管理网络和连接
StorageGRID

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/storagegrid-116/admin/guidelines-for-storagegrid-networks.html on April 10, 2024. Always check docs.netapp.com for the latest.

目录

管理网络和连接 1
StorageGRID 网络准则 1
查看 IP 地址 2
支持传出 TLS 连接的密码 3
更改网络传输加密 4
管理流量分类策略 5
管理链路成本 18

管理网络和连接

StorageGRID 网络准则

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。

默认 StorageGRID 网络

默认情况下， StorageGRID 支持每个网格节点使用三个网络接口，从而可以根据您的安全和访问要求为每个网格节点配置网络。

有关网络拓扑的详细信息，请参见 网络连接准则。

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。

可选接口

您也可以向节点添加额外的接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 VLAN 接口 隔离属于不同应用程序或租户的流量。或者，您可能希望添加要在中使用的访问接口 高可用性（HA）组。

要添加中继或访问接口，请参见以下内容：

- * VMware （安装节点后） *： VMware： 向节点添加中继或访问接口
- * RHEL 或 CentOS （安装节点之前） *： 创建节点配置文件
- * Ubuntu 或 Debian （安装节点之前） *： 创建节点配置文件
- * RHEL， CentOS， Ubuntu 或 Debian （安装节点后） *： Linux： 向节点添加中继或访问接口

