Managing traffic classification policies

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/us-en/storagegrid-115/admin/creating-traffic-classification-policies.html on October 03, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Managing traffic classification policies . . . 1
- Matching rules and optional limits . . . 1
- Traffic limiting . . . 1
- Using traffic classification policies with SLAs . . . 2
- Creating traffic classification policies . . . 2
- Editing a traffic classification policy . . . 8
- Deleting a traffic classification policy . . . 9
- Viewing network traffic metrics . . . 10

Managing traffic classification policies

To enhance your quality-of-service (QoS) offerings, you can create traffic classification policies to identify and monitor different types of network traffic. These policies can assist with traffic limiting and monitoring.

Traffic classification policies are applied to endpoints on the StorageGRID Load Balancer service for Gateway Nodes and Admin Nodes. To create traffic classification policies, you must have already created load balancer endpoints.

Matching rules and optional limits

Each traffic classification policy contains one or more matching rules to identify the network traffic related to one or more of the following entities:

- Buckets
- Tenants
- Subnets (IPv4 subnets containing the client)
- Endpoints (load balancer endpoints)

StorageGRID monitors traffic that matches any rule within the policy according to the objectives of the rule. Any traffic that matches any rule for a policy is handled by that policy. Conversely, you can set rules to match all traffic except a specified entity.

Optionally, you can set limits for a policy based on the following parameters:

- Aggregate Bandwidth In
- Aggregate Bandwidth Out
- Concurrent Read Requests
- Concurrent Write Requests
- Per-Request Bandwidth In
- Per-Request Bandwidth Out
- Read Request Rate
- Write Requests Rate

> ⓘ You can create policies to limit aggregate bandwidth or to limit per-request bandwidth. However, StorageGRID cannot limit both types of bandwidth at the same time. Aggregate bandwidth limits might impose an additional minor performance impact on non-limited traffic.

Traffic limiting

When you have created traffic classification policies, traffic is limited according to the type of rules and limits you set. For aggregate or per-request bandwidth limits, the requests stream in or out at the rate you set. StorageGRID can only enforce one speed, so the most specific policy match, by matcher type, is the one enforced. For all other limit types, client requests are delayed by 250 milliseconds and receive a 503 Slow Down response for requests that exceed any matching policy limit.

In the Grid Manager, you can view traffic charts and verify that the polices are enforcing the traffic limits you expect.

Using traffic classification policies with SLAs

You can use traffic classification policies in conjunction with capacity limits and data protection to enforce service-level agreements (SLAs) that provide specifics for capacity, data protection, and performance.

Traffic classification limits are implemented per load balancer. If traffic is distributed simultaneously across multiple load balancers, the total maximum rates are a multiple of the rate limits you specify.

The following example shows three tiers of an SLA. You can create traffic classification policies to achieve the performance objectives of each SLA tier.

Service Level Tier	Capacity	Data Protection	Performance	Cost
Gold	1 PB storage allowed	3 copy ILM rule	25 K requests/sec 5 GB/sec (40 Gbps) bandwidth	$$$ per month
Silver	250 TB storage allowed	2 copy ILM rule	10 K requests/sec 1.25 GB/sec (10 Gbps) bandwidth	$$ per month
Bronze	100 TB storage allowed	2 copy ILM rule	5 K requests/sec 1 GB/sec (8 Gbps) bandwidth	$ per month

Creating traffic classification policies

You create traffic classification policies if you want to monitor, and optionally limit, network traffic by bucket, tenant, IP subnet, or load balancer endpoint. Optionally, you can set limits for a policy based on bandwidth, the number of concurrent requests, or the request rate.

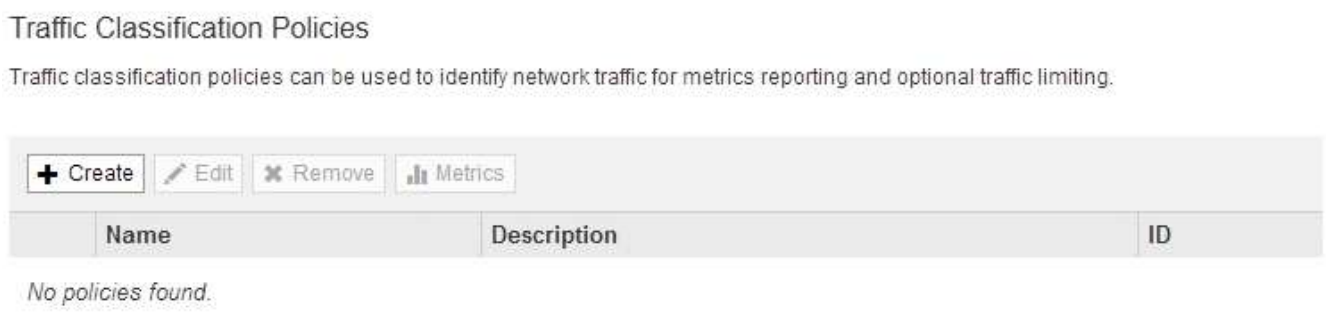
What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have the Root Access permission.
- You must have created any load balancer endpoints you want to match.
- You must have created any tenants you want to match.

