管理StorageGRID 网络和连接

StorageGRID 11.5

NetApp
April 11, 2024

目录

管理StorageGRID 网络和连接

您可以使用网格管理器配置和管理 StorageGRID 网络和连接。

请参见 "配置S3和Swift客户端连接" 了解如何连接 S3 或 Swift 客户端。

- "StorageGRID 网络准则"
- "查看IP地址"
- "支持传出 TLS 连接的密码"
- "更改网络传输加密"
- "配置服务器证书"
- "配置存储代理设置"
- "配置管理员代理设置"
- "管理流量分类策略"
- "链路成本是多少"

StorageGRID 网络准则

StorageGRID 在每个网格节点上最多支持三个网络接口，使您可以根据安全和访问要求为每个网格节点配置网络。

> 要修改或添加网格节点的网络、请参见恢复和维护说明。有关网络拓扑的详细信息、请参见网络连接说明。

网格网络

Required网格网络用于所有内部 StorageGRID 流量。它可以在网格中的所有节点之间以及所有站点和子网之间建立连接。

管理网络

可选。管理网络通常用于系统管理和维护。它也可用于客户端协议访问。管理网络通常是一个专用网络，不需要在站点之间进行路由。

客户端网络

可选。客户端网络是一种开放网络，通常用于提供对 S3 和 Swift 客户端应用程序的访问，因此网格网络可以进行隔离和保护。客户端网络可以与可通过本地网关访问的任何子网进行通信。

准则

- 每个 StorageGRID 网格节点都需要为其分配到的每个网络配置一个专用网络接口， IP 地址，子网掩码和网关。

- 一个网格节点在一个网络上不能有多个接口。
- 支持每个网格节点在每个网络上使用一个网关，并且该网关必须与节点位于同一子网中。如果需要，您可以在网关中实施更复杂的路由。
- 在每个节点上，每个网络都映射到一个特定的网络接口。

网络	接口名称
网格	eth0
admin （可选）	Eth1
客户端（可选）	Eth2

- 如果节点连接到 StorageGRID 设备，则每个网络都使用特定端口。有关详细信息，请参见适用于您的设备的安装说明。
- 每个节点都会自动生成默认路由。如果启用了 eth2 ，则 0.0.0.0/0 将在 eth2 上使用客户端网络。如果未启用 eth2 ，则 0.0.0.0/0 将在 eth0 上使用网格网络。
- 只有在网格节点加入网格后，客户端网络才会正常运行
- 可以在网格节点部署期间配置管理网络，以便在网格完全安装之前能够访问安装用户界面。

相关信息

"保持并恢复()"

"网络准则"

查看IP地址

您可以查看 StorageGRID 系统中每个网格节点的 IP 地址。然后，您可以使用此 IP 地址通过命令行登录到网格节点并执行各种维护过程。

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。

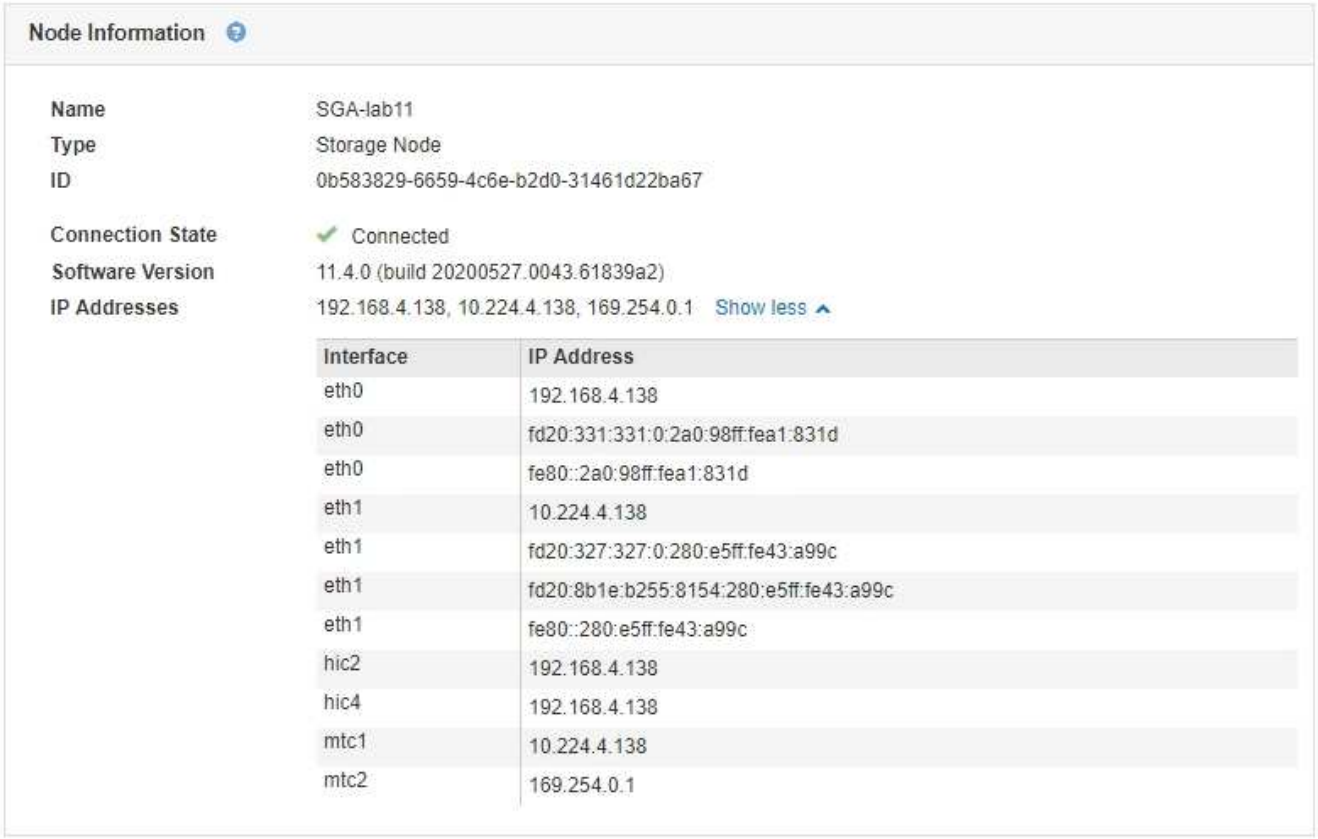
关于此任务

有关更改IP地址的信息、请参见恢复和维护说明。

步骤

1. 选择*节点*>*网格节点_*>*概述*。
2. 单击IP地址标题右侧的*显示更多*。

   此网格节点的 IP 地址会在表中列出。



相关信息

"保持并恢复()"

支持传出 TLS 连接的密码

StorageGRID 系统支持一组有限的密码套件，用于将传输层安全（ Transport Layer Security ， TLS ）连接到用于身份联合和云存储池的外部系统。

支持的 TLS 版本

StorageGRID 支持使用 TLS 1.2 和 TLS 1.3 连接到用于身份联合和云存储池的外部系统。

为了确保与一系列外部系统兼容，我们选择了可与外部系统结合使用的 TLS 密码。此列表大于支持在 S3 或 Swift 客户端应用程序中使用的密码列表。

协议版本，密码，密钥交换算法和 MAC 算法等 TLS 配置选项在 StorageGRID 中不可配置。如果您对这些设置有特定要求，请联系您的 NetApp 客户代表。

支持的 TLS 1.2 密码套件

支持以下 TLS 1.2 密码套件：

- tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256
- tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384

- tls_ECDHE_ECDSA_WIT_AES_128_GCM_SHA256
- tls_ECDHE_ECDSA_WIT_AES_256_GCM_SHA384
- tls_ECDHE_RSA_WIT_CHACHA20_POLY1305
- tls_ECDHE_ECDSA_ING_CHACHA20_POLY1305
- tls_rsa_and_aes_128_gcm_SHA256
- tls_rsa_and_aes_256_gcm_SHA384

支持的 **TLS 1.3** 密码套件

支持以下 TLS 1.3 密码套件：

- tls_aes_256_gcm_SHA384
- tls_chacHA20_POLY1305_SHA256
- tls_aes_128_gcm_SHA256

更改网络传输加密

StorageGRID 系统使用传输层安全（ Transport Layer Security ， TLS ）保护网格节点之间的内部控制流量。网络传输加密选项用于设置 TLS 用于加密网格节点之间的控制流量的算法。此设置不会影响数据加密。