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

您将使用登录到网格管理器 支持的 Web 浏览器。

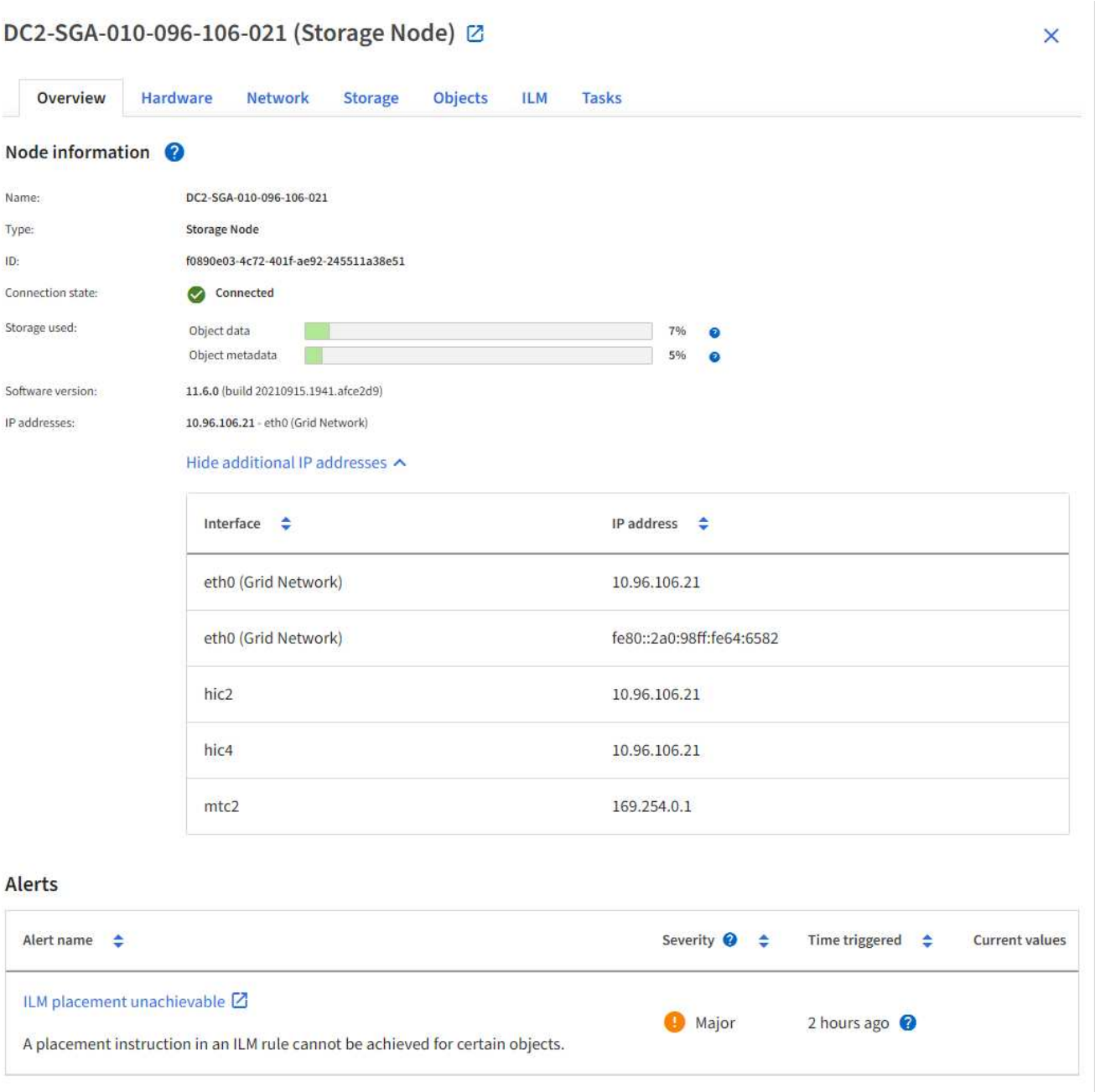
关于此任务

有关更改 IP 地址的信息，请参见 恢复和维护。

步骤

1. 选择 * 节点 * > * 网格节点 _* > * 概述 * 。
2. 选择 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。



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

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您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 * > * 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. 选择 * 保存 * 。

管理流量分类策略

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

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。

流量限制

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

限制值按负载平衡器强制实施。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。

> 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。

使用具有 **SLA** 的流量分类策略

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。
- 您已创建要匹配的任何负载平衡器端点。

- 您已创建要匹配的任何租户。

步骤

1. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

   此时将显示 " 流量分类策略 " 页面。

   Traffic Classification Policies

   Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

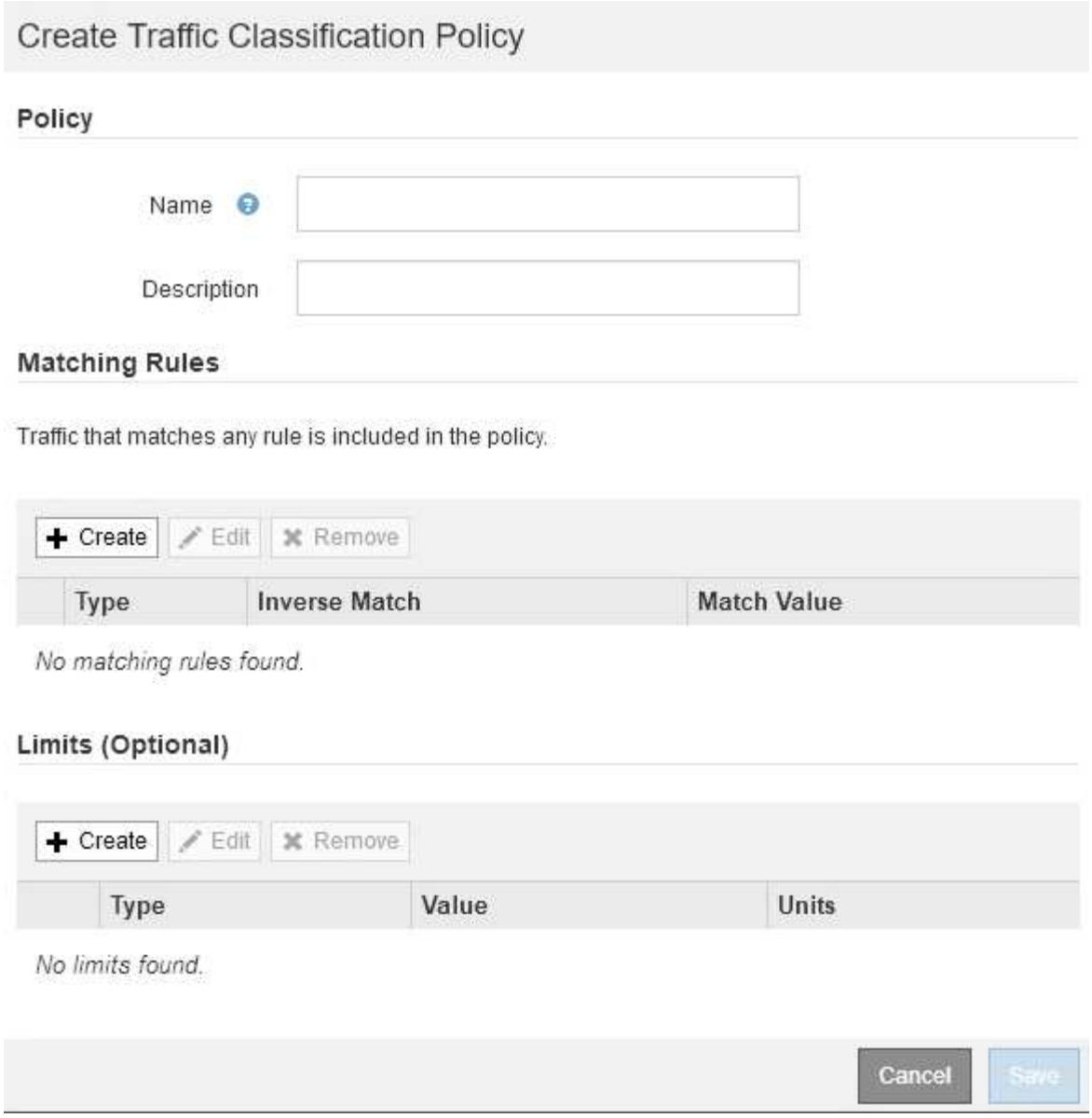
Create	Edit	Remove	Metrics

	Name	Description	ID

   No policies found.

