点时使用的端口。

选择选项

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

步骤

1. 选择*configuration*>*Security*>*Security settings。
2. 选择*网络和对象*选项卡。
3. 对于存储的对象加密，如果不希望对存储的对象进行加密，请使用*None*(默认)设置，或者选择*AES-128*或*AES-256*对存储的对象进行加密。
4. 如果要阻止S3和Swift客户端发出特定请求，可选择*prevent client修改*。

   如果更改此设置，则应用新设置需要大约一分钟的时间。已配置的值将进行缓存以提高性能和扩展能力。

5. 如果客户端直接连接到存储节点并且您要使用HTTP连接，则可以选择*为存储节点连接启用HTTP *。

   为生产网格启用 HTTP 时请务必小心，因为请求会以未加密方式发送。

6. 选择 * 保存 * 。

更改接口安全设置

通过接口安全设置、您可以控制在用户处于非活动状态的时间超过指定时间时是否注销、以及是否在API错误响应中包含堆栈跟踪。

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 "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

指示用户的浏览器在注销前可以处于非活动状态的时间长度。默认值为 15 分钟。

浏览器非活动超时还受以下因素控制：

- 一个单独的不可配置 StorageGRID 计时器，其中包括用于系统安全保护的计时器。每个用户的身份验证令牌将在用户登录后16小时过期。当用户的身份验证过期时、即使禁用了浏览器非活动超时或尚未达到浏览器超时值、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(假设为StorageGRID 启用了单点登录(SSO))。

  如果启用了SSO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。请参见 "配置单点登录"。

管理**API**堆栈跟踪

控制是否在Grid Manager和租户管理器API错误响应中返回堆栈跟踪。

默认情况下、此选项处于禁用状态、但您可能希望在测试环境中启用此功能。通常、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*configuration*>*Security*>*Security settings。
2. 选择*Interface*选项卡。
3. 要更改浏览器非活动超时设置：
   a. 展开可展开面。
   b. 要更改超时期限、请指定一个介于60秒和7天之间的值。默认超时为15分钟。
   c. 要禁用此功能、请取消选中此复选框。
   d. 选择 * 保存 * 。

      新设置不会影响当前已登录的用户。用户必须重新登录或刷新浏览器，新的超时设置才能生效。
4. 要更改管理API堆栈跟踪设置、请执行以下操作：
   a. 展开可展开面。

b. 选中此复选框可在Grid Manager和租户管理器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 * 保存 * 。