



Manage networks and connections

StorageGRID

NetApp
March 03, 2022

Table of Contents

- Manage networks and connections 1
 - Guidelines for StorageGRID networks 1
 - View IP addresses 2
 - Supported ciphers for outgoing TLS connections 3
 - Change network transfer encryption 4
 - Manage traffic classification policies 5
 - Manage link costs 18

Manage networks and connections

Guidelines for StorageGRID networks

You can use the Grid Manager to configure and manage StorageGRID networks and connections.

See [Configure S3 and Swift client connections](#) to learn how to connect S3 or Swift clients.

Default StorageGRID networks

By default, StorageGRID supports three network interfaces per grid node, allowing you to configure the networking for each individual grid node to match your security and access requirements.

For more information about network topology, see [Networking guidelines](#).

Grid Network

Required. The Grid Network is used for all internal StorageGRID traffic. It provides connectivity between all nodes in the grid, across all sites and subnets.

Admin Network

Optional. The Admin Network is typically used for system administration and maintenance. It can also be used for client protocol access. The Admin Network is typically a private network and does not need to be routable between sites.

Client Network

Optional. The Client Network is an open network typically used to provide access to S3 and Swift client applications, so the Grid Network can be isolated and secured. The Client Network can communicate with any subnet reachable through the local gateway.

Guidelines

- Each StorageGRID grid node requires a dedicated network interface, IP address, subnet mask, and gateway for each network it is assigned to.
- A grid node cannot have more than one interface on a network.
- A single gateway, per network, per grid node is supported, and it must be on the same subnet as the node. You can implement more complex routing in the gateway, if required.
- On each node, each network maps to a specific network interface.

| Network | Interface name |
|-------------------|----------------|
| Grid | eth0 |
| Admin (optional) | eth1 |
| Client (optional) | eth2 |

- If the node is connected to a StorageGRID appliance, specific ports are used for each network. For details, see the installation instructions for your appliance.
- The default route is generated automatically, per node. If eth2 is enabled, then 0.0.0.0/0 uses the Client Network on eth2. If eth2 is not enabled, then 0.0.0.0/0 uses the Grid Network on eth0.
- The Client Network does not become operational until the grid node has joined the grid
- The Admin Network can be configured during grid node deployment to allow access to the installation user interface before the grid is fully installed.

Optional interfaces

Optionally, you can add extra interfaces to a node. For example, you might want to add a trunk interface to an Admin or Gateway Node, so you can use [VLAN interfaces](#) to segregate the traffic belonging to different applications or tenants. Or, you might want to add an access interface to use in a [high availability \(HA\) group](#).

To add trunk or access interfaces, see the following:

- **VMware (after installing the node):** [VMware: Add trunk or access interfaces to a node](#)
 - **RHEL or CentOS (before installing the node):** [Create node configuration files](#)
 - **Ubuntu or Debian (before installing the node):** [Create node configuration files](#)
 - **RHEL, CentOS, Ubuntu, or Debian (after installing the node):** [Linux: Add trunk or access interfaces to a node](#)

View IP addresses

You can view the IP address for each grid node in your StorageGRID system. You can then use this IP address to log into the grid node at the command line and perform various maintenance procedures.

What you'll need

You are signed in to the Grid Manager using a [supported web browser](#).

About this task

For information on changing IP addresses, see [Recover and maintain](#).

Steps

1. Select **NODES > *grid node* > Overview**.
2. Select **Show more** to the right of the IP Addresses title.


The IP addresses for that grid node are listed in a table.

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  **Connected**

Storage used:

| | | | |
|-----------------|------------------------|----|-------------------|
| Object data | <div><div></div></div> | 7% | ? |
| Object metadata | <div><div></div></div> | 5% | ? |

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

| Interface ⬆ | IP address ⬆ |
|-----------------------------|------------------------------|
| eth0 (Grid Network) | 10.96.106.21 |
| eth0 (Grid Network) | fe80::2a0:98ff:fe64:6582 |
| hic2 | 10.96.106.21 |
| hic4 | 10.96.106.21 |
| mtc2 | 169.254.0.1 |

Alerts

| Alert name ⬆ | Severity ? ⬆ | Time triggered ⬆ | Current values |
|--|--|----------------------------------|----------------|
| ILM placement unachievable 🔗 |  Major | 2 hours ago ? | |
| A placement instruction in an ILM rule cannot be achieved for certain objects. | | | |

Supported ciphers for outgoing TLS connections

The StorageGRID system supports a limited set of cipher suites for Transport Layer Security (TLS) connections to the external systems used for identity federation and Cloud Storage Pools.