2. 选择 * 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 。

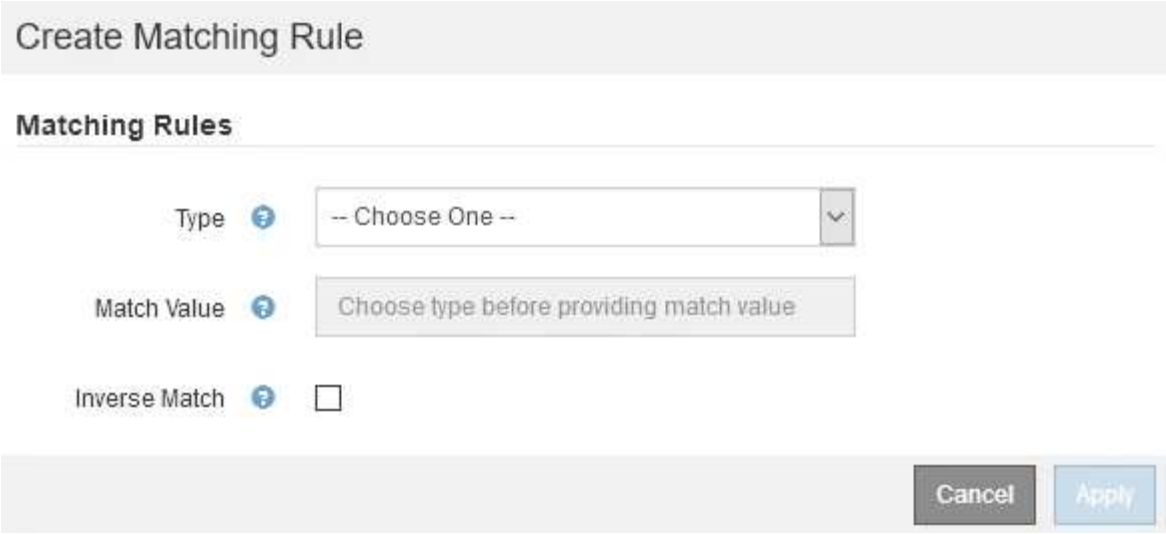
   例如，描述此流量分类策略适用场景 及其限制。

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. 在 * 匹配规则 * 部分中选择 * 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。请参见 配置负载平衡器端点。
- 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。

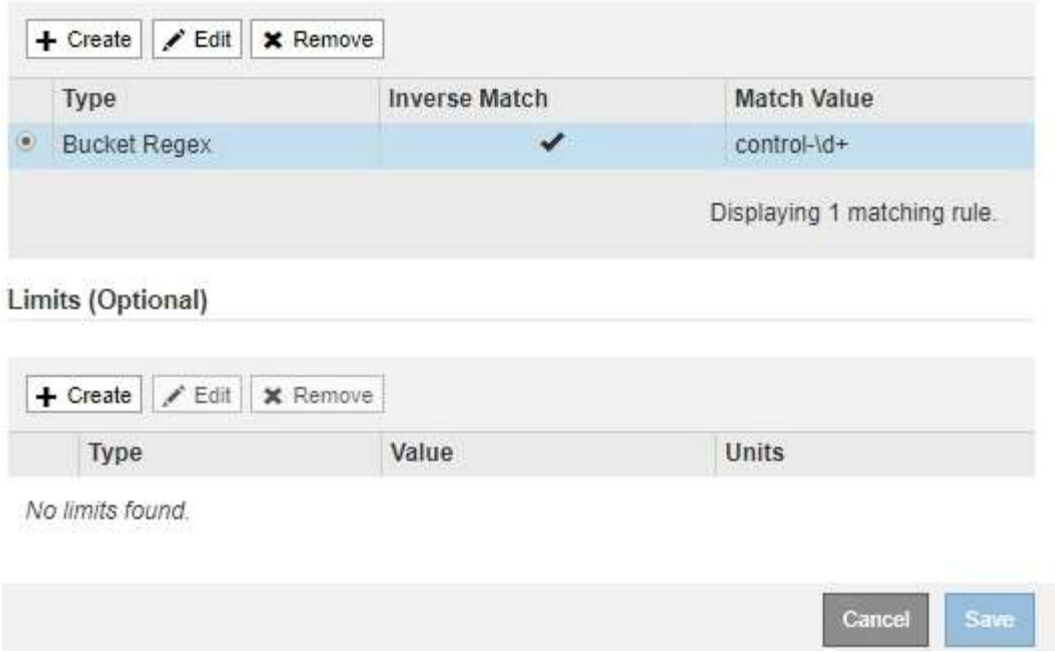
d. 如果要匹配与刚刚定义的类型和匹配值一致的所有网络流量 _except _ 流量，请选中 * 反向 * 复选框。否则，请取消选中此复选框。