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

默认情况下，网络传输加密使用 AES256-SHA 算法。此外，还可以使用 AES128-SHA 算法对控制流量进行加密。

步骤

1. 选择*配置系统设置网格选项*。
2. 在网络选项部分中，将网络传输加密更改为 * AES128-SHA* 或 * AES256-SHA* （默认）。

3. 单击 * 保存 * 。

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。

负载平衡器端点的证书

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

相关信息

"使用 S3"

"使用 Swift"

"配置负载平衡器端点"

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*。

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。

还原网格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格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平衡器服务连接到StorageGRID 的S3或Swift客户端使用为负载平衡器端点配置的证书。

> 负载平衡器端点的*负载平衡器端点证书到期*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。

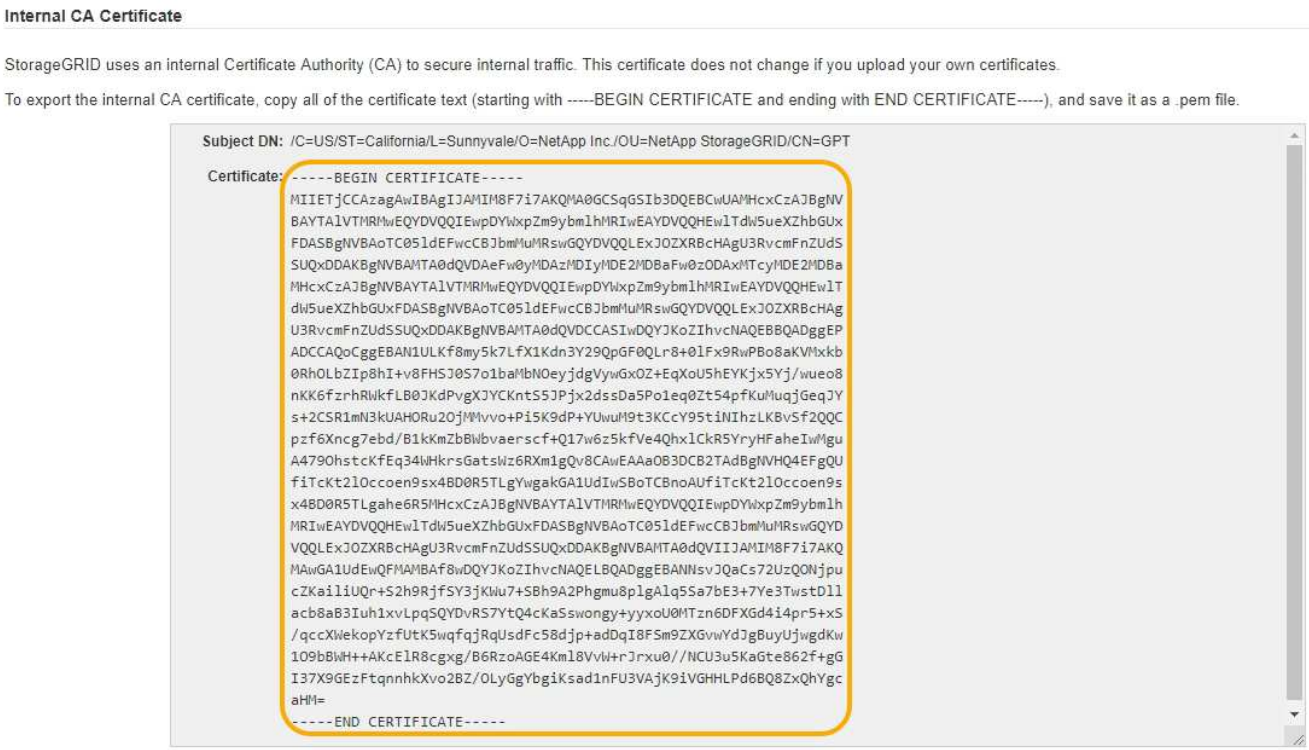
关于此任务

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。



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，您可以在配置负载平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格管理器。

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、请参见有关为FabricPool配置StorageGRID 的说明。

网关节点上的单独连接负载平衡器（ 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。

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。

配置存储代理设置

如果您使用的是平台服务或云存储池，则可以在存储节点和外部 S3 端点之间配置非透明代理。例如，您可能需要一个非透明代理来允许将平台服务消息发送到外部端点，例如 Internet 上的端点。

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格管理器。

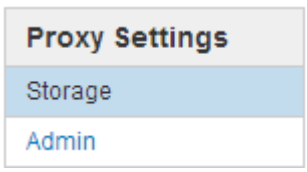
关于此任务

您可以为单个存储代理配置设置。

步骤

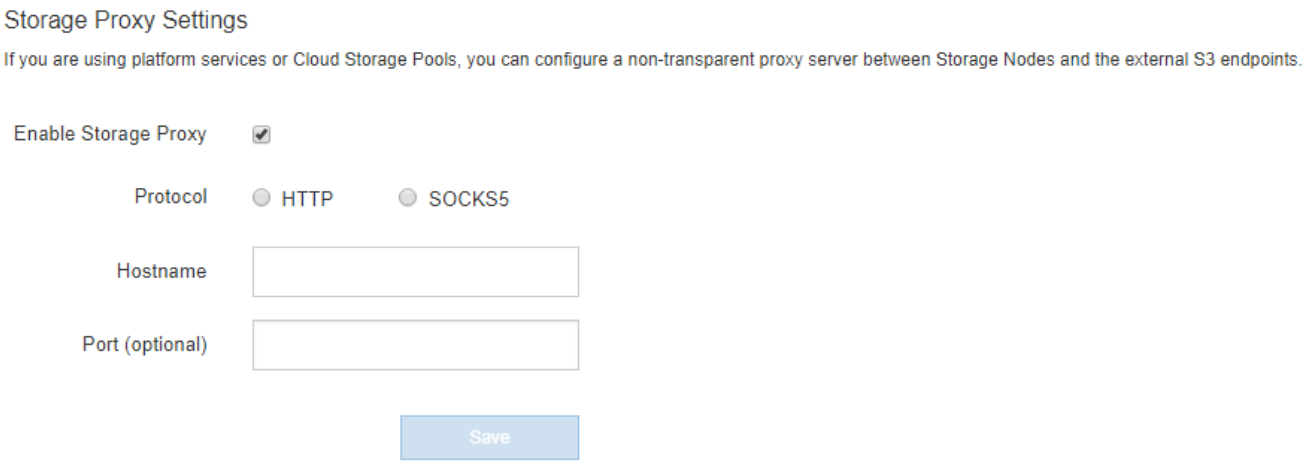
1. 选择*配置网络设置代理设置。

   此时将显示存储代理设置页面。默认情况下，在边栏菜单中选择了 * 存储 * 。



2. 选中 * 启用存储代理 * 复选框。

   此时将显示用于配置存储代理的字段。



3. 为非透明存储代理选择协议。
4. 输入代理服务器的主机名或 IP 地址。
5. （可选）输入用于连接到代理服务器的端口。

   如果对协议使用默认端口，则可以将此字段留空： 80 表示 HTTP ， 1080 表示 SOCKS5 。

6. 单击 * 保存 * 。

   保存存储代理后，可以配置和测试平台服务或云存储池的新端点。

   代理更改可能需要长达 10 分钟才能生效。

7. 检查代理服务器的设置，以确保不会阻止来自 StorageGRID 的平台服务相关消息。

完成后

如果需要禁用存储代理、请取消选中*启用存储代理*复选框、然后单击*保存*。

相关信息

"用于平台服务的网络和端口"

"使用 ILM 管理对象"