Steps

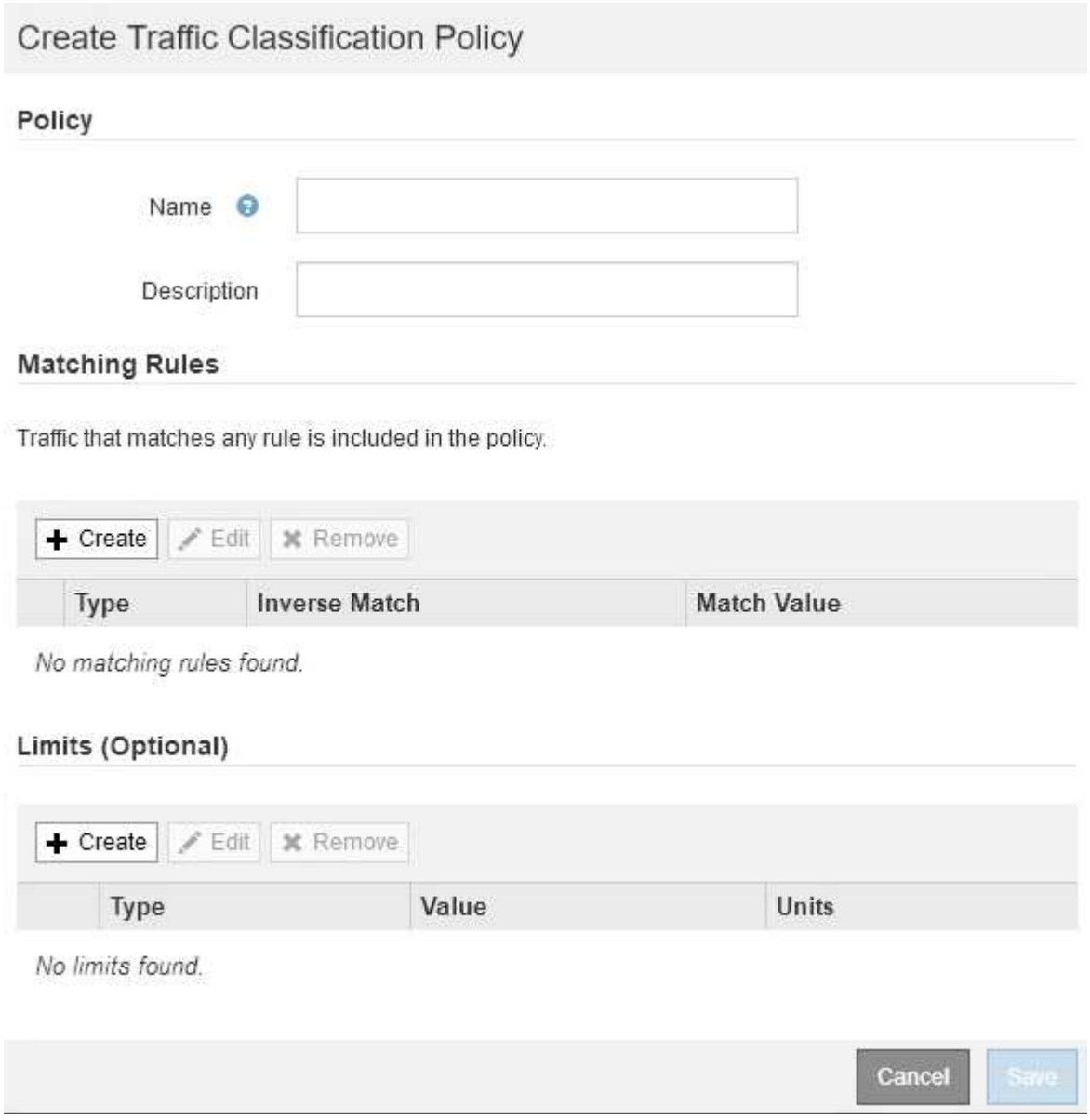
1. Select **Configuration** > **Network Settings** > **Traffic Classification**.

   The Traffic Classification Policies page appears.



2. Click **Create**.

   The Create Traffic Classification Policy dialog box appears.



3. In the **Name** field, enter a name for the policy.

   Enter a descriptive name so you can recognize the policy.