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. 选择 * 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。

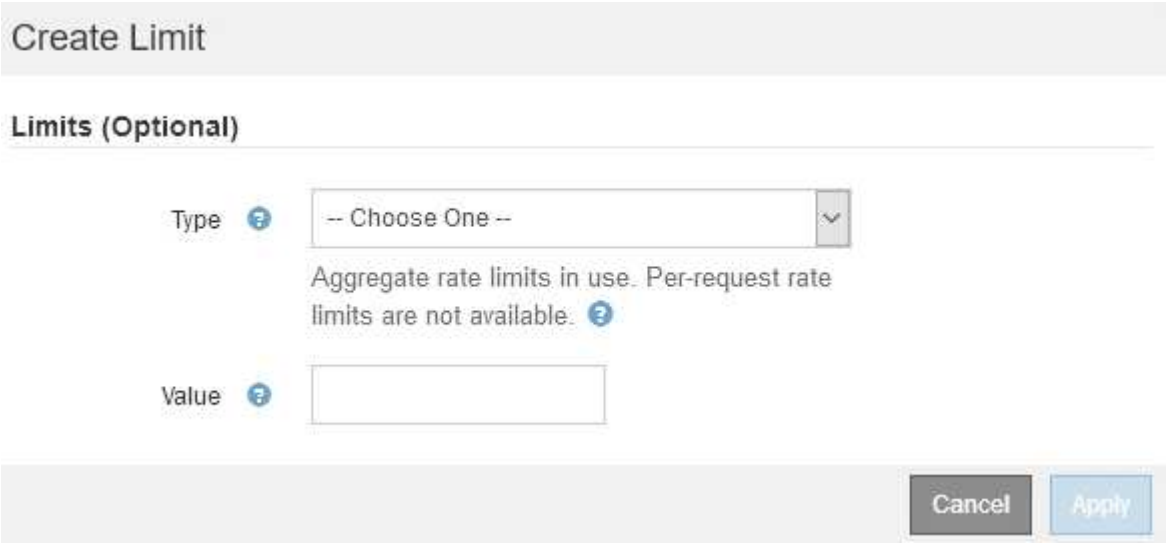
> 与任何规则匹配的流量由策略处理。

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. 在 * 限制 * 部分中选择 * 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：

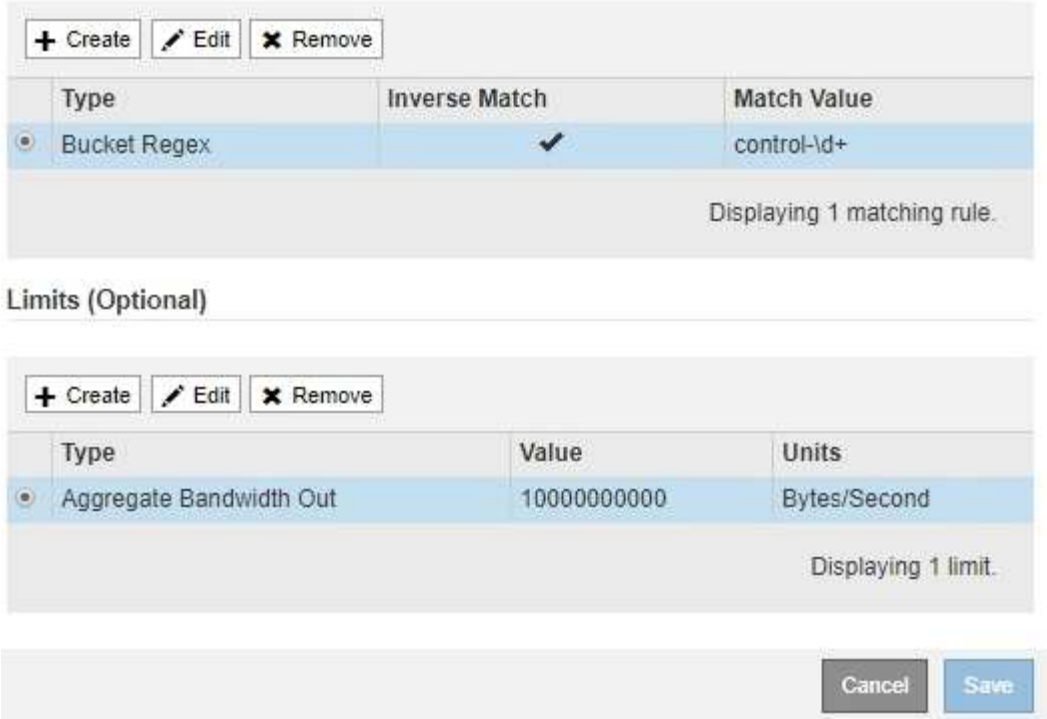
- 确切的 IP 地址（ /32 掩码）
- 确切的存储分段名称
- 分段正则表达式
- 租户
- 端点
- 非精确的 CIDR 匹配项（非 /32 ）
- 反向匹配