配置管理员代理设置

如果使用HTTP或HTTPS发送AutoSupport 消息、则可以在管理节点和技术支持(AutoSupport)之间配置非透明代理服务器。

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格管理器。

关于此任务

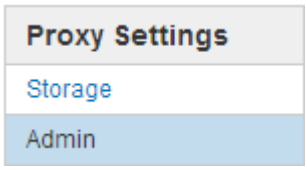
您可以为单个管理员代理配置设置。

步骤

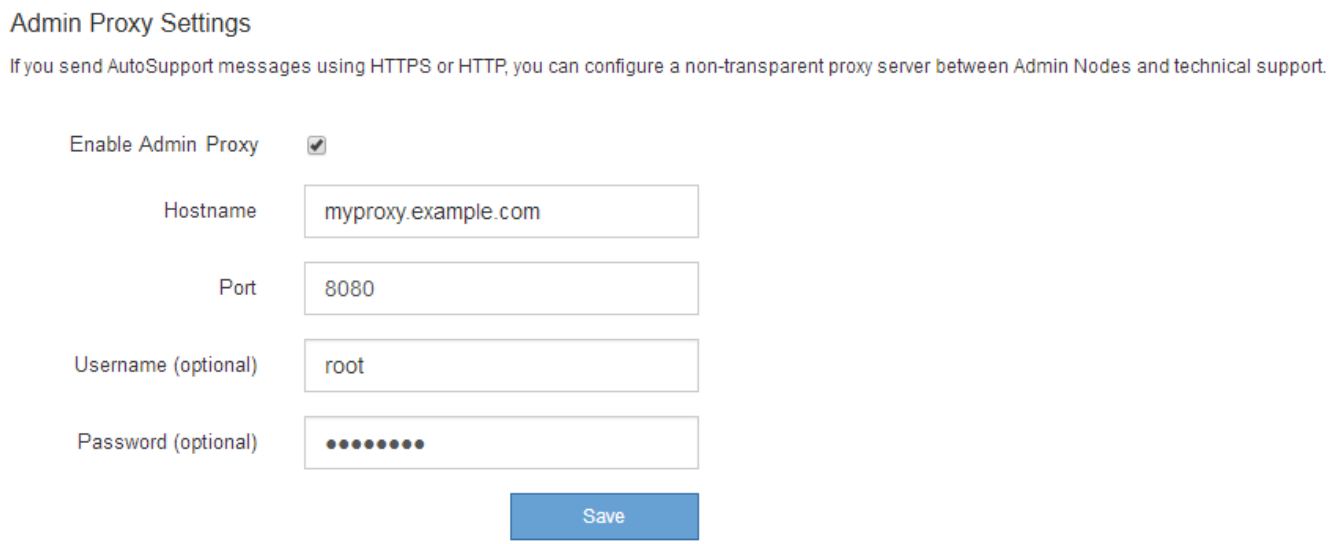
1. 选择*配置网络设置代理设置。

   此时将显示 Admin Proxy Settings 页面。默认情况下，在边栏菜单中选择了 * 存储 * 。

2. 从边栏菜单中选择 * 管理 * 。



3. 选中 * 启用管理代理 * 复选框。



4. 输入代理服务器的主机名或 IP 地址。
5. 输入用于连接到代理服务器的端口。
6. （可选）输入代理用户名。

   如果您的代理服务器不需要用户名，请将此字段留空。

7. （可选）输入代理密码。

   如果您的代理服务器不需要密码，请将此字段留空。

8. 单击 * 保存 * 。

   保存管理代理后，将在管理节点和技术支持之间配置代理服务器。

   代理更改可能需要长达 10 分钟才能生效。

9. 如果需要禁用代理、请取消选中*启用管理代理*复选框、然后单击*保存*。

相关信息

"指定AutoSupport 消息的协议"

管理流量分类策略

为了增强服务质量（ QoS ）服务，您可以创建流量分类策略来识别和监控不同类型的网络流量。这些策略有助于限制和监控流量。

流量分类策略应用于网关节点和管理节点的 StorageGRID 负载平衡器服务上的端点。要创建流量分类策略，必须已创建负载平衡器端点。

匹配规则和可选限制

每个流量分类策略都包含一个或多个匹配规则，用于标识与以下一个或多个实体相关的网络流量：

- 存储分段
- Tenants
- 子网（包含客户端的 IPv4 子网）
- 端点（负载平衡器端点）

StorageGRID 会根据规则的目标监控与策略中任何规则匹配的流量。与某个策略的任何规则匹配的任何流量均由该策略处理。相反，您可以设置规则来匹配除指定实体之外的所有流量。

您也可以根据以下参数为策略设置限制：

- 中的聚合带宽
- 聚合带宽不足
- 并发读取请求
- 并发写入请求
- 每个请求的带宽
- 每个请求的带宽不足
- 读取请求速率
- 写入请求速率

> 您可以创建策略来限制聚合带宽或限制每个请求的带宽。但是， StorageGRID 不能同时限制这两种类型的带宽。聚合带宽限制可能会对非受限流量产生额外的轻微性能影响。

流量限制

创建流量分类策略后、流量将根据您设置的规则和限制类型进行限制。对于聚合或每个请求的带宽限制，请求将以您设置的速率传入或移出。StorageGRID 只能强制执行一个速度，因此，按匹配器类型强制执行最具体的策略匹配。对于所有其他限制类型，客户端请求会延迟 250 毫秒，对于超过任何匹配策略限制的请求，客户端请求会收到 503 个响应速度较慢的响应。

在网格管理器中，您可以查看流量图表并验证策略是否正在强制实施预期的流量限制。

将流量分类策略与SLA结合使用

您可以将流量分类策略与容量限制和数据保护结合使用来实施服务级别协议（ SLA ），这些协议提供了有关容量，数据保护和性能的具体信息。

每个负载平衡器都会实施流量分类限制。如果流量同时分布在多个负载平衡器上，则总最大速率是您指定的速率限制的倍数。

以下示例显示了一个 SLA 的三个层。您可以创建流量分类策略以实现每个 SLA 层的性能目标。

服务级别层	**Capacity**	数据保护	性能	成本
金牌	允许 1 PB 存储	3 复制 ILM 规则	25 K 请求 / 秒 5 GB/ 秒（ 40 Gbps ）带宽	每月 $$
银牌	允许使用 250 TB 存储	2 复制 ILM 规则	每秒 10 K 个请求 1.25 GB/ 秒（ 10 Gbps ）带宽	每月 $$
铜牌	允许 100 TB 存储	2 复制 ILM 规则	5 K 请求 / 秒 1 GB/ 秒（ 8 Gbps ）带宽	每月 $

创建流量分类策略

如果要按分段，租户， IP 子网或负载平衡器端点监控网络流量，并可选择限制此流量，则可以创建流量分类策略。您也可以根据带宽，并发请求数或请求率为策略设置限制。

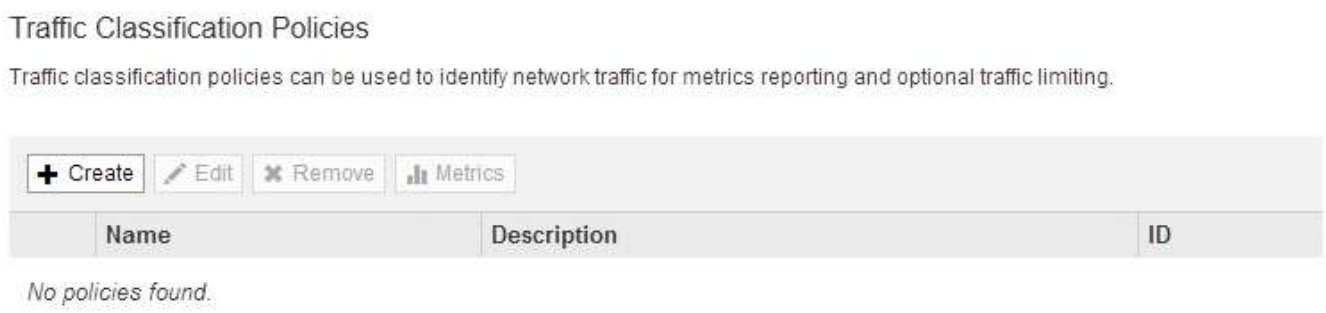
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。
- 您必须已创建要匹配的任何负载平衡器端点。
- 您必须已创建要匹配的任何租户。