4. Optionally, add a description for the policy in the **Description** field.

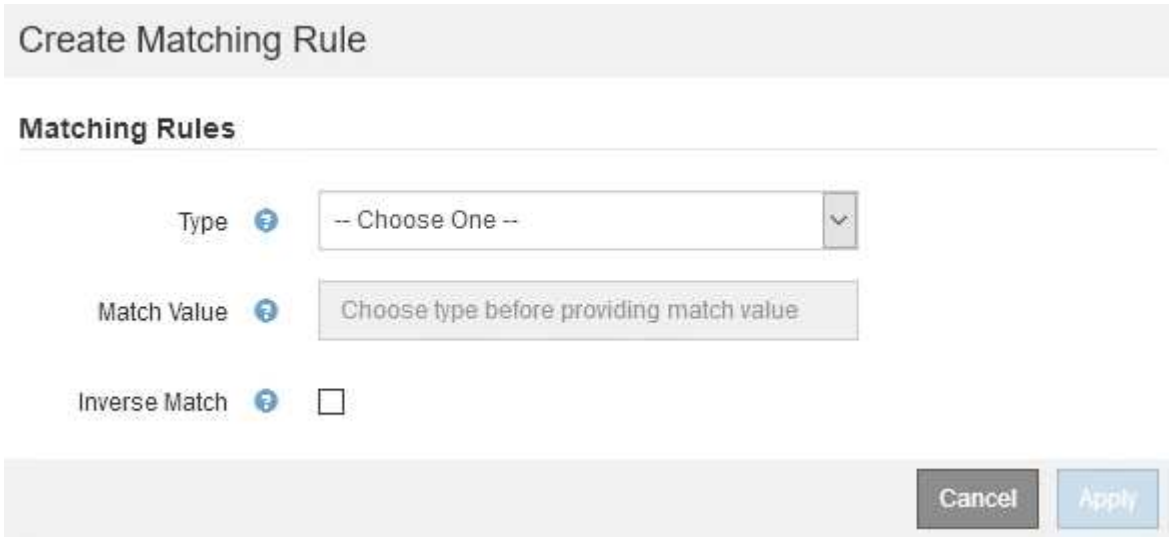
   For example, describe what this traffic classification policy applies to and what it will limit.

5. Create one or more matching rules for the policy.

   Matching rules control which entities will be affected by this traffic classification policy. For example, select Tenant if you want this policy to apply to the network traffic for a specific tenant. Or select Endpoint if you want this policy to apply to the network traffic on a specific load balancer endpoint.

   a. Click **Create** in the **Matching Rules** section.

      The Create Matching Rule dialog box appears.



   b. From the **Type** drop-down, select the type of entity to be included in the matching rule.

   c. In the **Match Value** field, enter a match value based on the type of entity you chose.

      - Bucket: Enter a bucket name.
      - Bucket Regex: Enter a regular expression that will be used to match a set of bucket names.

        The regular expression is unanchored. Use the ^ anchor to match at the beginning of the bucket name, and use the $ anchor to match at the end of the name.

      - CIDR: Enter an IPv4 subnet, in CIDR notation, that matches the desired subnet.
      - Endpoint: Select an endpoint from the list of existing endpoints. These are the load balancer endpoints you defined on the Load Balancer Endpoints page.
      - Tenant: Select a tenant from the list of existing tenants. Tenant matching is based on the ownership of the bucket being accessed. Anonymous access to a bucket matches the tenant that owns the bucket.

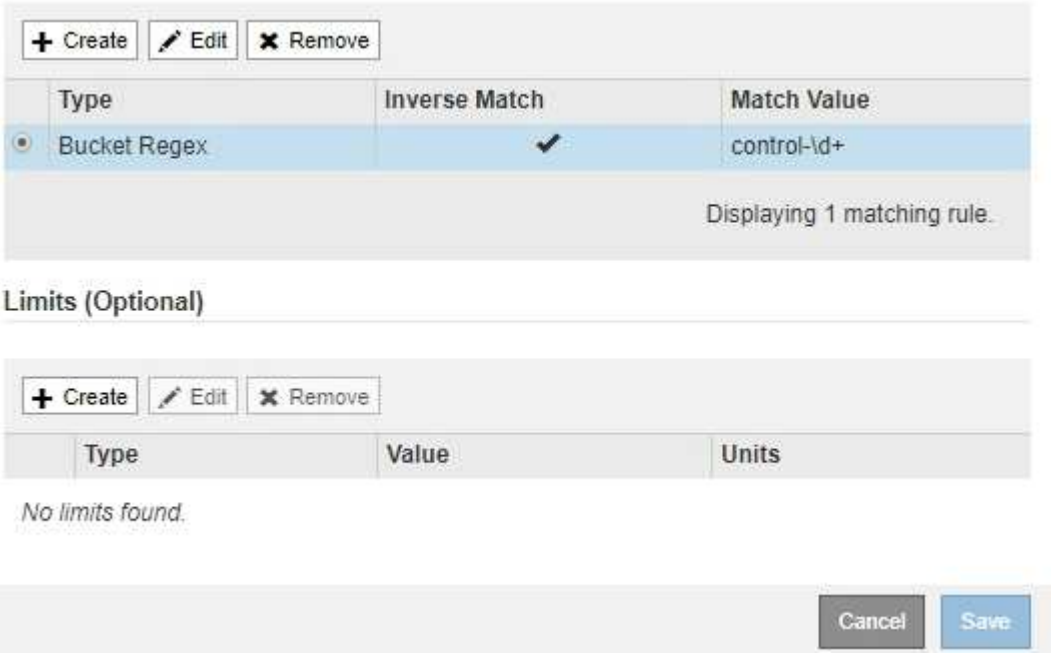
   d. If you want to match all network traffic *except* traffic consistent with the Type and Match Value just defined, select the **Inverse** check box. Otherwise, leave the check box unselected.

      For example, if you want this policy to apply to all but one of the load balancer endpoints, specify the load balancer endpoint to be excluded, and select **Inverse**.

For a policy containing multiple matchers where at least one is an inverse matcher, be careful not to create a policy that matches all requests.

e. Click **Apply**.