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. 选择 * 应用 * 。

此时将创建此限制，并将其列在限制表中。



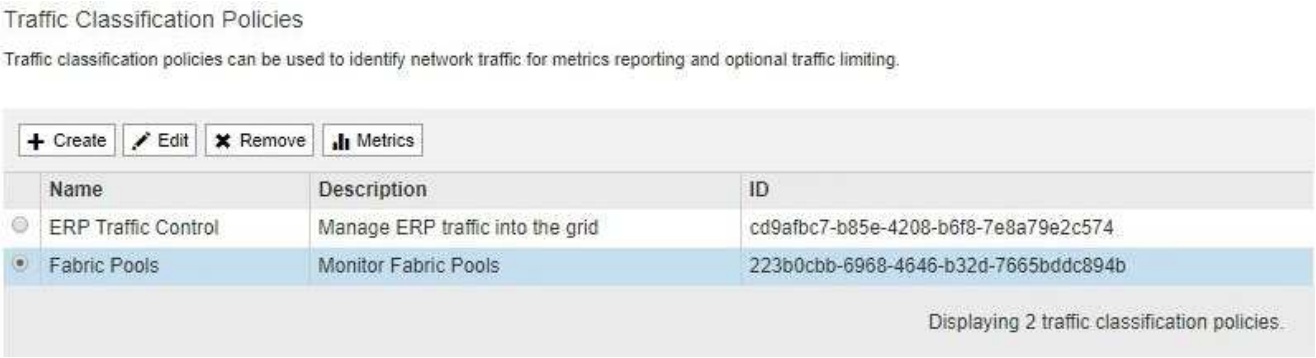
e. 对要添加到策略中的每个限制重复上述步骤。

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，请选择 * 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。请参见 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 * 配置 * > * 网络 * > * 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。