Supported versions of TLS

StorageGRID supports TLS 1.2 and TLS 1.3 for connections to external systems used for identity federation and Cloud Storage Pools.

The TLS ciphers that are supported for use with external systems have been selected to ensure compatibility with a range of external systems. The list is larger than the list of ciphers that are supported for use with S3 or Swift client applications.



TLS configuration options such as protocol versions, ciphers, key exchange algorithms, and MAC algorithms are not configurable in StorageGRID. Contact your NetApp account representative if you have specific requests about these settings.

Supported TLS 1.2 cipher suites

The following TLS 1.2 cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Supported TLS 1.3 cipher suites

The following TLS 1.3 cipher suites are supported:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Change network transfer encryption

The StorageGRID system uses Transport Layer Security (TLS) to protect internal control traffic between grid nodes. The Network Transfer Encryption option sets the algorithm used by TLS to encrypt control traffic between grid nodes. This setting does not affect data encryption.

What you'll need

- You are signed in to the Grid Manager using a [supported web browser](#).
- You have specific access permissions.

About this task

By default, network transfer encryption uses the AES256-SHA algorithm. Control traffic can also be encrypted using the AES128-SHA algorithm.

Steps

1. Select **CONFIGURATION > System > Grid options**.
2. In the Network Options section, change Network Transfer Encryption to **AES128-SHA** or **AES256-SHA** (default).

Network Options

Prevent Client Modification ☐ ☐

Enable HTTP Connection ☐ ☐

Network Transfer Encryption ☒ AES128-SHA ☒ AES256-SHA

3. Select **Save**.

Manage traffic classification policies

Manage 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.

Match 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 can be 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 policies are enforcing the traffic limits you expect.

Use 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 |

Create 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 are signed in to the Grid Manager using a [supported web browser](#).
- You have the Root access permission.
- You have created any load balancer endpoints you want to match.
- You have created any tenants you want to match.

Steps

1. Select **CONFIGURATION > Network > Traffic classification**.

The Traffic Classification Policies page appears.

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. Select **Create**.

The Create Traffic Classification Policy dialog box appears.

Create Traffic Classification Policy

Policy

Name ⓘ

Description

Matching Rules

Traffic that matches any rule is included in the policy.

+ Create

✎ Edit

✕ Remove

| Type | Inverse Match | Match Value |
|------|---------------|-------------|
|------|---------------|-------------|

No matching rules found.

Limits (Optional)

+ Create

✎ Edit

✕ Remove

| Type | Value | Units |
|------|-------|-------|
|------|-------|-------|

No limits found.

Cancel

Save

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. Select **Create** in the **Matching Rules** section.


The Create Matching Rule dialog box appears.



Create Matching Rule

Matching Rules

Type  -- Choose One -- 

Match Value  Choose type before providing match value

Inverse Match  ☐

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. See [Configure load balancer endpoints](#).
- **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. Select **Apply**.

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

| <div> <div>+ Create</div> <div>Edit</div> <div>✕ Remove</div> </div> | | |
|--|---------------|-------------|
| Type | Inverse Match | Match Value |
| <input checked="" type="radio"/> Bucket Regex | ✓ | control-ld+ |
| Displaying 1 matching rule. | | |


Limits (Optional)

| <div> <div>+ Create</div> <div>Edit</div> <div>✕ Remove</div> </div> | | |
|--|-------|--|
| Type | Value | Units |
| No limits found. | | |
| | | <div> <div>Cancel</div> <div>Save</div> </div> |

- 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. Select **Create** in the **Limits** section.


The Create Limit dialog box appears.


Create Limit

Limits (Optional)

Type 

-- Choose One --

Aggregate rate limits in use. Per-request rate limits are not available. 

Value 

Cancel

Apply

- 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. Select **Apply**.

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

+ Create
Edit
Remove

| Type | Inverse Match | Match Value |
|---|---------------|-------------|
| <input checked="" type="radio"/> Bucket Regex | ✓ | control-ld+ |

Displaying 1 matching rule.

Limits (Optional)

+ Create
Edit
Remove

| Type | Value | Units |
|--|-------------|--------------|
| <input checked="" type="radio"/> Aggregate Bandwidth Out | 10000000000 | Bytes/Second |

Displaying 1 limit.