步骤

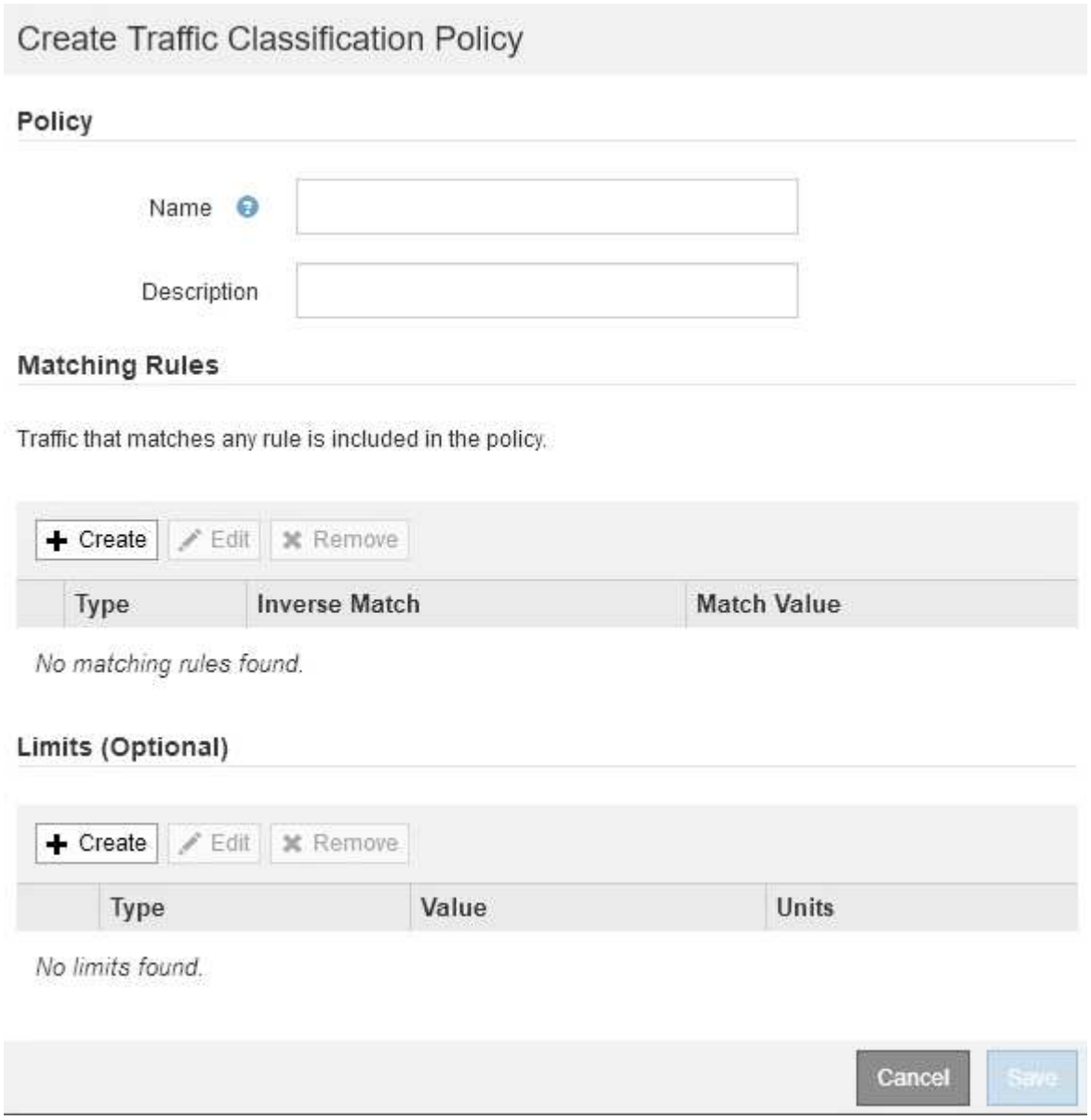
1. 选择*配置*>*网络设置*>*流量分类*。

   此时将显示 " 流量分类策略 " 页面。



2. 单击 * 创建 * 。

   此时将显示创建流量分类策略对话框。



3. 在 * 名称 * 字段中，输入策略的名称。

   输入描述性名称，以便识别策略。

4. 也可以在 * 问题描述 * 字段中为策略添加问题描述 。

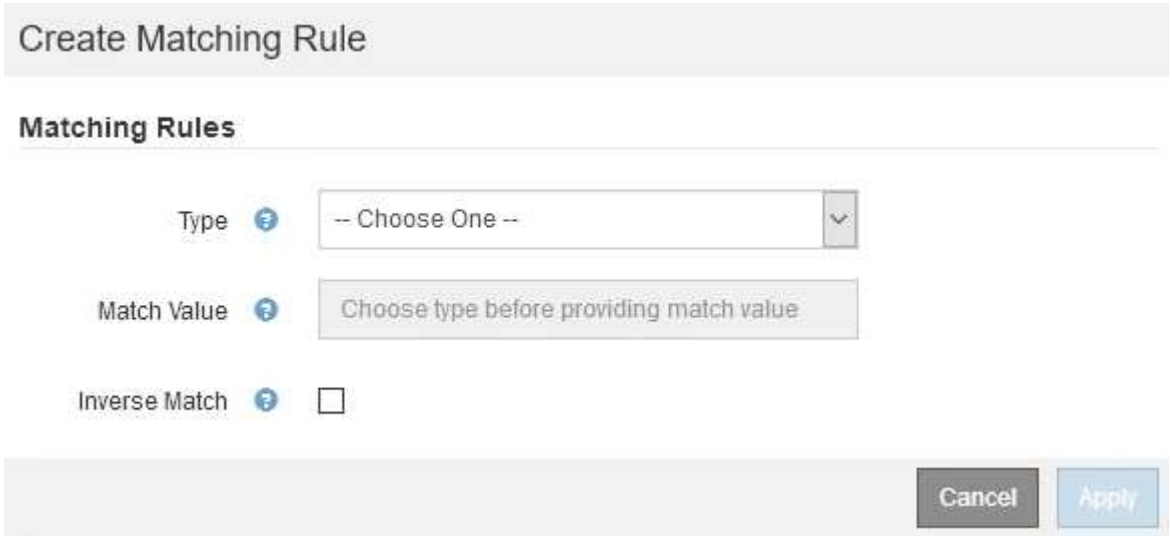
   例如，描述此流量分类策略适用场景 及其限制。

5. 为策略创建一个或多个匹配规则。

   匹配规则控制哪些实体将受此流量分类策略的影响。例如，如果要将此策略应用于特定租户的网络流量，请选择租户。或者，如果要将此策略应用于特定负载平衡器端点上的网络流量，请选择 Endpoint 。

   a. 单击*匹配规则*部分中的*创建*。

      此时将显示创建匹配规则对话框。



   b. 从 * 类型 * 下拉列表中，选择要包含在匹配规则中的实体类型。

   c. 在 * 匹配值 * 字段中，根据您选择的实体类型输入匹配值。

      - 存储分段：输入存储分段名称。
      - Bucket Rex ： 输入用于匹配一组存储分段名称的正则表达式。

        正则表达式已取消锁定。使用 ｛caret｝ 定位点在存储分段名称开头匹配，并使用 $ 定位点在存储分段名称末尾匹配。

      - CIDR ： 以 CIDR 表示法输入与所需子网匹配的 IPv4 子网。
      - Endpoint ： 从现有端点列表中选择一个端点。这些是您在负载平衡器端点页面上定义的负载平衡器端点。
      - 租户：从现有租户列表中选择一个租户。租户匹配取决于所访问的存储分段的所有权。对存储分段的匿名访问与拥有存储分段的租户匹配。

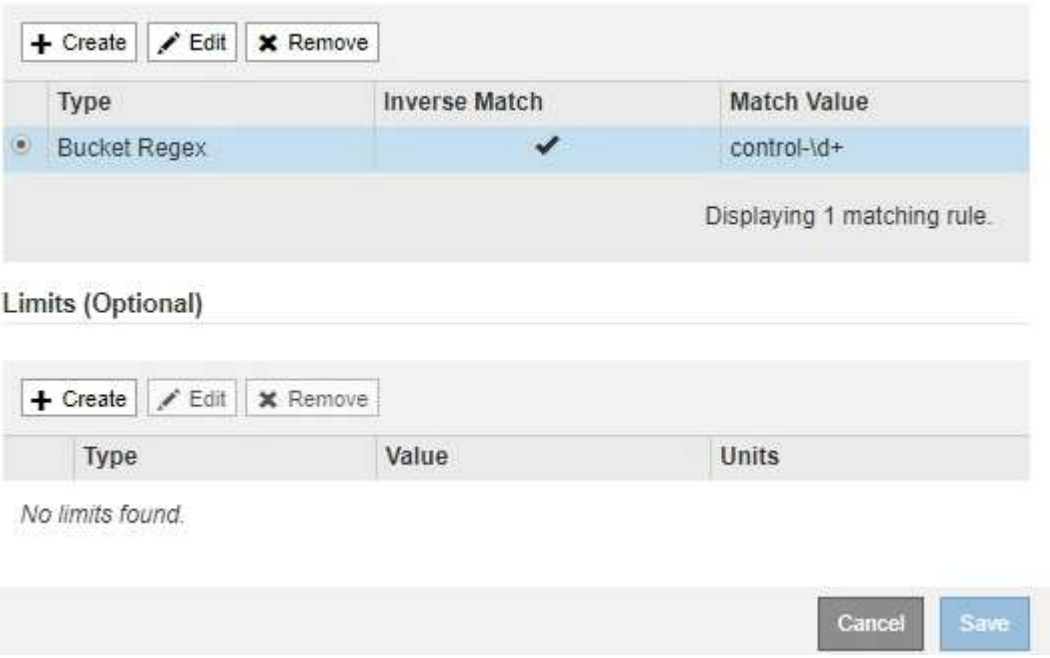
   d. 如果要匹配与刚刚定义的类型和匹配值一致的所有网络流量 _except _ 流量，请选中 * 反向 * 复选框。否则，请取消选中此复选框。