The rule is created and is listed in the Matching Rules table.



f. Repeat these steps for each rule you want to create for the policy.

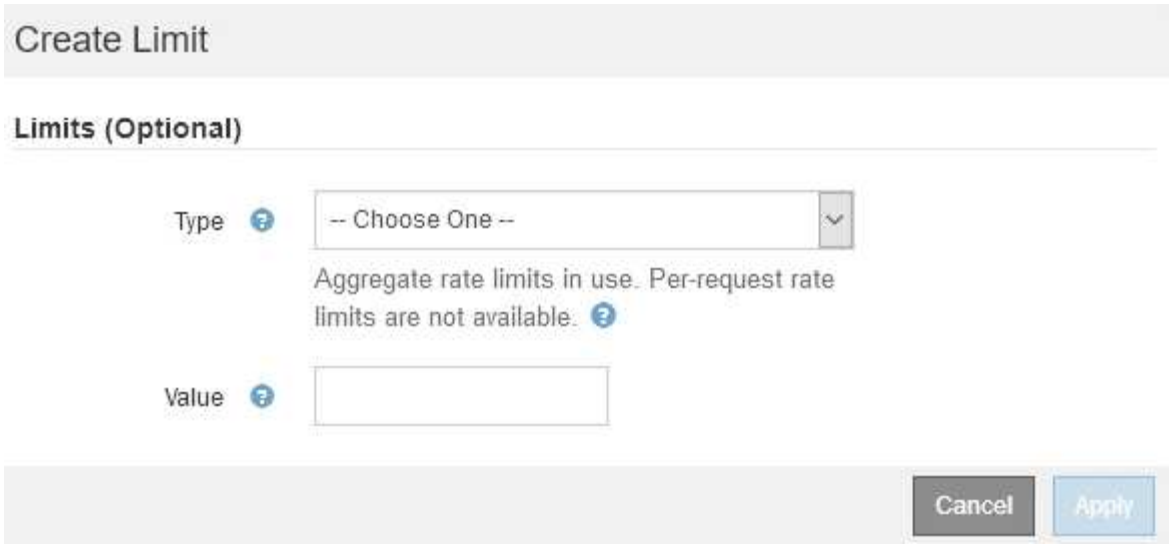
Traffic that matches any rule is handled by the policy.

6. Optionally, create limits for the policy.

Even if you do not create limits, StorageGRID collects metrics so that you can monitor network traffic that matches the policy.

a. Click **Create** in the **Limits** section.

The Create Limit dialog box appears.



b. From the **Type** drop-down, select the type of limit you want to apply to the policy.

In the following list, **In** refers to traffic from S3 or Swift clients to the StorageGRID load balancer, and **Out** refers to traffic from the load balancer to S3 or Swift clients.

- Aggregate Bandwidth In
- Aggregate Bandwidth Out
- Concurrent Read Requests
- Concurrent Write Requests
- Per-Request Bandwidth In
- Per-Request Bandwidth Out
- Read Request Rate
- Write Requests Rate

> ⓘ You can create policies to limit aggregate bandwidth or to limit per-request bandwidth. However, StorageGRID cannot limit both types of bandwidth at the same time. Aggregate bandwidth limits might impose an additional minor performance impact on non-limited traffic.

For bandwidth limits, StorageGRID applies the policy that best matches the type of limit set. For example, if you have a policy that limits traffic in only one direction, then traffic in the opposite direction will be unlimited, even if there is traffic that matches additional policies that have bandwidth limits. StorageGRID implements “best” matches for bandwidth limits in the following order:

- Exact IP address (/32 mask)
- Exact bucket name
- Bucket regex
- Tenant
- Endpoint
- Non-exact CIDR matches (not /32)