Cancel
Save

- 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, select **Save**.

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

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 |
| <input type="radio"/> ERP Traffic Control | Manage ERP traffic into the grid | cd9afbc7-b85e-4208-b6f8-7e8a79e2c574 |
| <input checked="" type="radio"/> Fabric Pools | Monitor Fabric Pools | 223b0cbb-6968-4646-b32d-7665bdbc894b |

Displaying 2 traffic classification policies.

S3 and Swift client traffic is now handled according to the traffic classification policies. You can view traffic charts and verify that the policies are enforcing the traffic limits you expect. See [View network traffic metrics](#).

Edit 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 are signed in to the Grid Manager using a [supported web browser](#).
- You have the Root access permission.

Steps

1. Select **CONFIGURATION > Network > Traffic classification**.

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

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 |
|----------------------------------|---------------------|----------------------------------|--------------------------------------|
| <input type="radio"/> | ERP Traffic Control | Manage ERP traffic into the grid | cd9afbc7-b85e-4208-b6f8-7e8a79e2c574 |
| <input checked="" type="radio"/> | Fabric Pools | Monitor Fabric Pools | 223b0cbb-6968-4646-b32d-7665bddc894b |


Displaying 2 traffic classification policies.

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

The Edit Traffic Classification Policy dialog box appears.

Edit Traffic Classification Policy "Fabric Pools"

Policy

Name 

Fabric Pools

Description (optional)

Monitor Fabric Pools

Matching Rules

Traffic that matches any rule is included in the policy.

+ Create  Edit  Remove

| | Type | Inverse Match | Match Value |
|----------------------------------|------|---------------|----------------|
| <input checked="" type="radio"/> | CIDR | | 10.10.152.0/24 |

Displaying 1 matching rule.

Limits (Optional)

+ Create  Edit  Remove

| | Type | Value | Units |
|--|------|-------|-------|
|--|------|-------|-------|

No limits found.

Cancel

Save

4. Create, edit, or remove matching rules and limits as needed.
 - a. To create a matching rule or limit, select **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, select **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 select **Remove**. Then, select **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, select **Apply**.
6. When you are finished editing the policy, select **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 policies are enforcing the traffic limits you expect.

Delete a traffic classification policy

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

What you'll need

- You are signed in to the Grid Manager using a [supported web browser](#).
- You have the Root access permission.

Steps

1. Select **CONFIGURATION > Network > Traffic classification**.

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

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 |
|----------------------------------|---------------------|----------------------------------|--------------------------------------|
| <input type="radio"/> | ERP Traffic Control | Manage ERP traffic into the grid | cd9afbc7-b85e-4208-b6f8-7e8a79e2c574 |
| <input checked="" type="radio"/> | Fabric Pools | Monitor Fabric Pools | 223b0cbb-6968-4646-b32d-7665bdc894b |

Displaying 2 traffic classification policies.

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

A Warning dialog box appears.



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

The policy is deleted.

View 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 are signed in to the Grid Manager using a [supported web browser](#).
- You have the Root access permission or the Tenant Accounts 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 > Traffic classification**.

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

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 |
|----------------------------------|---------------------|----------------------------------|--------------------------------------|
| <input type="radio"/> | ERP Traffic Control | Manage ERP traffic into the grid | cd9afbc7-b85e-4208-b6f8-7e8a79e2c574 |
| <input checked="" type="radio"/> | Fabric Pools | Monitor Fabric Pools | 223b0cbb-6968-4646-b32d-7665bddc894b |

Displaying 2 traffic classification policies.