      例如，如果要将此策略应用于除一个负载平衡器端点之外的所有其他端点，请指定要排除的负载平衡器端点，然后选择 * 反向 * 。

对于包含多个匹配器且至少有一个是反向匹配器的策略，请注意不要创建与所有请求匹配的策略。

e. 单击 * 应用 * 。

此时将创建此规则，并将其列在匹配规则表中。



a. 对要为策略创建的每个规则重复上述步骤。

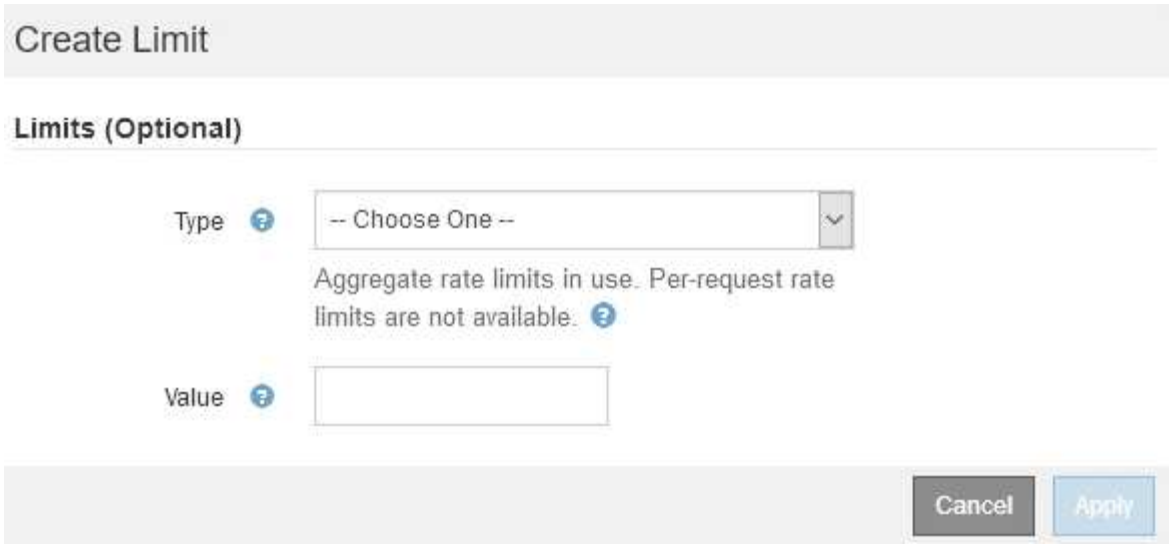
与任何规则匹配的流量由策略处理。

6. 也可以为策略创建限制。

即使不创建限制， StorageGRID 也会收集指标，以便监控与策略匹配的网络流量。

a. 单击*限制*部分中的*创建*。

此时将显示创建限制对话框。



b. 从 * 类型 * 下拉列表中，选择要应用于策略的限制类型。

在以下列表中， * 输入 * 是指从 S3 或 Swift 客户端到 StorageGRID 负载平衡器的流量， * 输出 * 是指从负载平衡器到 S3 或 Swift 客户端的流量。

- 中的聚合带宽
- 聚合带宽不足
- 并发读取请求
- 并发写入请求
- 每个请求的带宽
- 每个请求的带宽不足
- 读取请求速率
- 写入请求速率

> 您可以创建策略来限制聚合带宽或限制每个请求的带宽。但是， StorageGRID 不能同时限制这两种类型的带宽。聚合带宽限制可能会对非受限流量产生额外的轻微性能影响。

对于带宽限制， StorageGRID 会应用与设置的限制类型最匹配的策略。例如，如果您的策略仅限制一个方向的流量，则相反方向的流量将是无限制的，即使存在与具有带宽限制的其他策略匹配的流量也是如此。StorageGRID 按以下顺序实施 "`最佳` " 匹配的带宽限制：

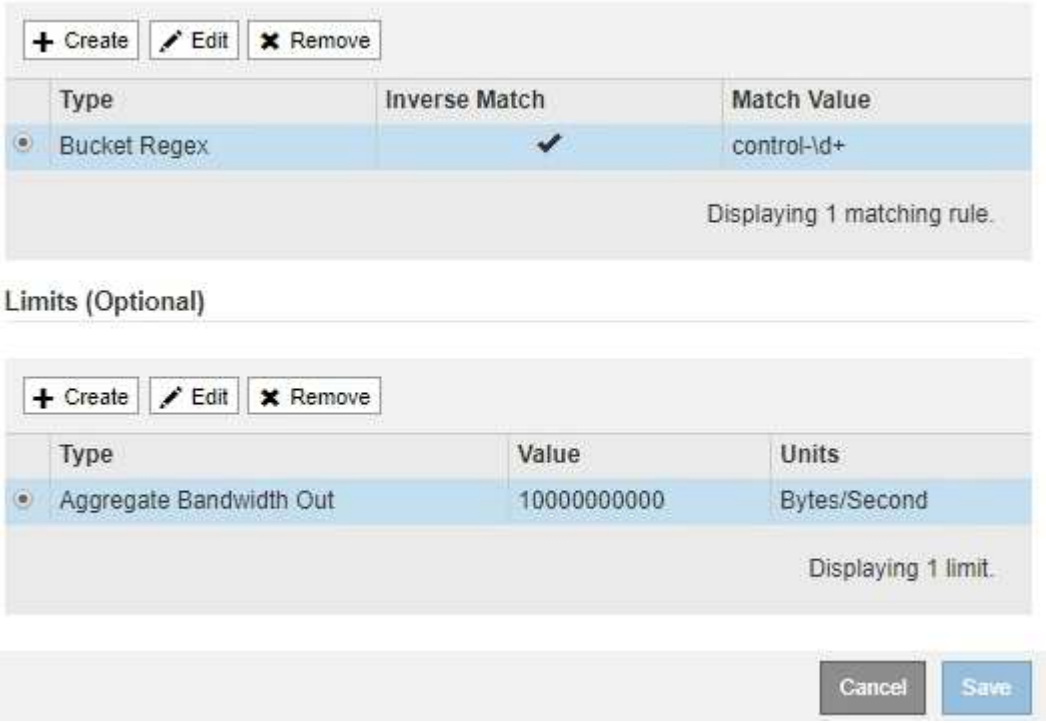
- 确切的 IP 地址（ /32 掩码）
- 确切的存储分段名称
- 分段正则表达式
- 租户
- 端点
- 非精确的 CIDR 匹配项（非 /32 ）
- 反向匹配

c. 在 * 值 * 字段中，输入所选限制类型的数值。

选择限制时，系统将显示预期单位。

d. 单击 * 应用 * 。

此时将创建此限制，并将其列在限制表中。



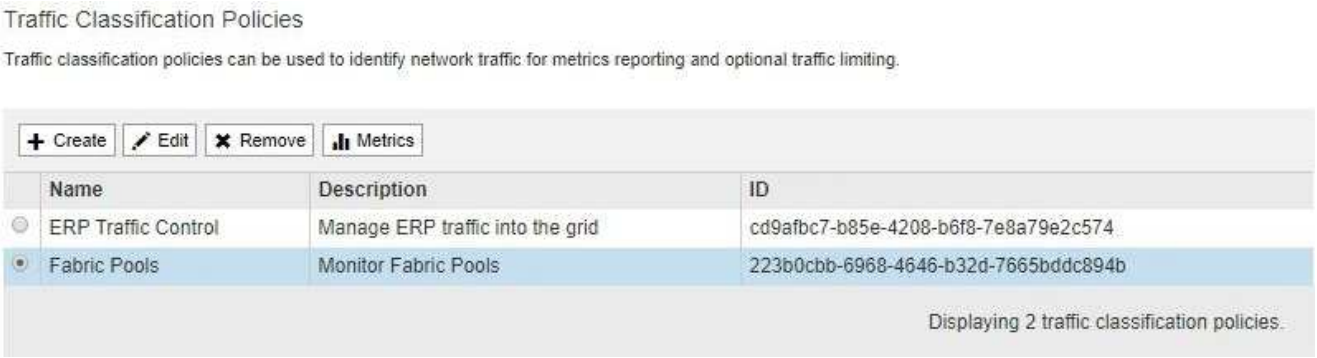
e. 对要添加到策略中的每个限制重复上述步骤。

例如，如果要为 SLA 层创建 40 Gbps 带宽限制，请创建 " 聚合带宽限制 " 和 " 聚合带宽超限 " ，并将每个限制设置为 40 Gbps 。

要将每秒兆字节数转换为每秒千兆位数，请乘以 8 。例如， 125 MB/ 秒相当于 1 ， 000 Mbps 或 1 Gbps 。

7. 创建完规则和限制后、单击*保存*。

此策略将保存并列出在 " 流量分类策略 " 表中。



现在， S3 和 Swift 客户端流量将根据流量分类策略进行处理。您可以查看流量图表并验证策略是否正在强制实施预期的流量限制。

相关信息

"管理负载平衡"