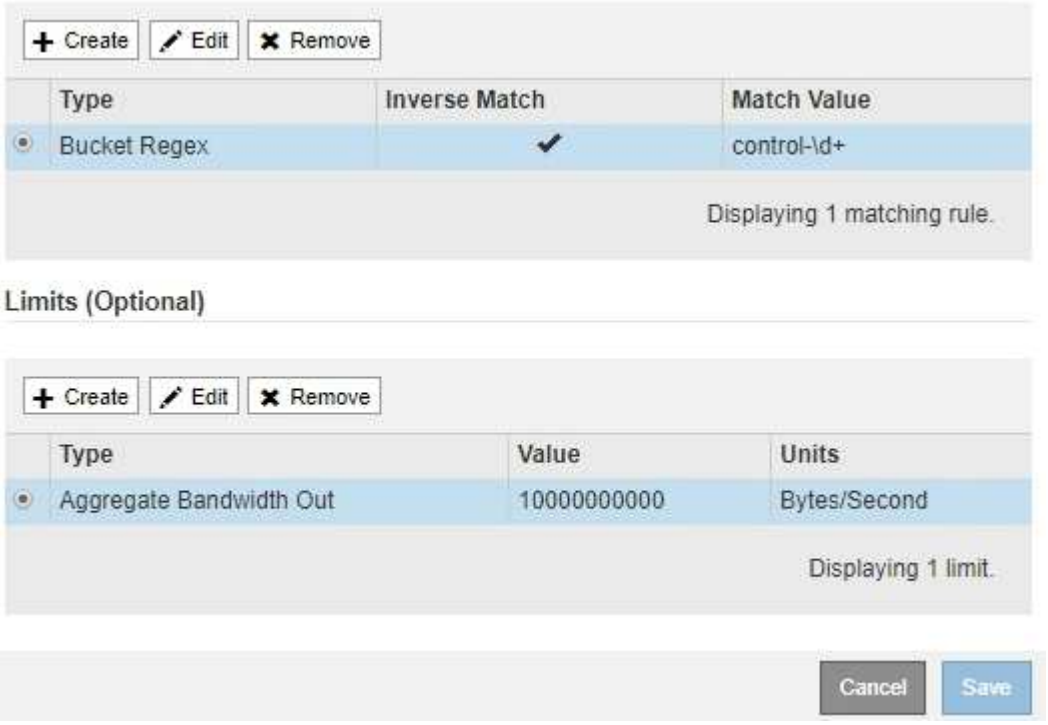
- Inverse matches

c. In the **Value** field, enter a numerical value for the type of limit you chose.

   The expected units are shown when you select a limit.

d. Click **Apply**.

   The limit is created and is listed in the Limits table.



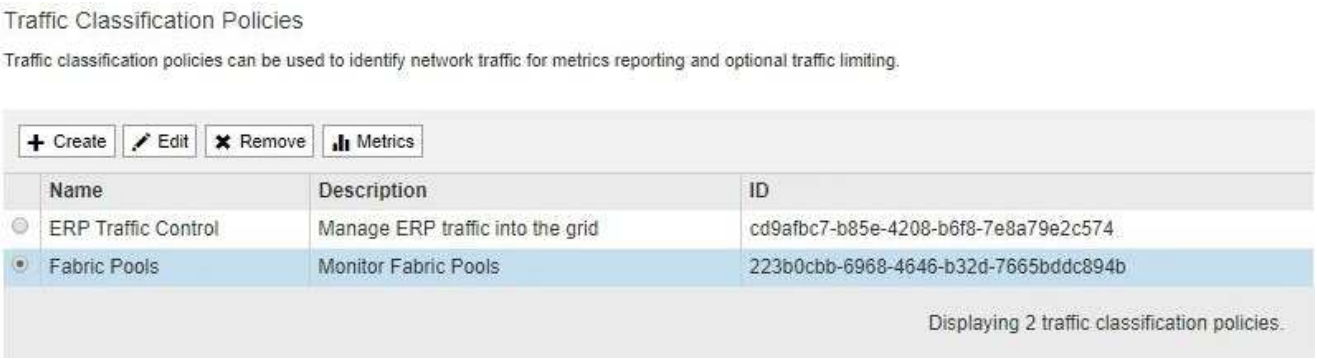
e. Repeat these steps for each limit you want to add to the policy.

   For example, if you want to create a 40 Gbps bandwidth limit for an SLA tier, create an Aggregate Bandwidth In limit and an Aggregate Bandwidth Out limit and set each one to 40 Gbps.

   To convert megabytes per second to gigabits per second, multiply by eight. For example, 125 MB/s is equivalent to 1,000 Mbps or 1 Gbps.

7. When you are finished creating rules and limits, click **Save**.

The policy is saved and is listed in the Traffic Classification Policies table.



S3 and Swift client traffic is now handled according to the traffic classification policies. You can view traffic charts and verify that the polices are enforcing the traffic limits you expect.

Related information

Managing load balancing

Viewing network traffic metrics

Editing a traffic classification policy

You can edit a traffic classification policy to change its name or description, or to create, edit, or delete any rules or limits for the policy.

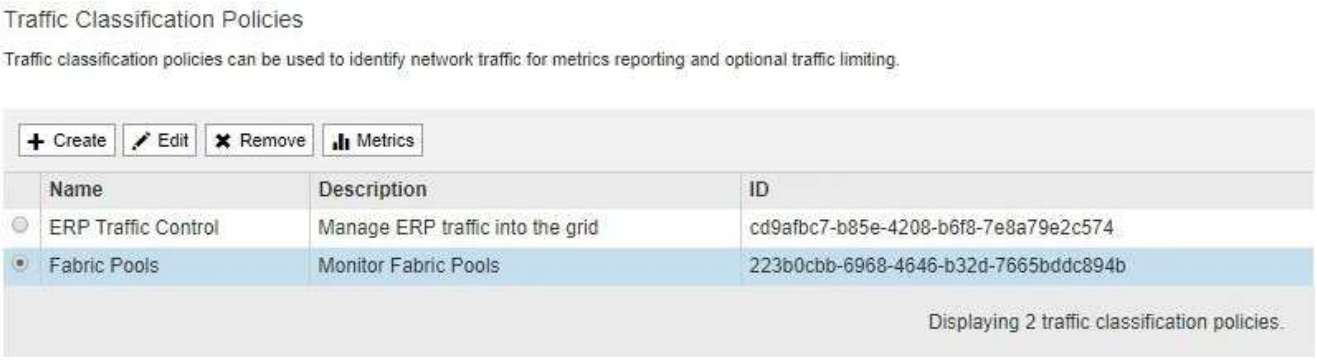
What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have the Root Access permission.