   Traffic Classification Policies

   Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

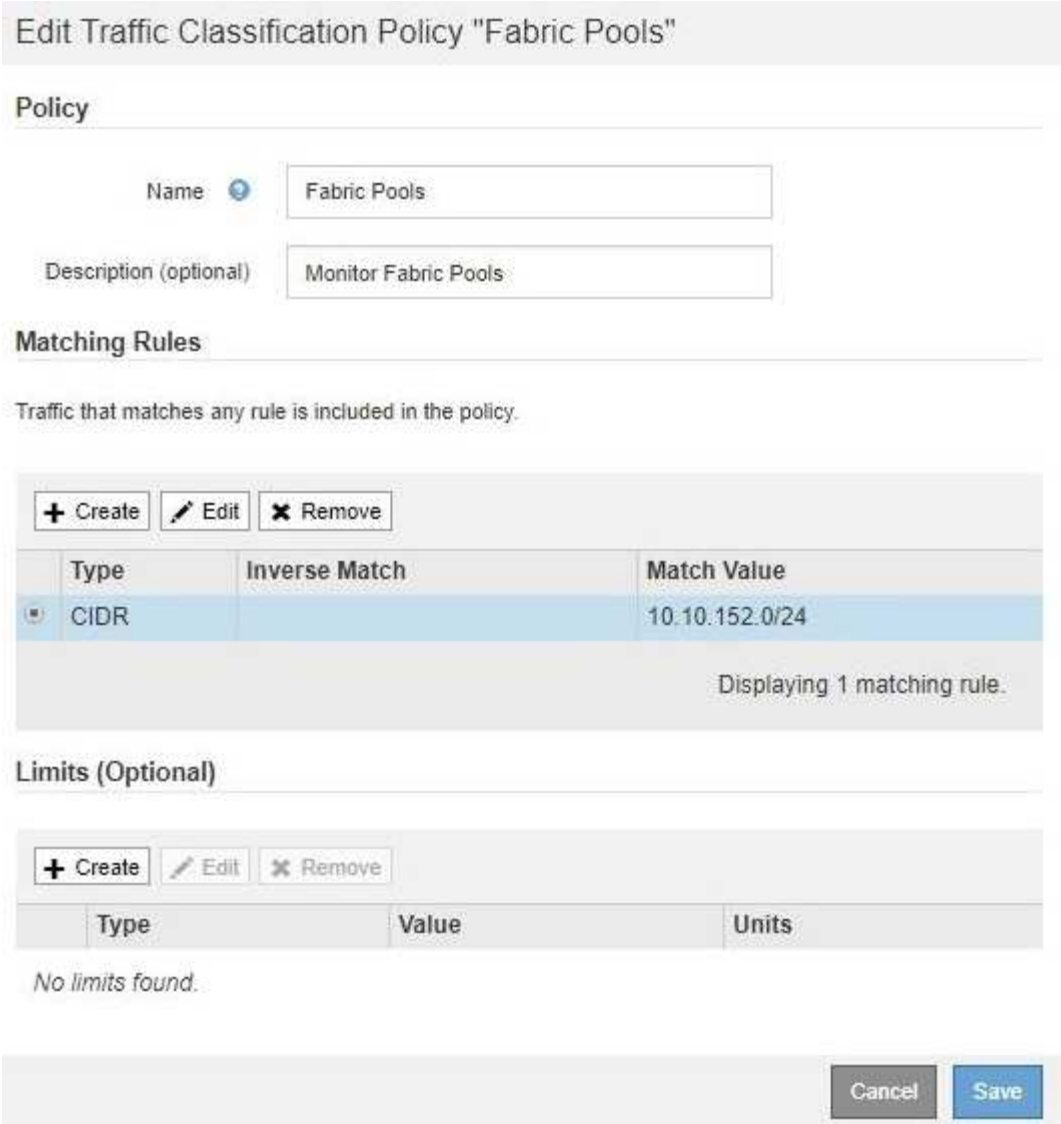
   + Create | Edit | Remove | Metrics

	Name	Description	ID
○	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
◉	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

   Displaying 2 traffic classification policies.

2. 选择要编辑的策略左侧的单选按钮。
3. 选择 * 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，请选择 * 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，在 * 匹配规则 * 部分或 * 限制 * 部分中选择 * 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，请选择规则或限制的单选按钮，然后选择 * 删除 * 。然后，选择 * 确定 * 以确认要删除规则或限制。
5. 创建或编辑规则或限制后，请选择 * 应用 * 。
6. 编辑完策略后，选择 * 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。

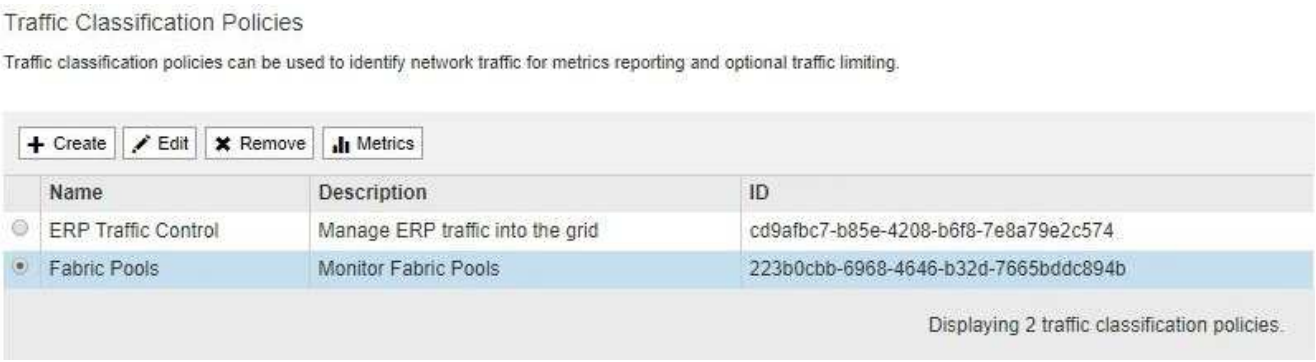
您需要的内容

- 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 * 配置 * > * 网络 * > * 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. 选择 * 删除 * 。

   此时将显示警告对话框。

4. 选择 * 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 访问权限或租户帐户权限。

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 * > * 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。

   Traffic Classification Policies

   Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

   + Create | Edit | Remove | Metrics

	Name	Description	ID
○	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
◉	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

   Displaying 2 traffic classification policies.