"查看网络流量指标"

编辑流量分类策略

您可以编辑流量分类策略以更改其名称或问题描述 ，或者创建，编辑或删除此策略的任何规则或限制。

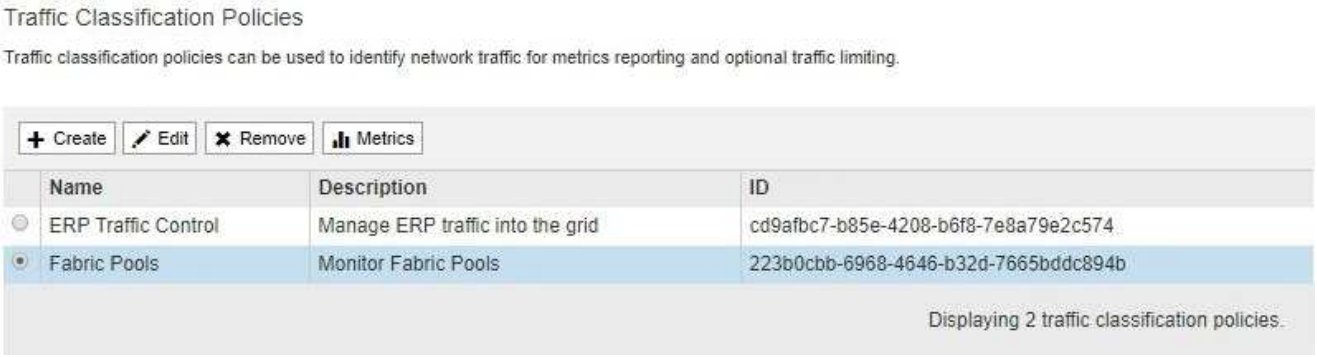
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。

步骤

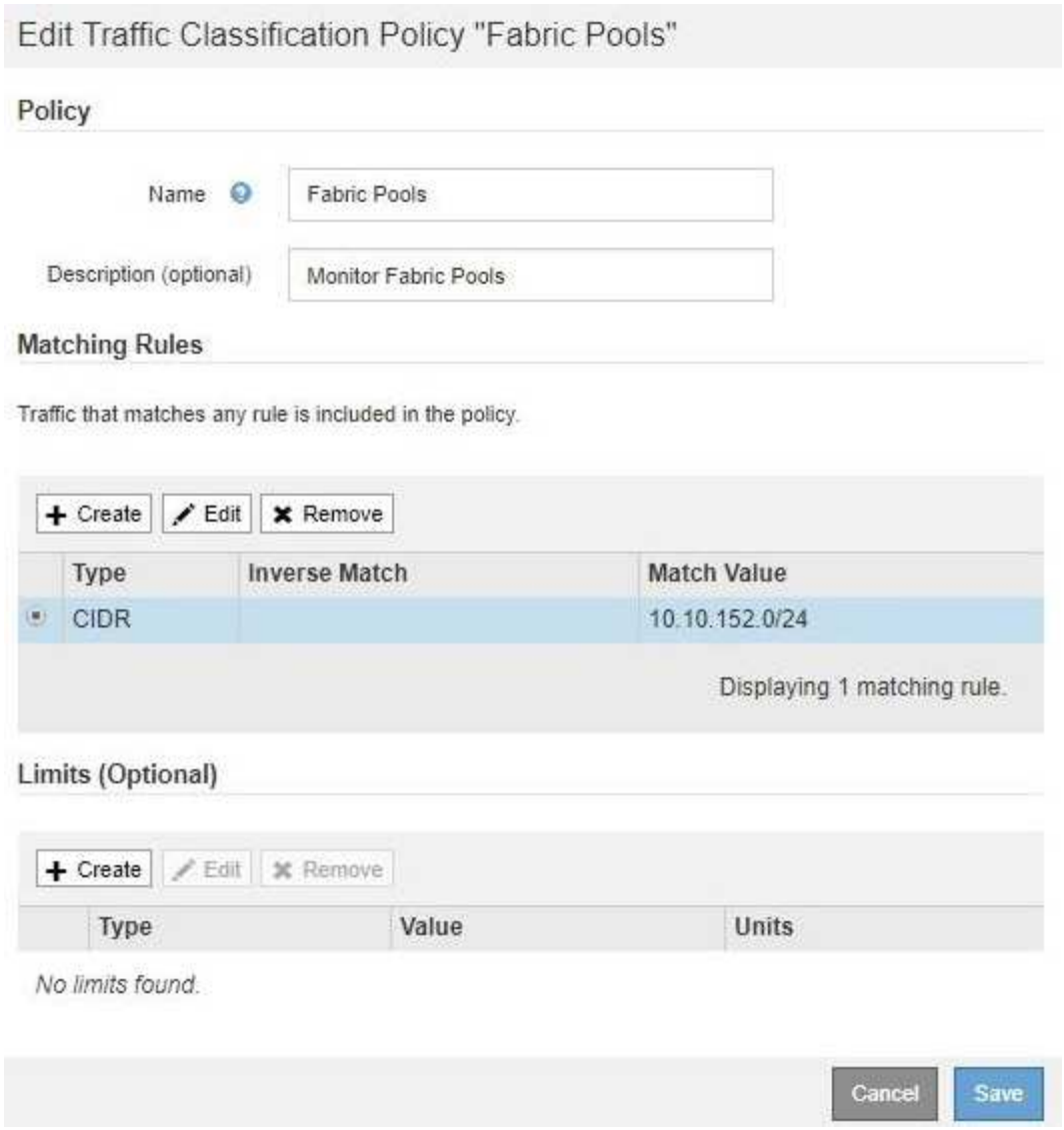
1. 选择*配置*>*网络设置*>*流量分类*。

   此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



2. 选择要编辑的策略左侧的单选按钮。
3. 单击 * 编辑 * 。

   此时将显示编辑流量分类策略对话框。



4. 根据需要创建，编辑或删除匹配的规则和限制。
   a. 要创建匹配的规则或限制、请单击*创建*、然后按照说明创建规则或创建限制。
   b. 要编辑匹配的规则或限制、请选择规则或限制的单选按钮、单击*匹配规则*部分或*限制*部分中的*编辑*、然后按照说明创建规则或创建限制。
   c. 要删除匹配的规则或限制、请选择该规则或限制的单选按钮、然后单击*删除*。然后、单击*确定*以确认要删除此规则或限制。
5. 创建或编辑规则或限制后、单击*应用*。
6. 编辑完策略后、单击*保存*。