Steps

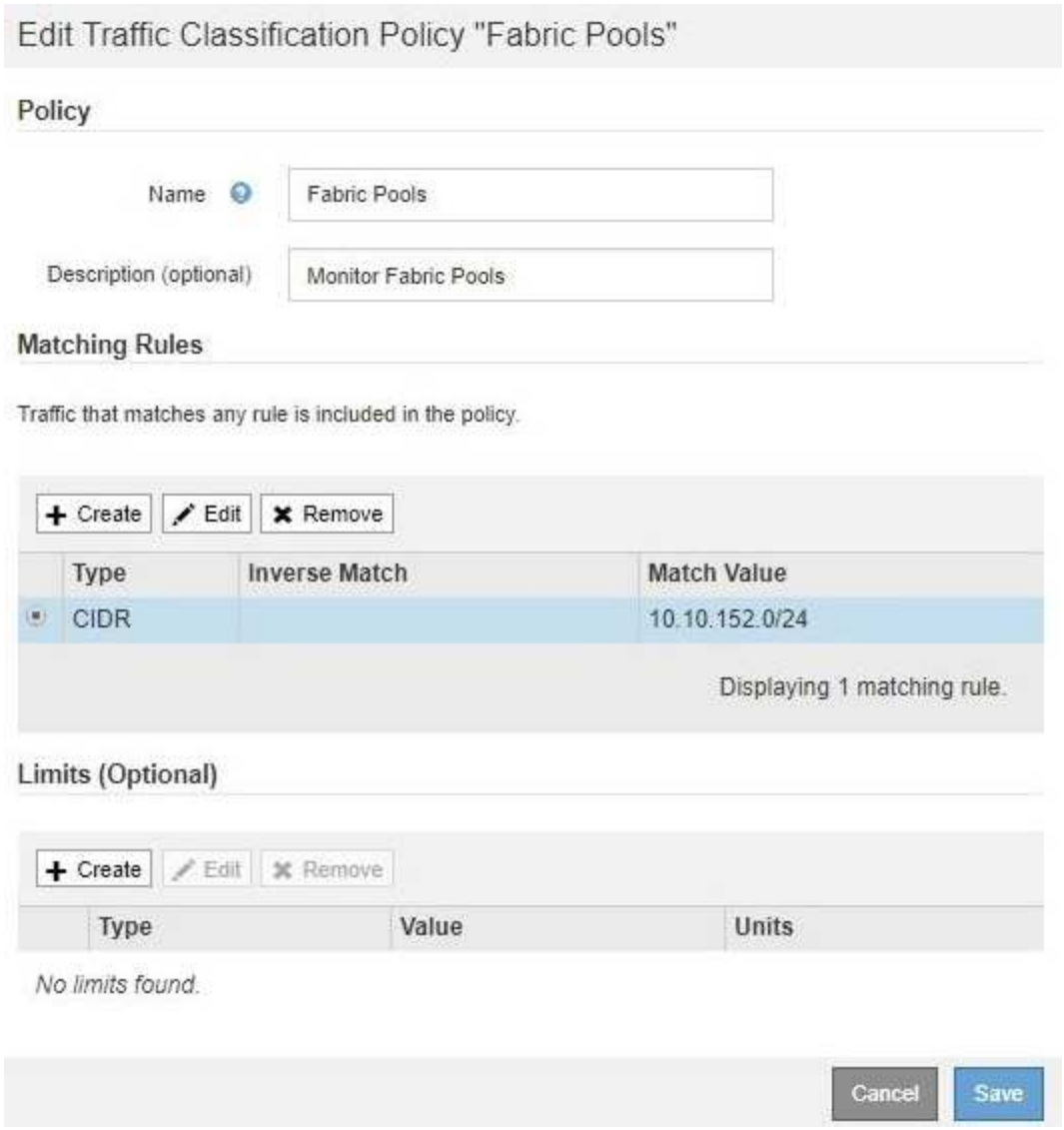
1. Select **Configuration** > **Network Settings** > **Traffic Classification**.

   The Traffic Classification Policies page appears, and the existing policies are listed in the table.



2. Select the radio button to the left of the policy you want to edit.
3. Click **Edit**.

   The Edit Traffic Classification Policy dialog box appears.



4. Create, edit, or remove matching rules and limits as needed.
   a. To create a matching rule or limit, click **Create**, and follow the instructions for creating a rule or creating a limit.
   b. To edit a matching rule or limit, select the radio button for the rule or limit, click **Edit** in the **Matching Rules** section or the **Limits** section, and follow the instructions for creating a rule or creating a limit.
   c. To remove a matching rule or limit, select the radio button for the rule or limit, and click **Remove**. Then, click **OK** to confirm that you want to remove the rule or limit.
5. When you are finished creating or editing a rule or a limit, click **Apply**.
6. When you are finished editing the policy, click **Save**.

   The changes you made to the policy are saved, and network traffic is now handled according to the traffic classification policies. You can view traffic charts and verify that the polices are enforcing the traffic limits you expect.

Deleting a traffic classification policy

If you no longer need a traffic classification policy, you can delete it.