   > 如果您具有租户帐户权限，但没有 root 访问权限，则 * 创建 * ， * 编辑 * 和 * 删除 * 按钮将被禁用。

2. 选择要查看指标的策略左侧的单选按钮。
3. 选择 * 指标 * 。

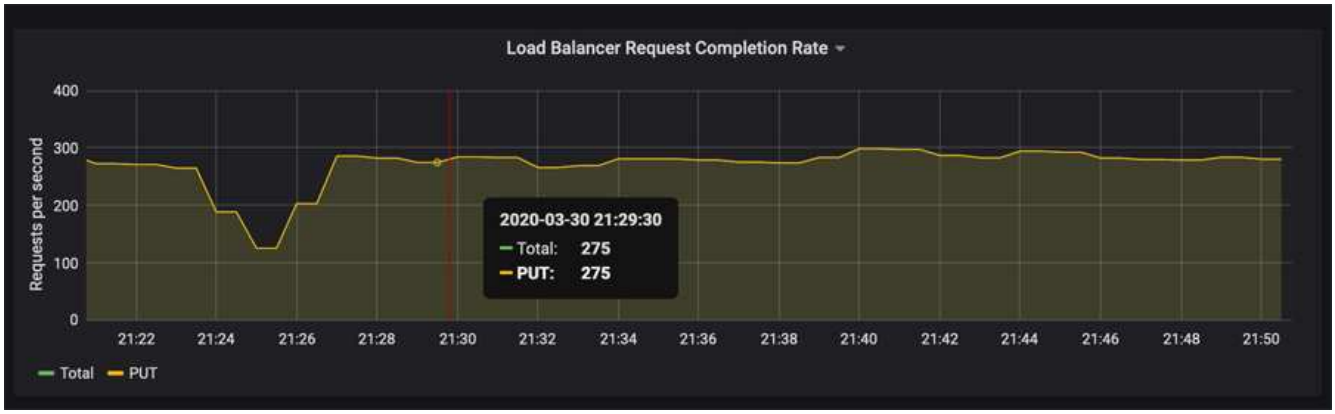
   此时将打开一个新浏览器窗口，并显示流量分类策略图形。这些图形仅显示与选定策略匹配的流量的指标。