   您对策略所做的更改将被保存，网络流量现在将根据流量分类策略进行处理。您可以查看流量图表并验证策略是否正在强制实施预期的流量限制。

删除流量分类策略

如果您不再需要流量分类策略，可以将其删除。

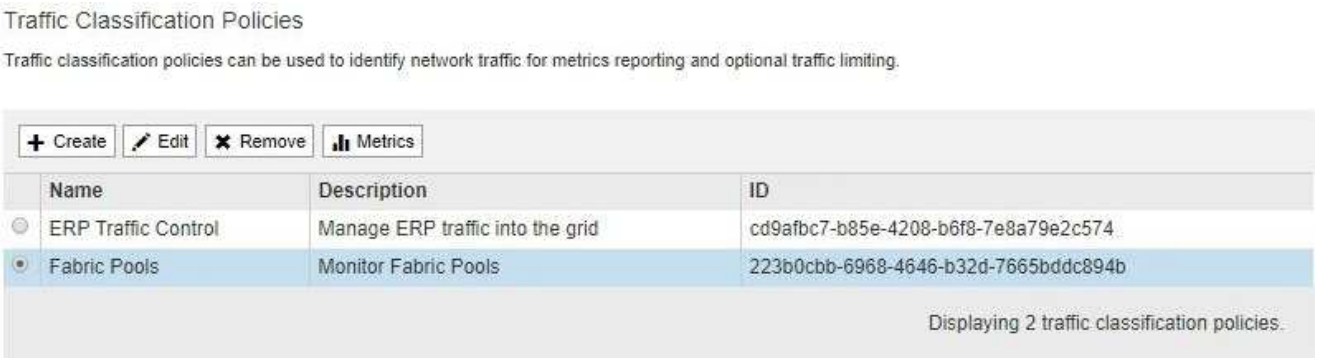
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。

步骤

1. 选择*配置*>*网络设置*>*流量分类*。

   此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



2. 选择要删除的策略左侧的单选按钮。
3. 单击 * 删除 * 。

   此时将显示警告对话框。

4. 单击*确定*确认要删除此策略。

   此策略将被删除。

查看网络流量指标

您可以通过查看 " 流量分类策略 " 页面上的图形来监控网络流量。

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 root 访问权限。

关于此任务

对于任何现有流量分类策略，您可以查看负载平衡器服务的指标，以确定该策略是否成功限制网络中的流量。图

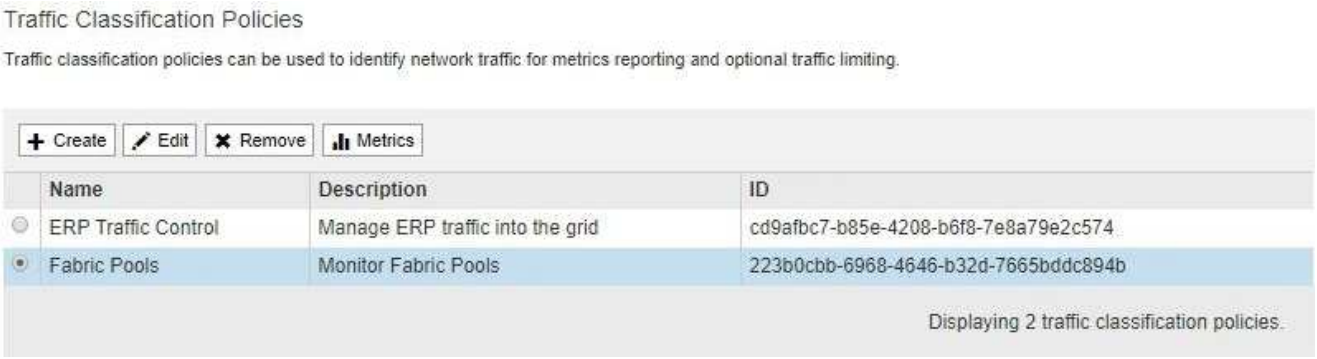
形中的数据可以帮助您确定是否需要调整策略。

即使没有为流量分类策略设置限制，也会收集指标，并且图形可提供有用的信息来了解流量趋势。

步骤

1. 选择*配置*>*网络设置*>*流量分类*。

   此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



2. 选择要查看指标的策略左侧的单选按钮。
3. 单击*指标*。

   此时将打开一个新浏览器窗口，并显示流量分类策略图形。这些图形仅显示与选定策略匹配的流量的指标。

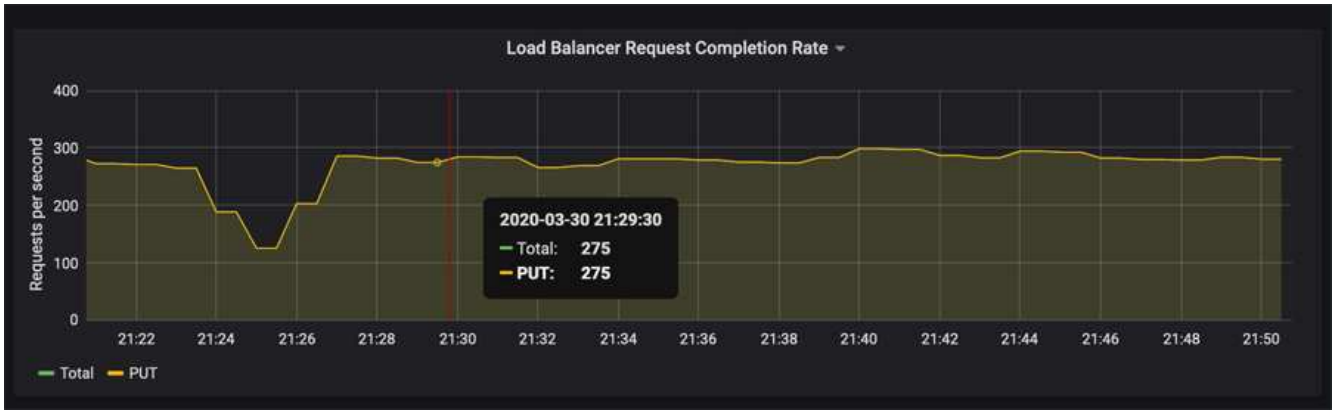
   您可以使用 * 策略 * 下拉列表选择其他要查看的策略。

   网页上包含以下图形。

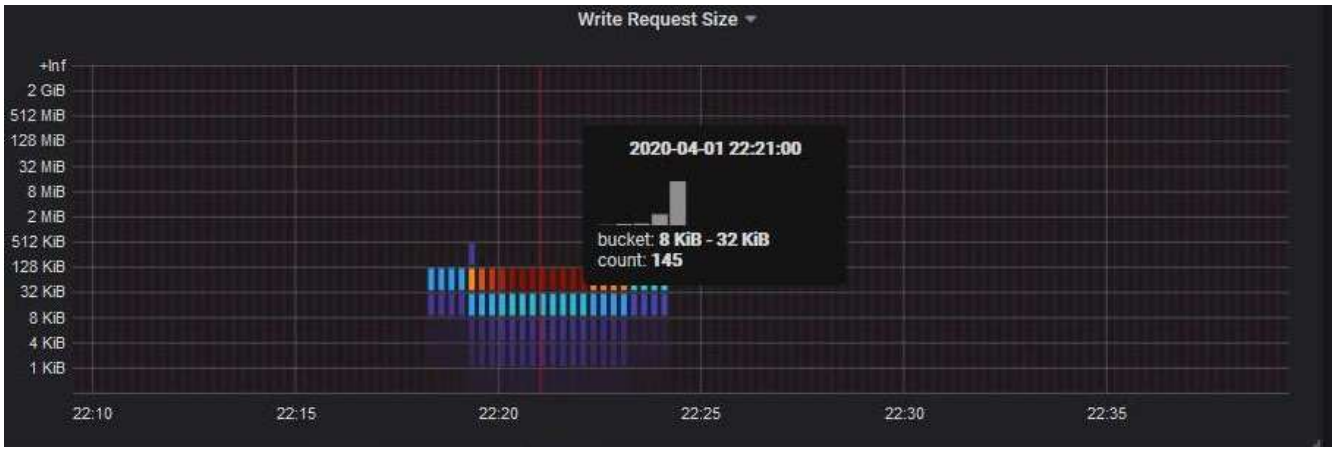
   - 负载平衡器请求流量：此图提供负载平衡器端点与发出请求的客户端之间传输的数据吞吐量的 3 分钟移动平均值，以每秒位数为单位。

- 负载平衡器请求完成率：此图按请求类型（ GET ， PUT ， HEAD 和 DELETE ）细分，提供每秒已完成请求数的 3 分钟移动平均值。验证新请求的标头后，此值将更新。
- 错误响应率：此图提供了每秒返回给客户端的错误响应数的 3 分钟移动平均值，并按错误响应代码进行细分。
- 平均请求持续时间（非错误）：此图提供了按请求类型（ GET ， PUT ， HEAD 和 DELETE ）细分的 3 分钟移动平均请求持续时间。每个请求持续时间从负载平衡器服务解析请求标头时开始，到将完整的响应正文返回给客户端时结束。
- 按对象大小划分的写入请求速率：此热图根据对象大小提供 3 分钟的写入请求完成速率移动平均值。在这种情况下，写入请求仅指 PUT 请求。
- 按对象大小划分的读取请求速率：此热图提供了根据对象大小完成读取请求的 3 分钟移动平均值。在这种情况下，读取请求仅指获取请求。热图中的颜色表示各个图形中对象大小的相对频率。较冷的颜色（例如紫色和蓝色）表示相对速率较低，较热的颜色（例如橙色和红色）表示相对速率较高。