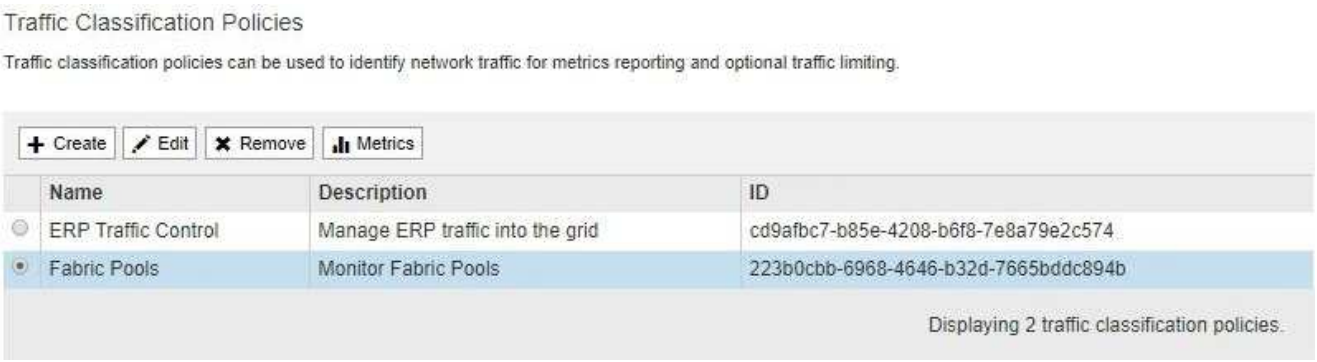
What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have the Root Access permission.

Steps

1. Select **Configuration** > **Network Settings** > **Traffic Classification**.

   The Traffic Classification Policies page appears, and the existing policies are listed in the table.



2. Select the radio button to the left of the policy you want to delete.
3. Click **Remove**.

   A Warning dialog box appears.

4. Click **OK** to confirm that you want to delete the policy.

   The policy is deleted.

Viewing network traffic metrics

You can monitor network traffic by viewing the graphs that are available from the Traffic Classification Policies page.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have the Root Access permission.

About this task

For any existing traffic classification policy, you can view metrics for the Load Balancer service to determine if the policy is successfully limiting traffic across the network. The data in the graphs can help you determine if

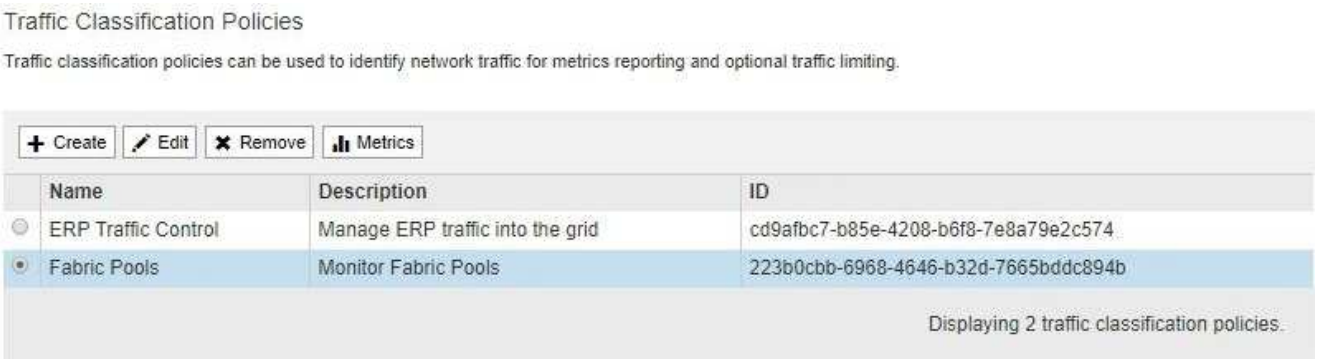
you need adjust the policy.

Even if no limits are set for a traffic classification policy, metrics are collected and the graphs provide useful information for understanding traffic trends.

Steps

1. Select **Configuration** > **Network Settings** > **Traffic Classification**.

   The Traffic Classification Policies page appears, and the existing policies are listed in the table.



2. Select the radio button to the left of the policy you want to view metrics for.
3. Click **Metrics**.

   A new browser window opens, and the Traffic Classification Policy graphs appear. The graphs display metrics only for the traffic that matches the selected policy.

   You can select other policies to view by using the **policy** pull-down.