   您可以使用 * 策略 * 下拉列表选择其他要查看的策略。

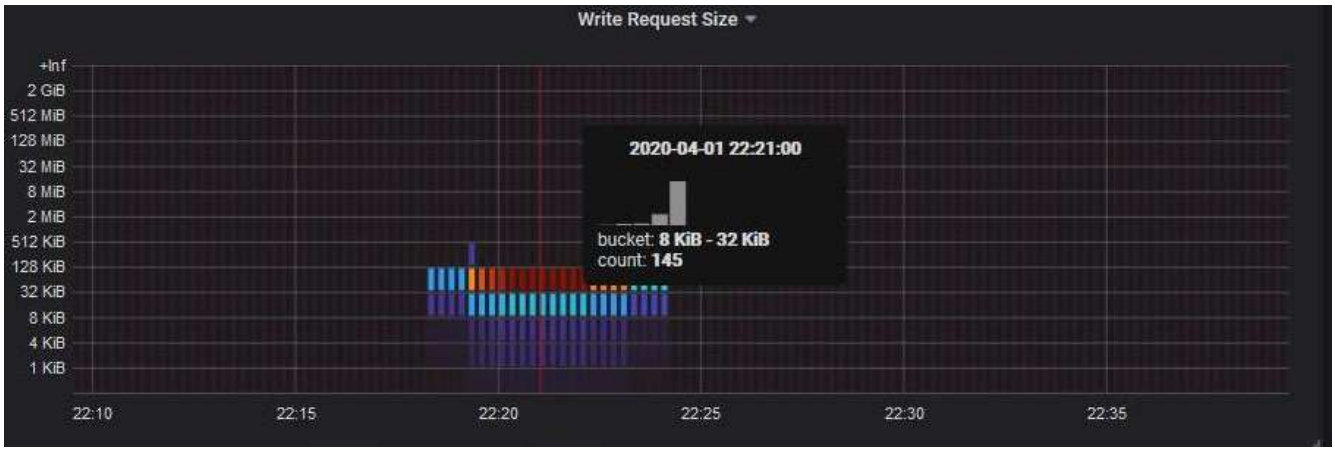
   网页上包含以下图形。

- 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

监控和故障排除

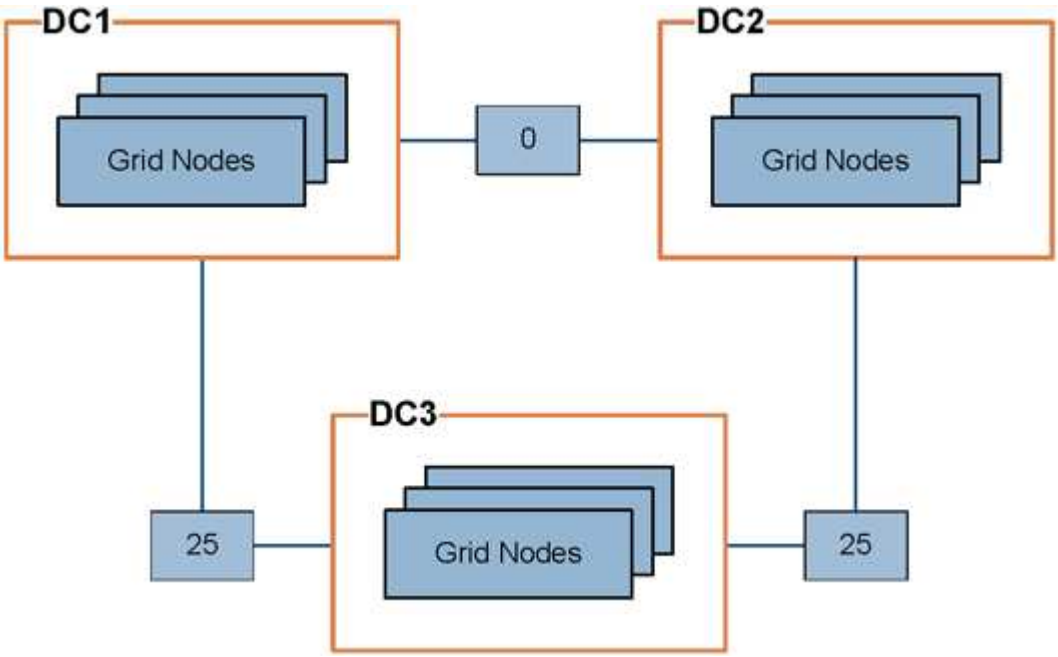
管理链路成本

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已弃用的连接负载平衡器（ CLB ）服务用于指导客户端连接。请参见 负载平衡的工作原理— CLB 服务。

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。

更新链路成本

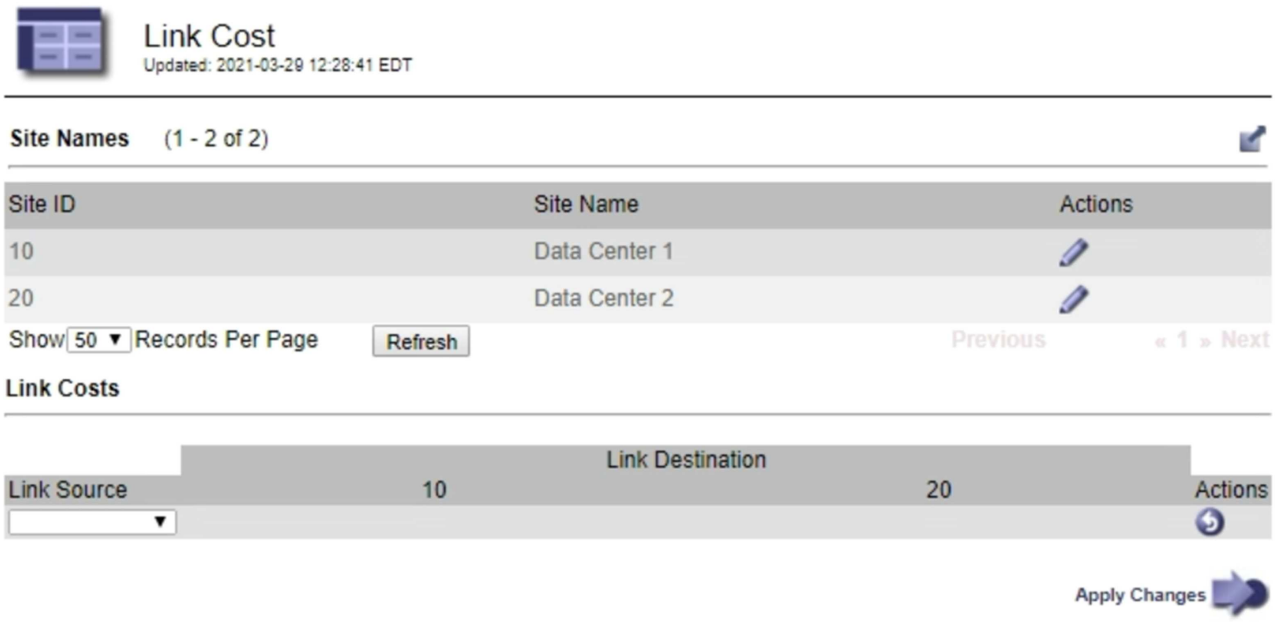
您可以更新数据中心站点之间的链路成本，以反映站点之间的延迟。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有网格拓扑页面配置权限。

步骤

1. 选择 * 配置 * > * 网络 * > * 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，请选择 * 还原 * 。

3. 选择 * 应用更改 * 。

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，本文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。