4. 将光标悬停在折线图上可查看该图特定部分的值弹出窗口。



5. 将光标悬停在热图上可看到一个弹出窗口，其中显示样本的日期和时间，聚合到计数中的对象大小以及该时间段内的每秒请求数。



6. 使用左上角的 * 策略 * 下拉列表选择其他策略。

   此时将显示选定策略的图形。

7. 或者、也可以从*支持*菜单访问这些图形。
   a. 选择*支持*>*工具*>*指标*。

b. 在页面的 * Grafan* 部分中，选择 * 流量分类策略 * 。

c. 从页面左上角的下拉列表中选择策略。

流量分类策略通过其 ID 进行标识。策略 ID 会列在 " 流量分类策略 " 页面上。

8. 分析图形以确定策略限制流量的频率以及是否需要调整策略。

相关信息

"监控和放大；故障排除"

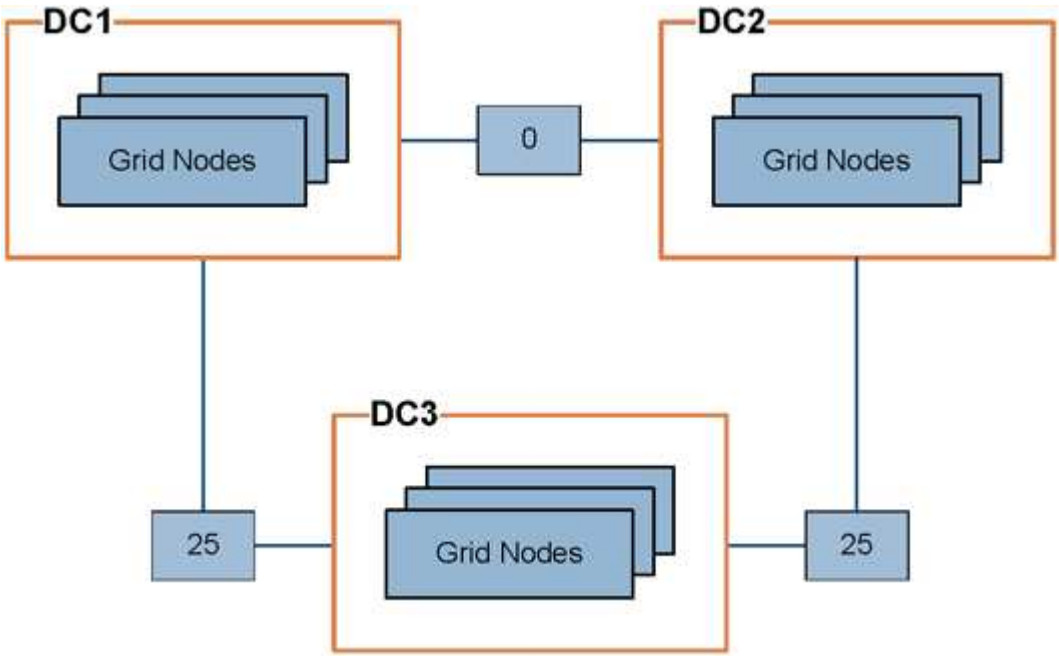
链路成本是多少

链路成本可用于确定存在两个或更多数据中心站点时哪个数据中心站点提供请求的服务的优先级。您可以调整链路成本以反映站点之间的延迟。

- 链接成本用于确定用于实现对象检索的对象副本的优先级。
- 网格管理 API 和租户管理 API 使用链路成本来确定要使用的内部 StorageGRID 服务。
- 链路成本由网关节点上的CLB服务用于指导客户端连接。

CLB 服务已弃用。

此图显示了一个三站点网格，其中在站点之间配置了链路成本：



- 网关节点上的 CLB 服务会将客户端连接平均分布到同一数据中心站点上的所有存储节点以及任何数据中心站点，链路成本为 0 。

  在此示例中，数据中心站点 1 （ DC1 ）的网关节点会将客户端连接平均分布到 DC1 的存储节点和 DC2 的存储节点。DC3 上的网关节点仅向 DC3 上的存储节点发送客户端连接。

- 在检索作为多个复制副本存在的对象时， StorageGRID 会在链路成本最低的数据中心检索此副本。

  在此示例中，如果 DC2 上的客户端应用程序检索存储在 DC1 和 DC3 上的对象，则会从 DC1 检索该对象，因为从 DC1 到 D2 的链路成本为 0 ，低于从 DC3 到 DC2 的链路成本（ 25 ）。

链路成本是任意的相对数字，没有特定的度量单位。例如，使用链路成本 50 比使用链路成本 25 更低。下表显示了常用链路成本。

链接。	链路成本	注释：
物理数据中心站点之间	25 （默认）	通过 WAN 链路连接的数据中心。
位于同一物理位置的逻辑数据中心站点之间	0	逻辑数据中心位于通过 LAN 连接的同一物理建筑或园区中。

相关信息

"负载平衡的工作原理— CLB 服务"

更新链路成本

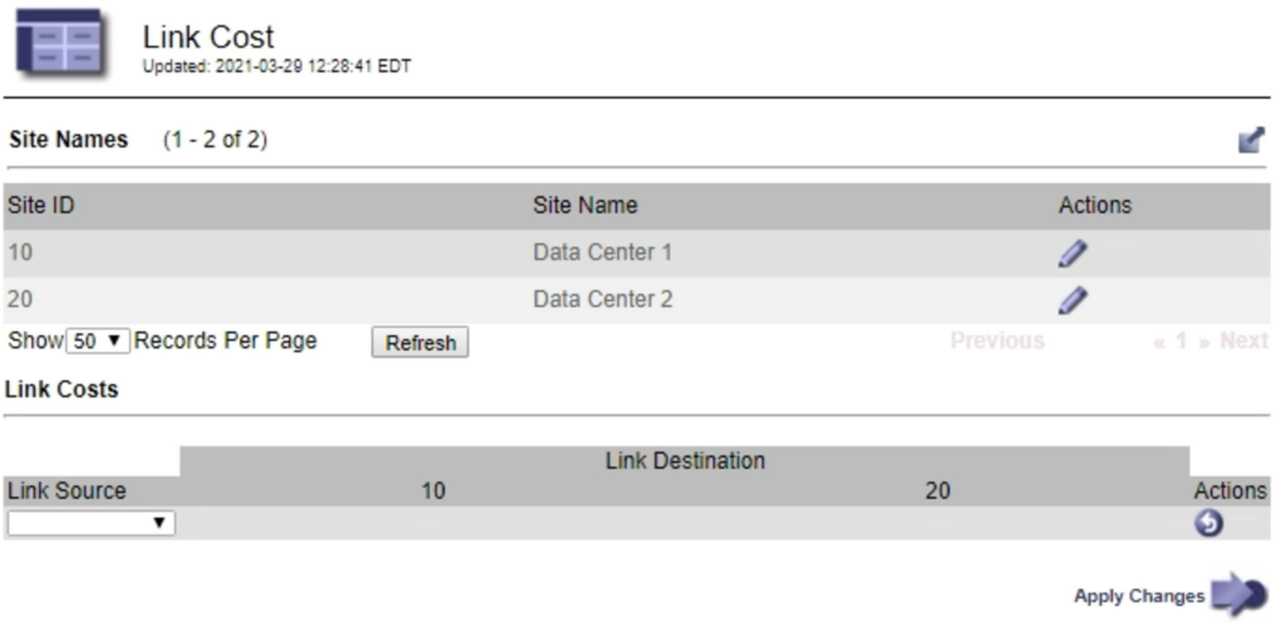
您可以更新数据中心站点之间的链路成本，以反映站点之间的延迟。

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。
- 您必须具有网格拓扑页面配置权限。

步骤

1. 选择*配置*>*网络设置*>*链路成本*。



2. 在 * 链路源 * 下选择一个站点，然后在 * 链路目标 * 下输入一个介于 0 和 100 之间的成本值。

   如果源与目标相同，则无法更改链路成本。

   要取消更改、请单击  * 还原 * 。

3. 单击 * 应用更改 * 。

版权信息

商标信息