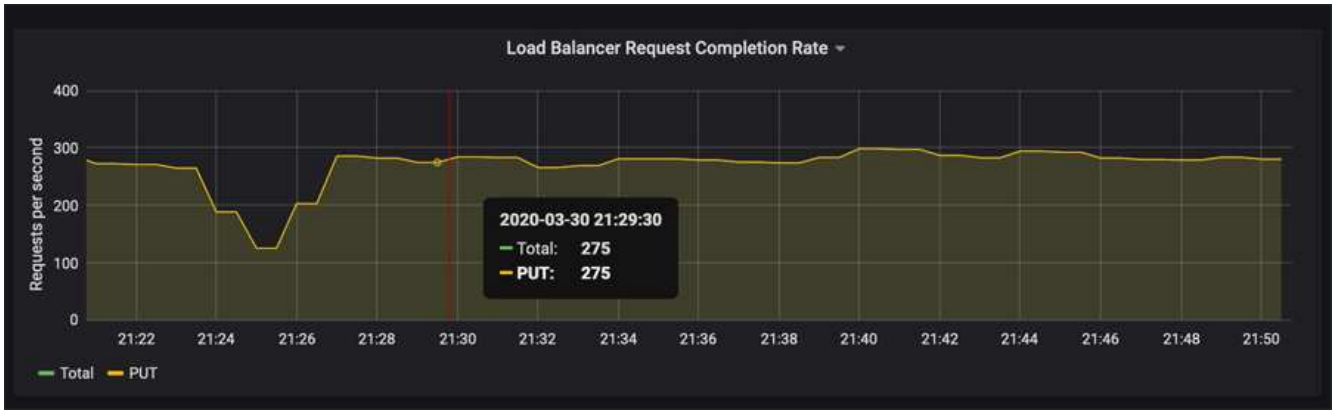
   The following graphs are included on the web page.

   - Load Balancer Request Traffic: This graph provides a 3-minute moving average of the throughput of data transmitted between load balancer endpoints and the clients making the requests, in bits per

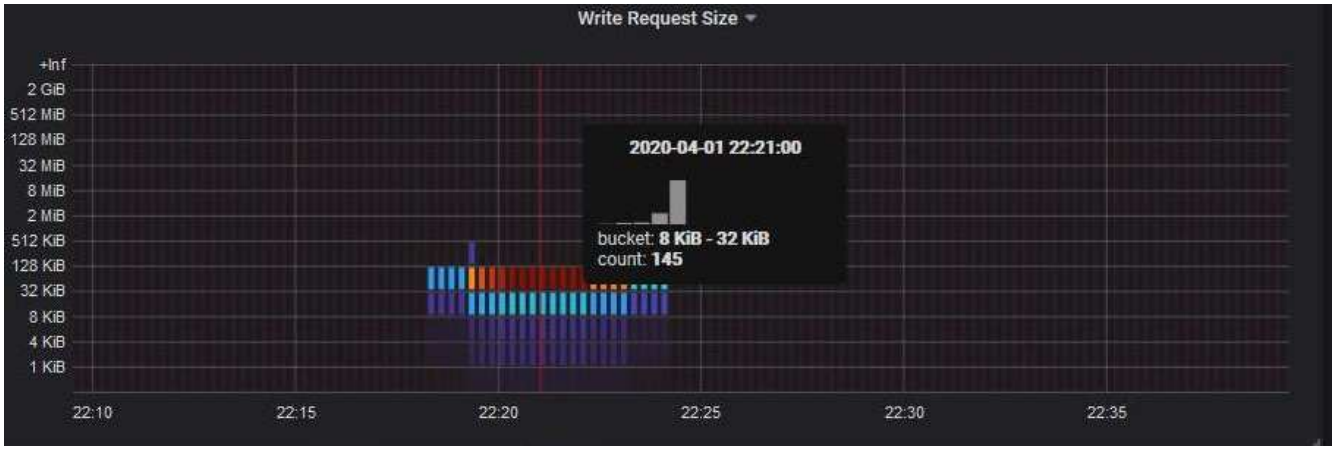
second.

- Load Balancer Request Completion Rate: This graph provides a 3-minute moving average of the number of completed requests per second, broken down by request type (GET, PUT, HEAD, and DELETE). This value is updated when the headers of a new request have been validated.
- Error Response Rate: This graph provides a 3-minute moving average of the number of error responses returned to clients per second, broken down by the error response code.
- Average Request Duration (Non-Error): This graph provides a 3-minute moving average of request durations, broken down by request type (GET, PUT, HEAD, and DELETE). Each request duration starts when a request header is parsed by the Load Balancer service and ends when the complete response body is returned to the client.
- Write Request Rate by Object Size: This heatmap provides a 3-minute moving average of the rate at which write requests are completed based on object size. In this context, write requests refer only to PUT requests.
- Read Request Rate by Object Size: This heatmap provides a 3-minute moving average of the rate at which read requests are completed based on object size. In this context, read requests refer only to GET requests. The colors in the heatmap indicate the relative frequency of an object size within an individual graph. The cooler colors (for example, purple and blue) indicate lower relative rates, and the warmer colors (for example, orange and red) indicate higher relative rates.

4. Hover the cursor over a line graph to see a pop-up of values on a specific part of the graph.



5. Hover the cursor over a heatmap to see a pop-up that shows the date and time of the sample, object sizes that are aggregated into the count, and the number of requests per second during that time period.



6. Use the **Policy** pull-down in the upper left to select a different policy.

   The graphs for the selected policy appear.

7. Alternatively, access the graphs from the **Support** menu.
    a. Select **Support** > **Tools** > **Metrics**.
    b. In the **Grafana** section of the page, select **Traffic Classification Policy**.
    c. Select the policy from the pull-down on the upper left of the page.

        Traffic classification policies are identified by their ID. Policy IDs are listed on the Traffic Classification Policies page.

8. Analyze the graphs to determine how often the policy is limiting traffic and whether you need to adjust the policy.

Related information

Monitor & troubleshoot

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.