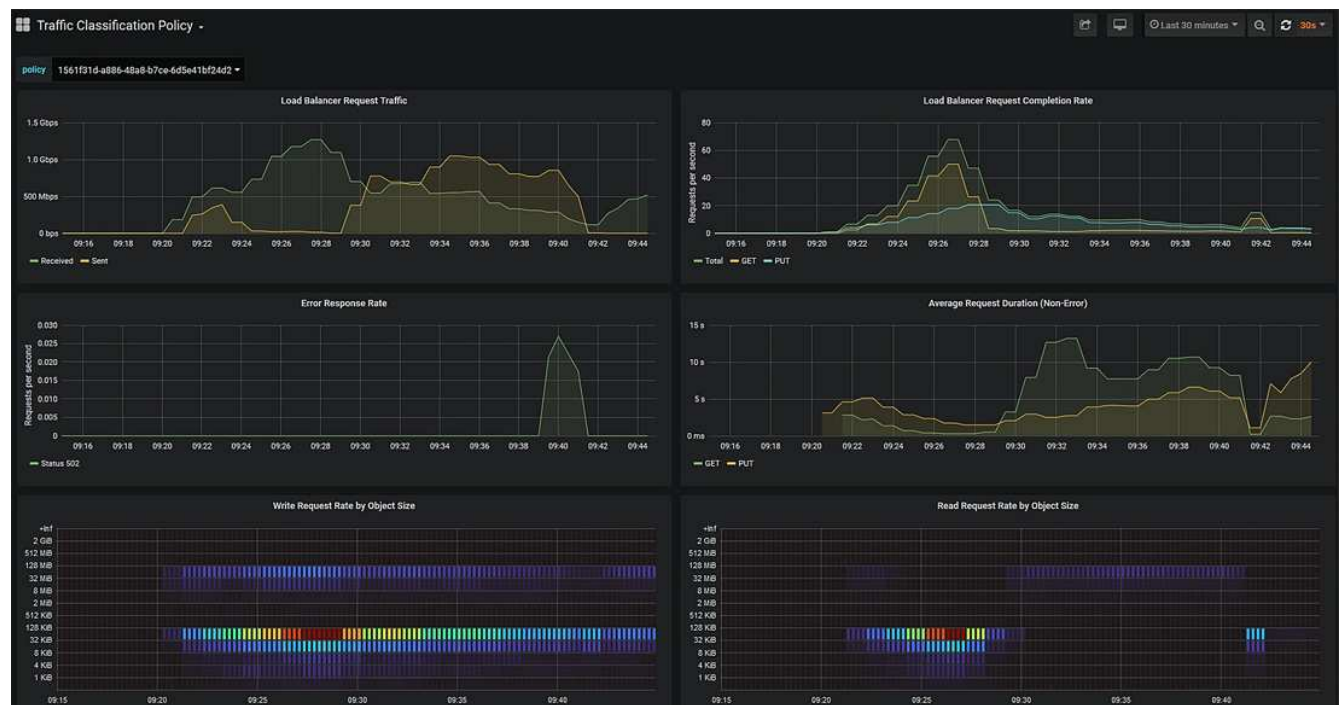


The **Create**, **Edit**, and **Remove** buttons are disabled if you have the Tenant Accounts permission but you do not have the Root access permission.

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

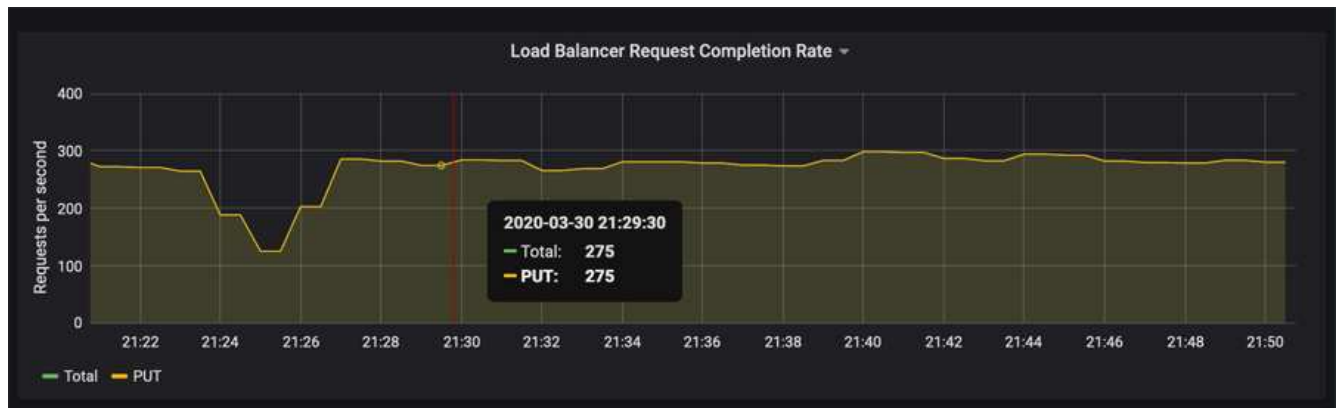
You can select other policies to view by using the **policy** pull-down.



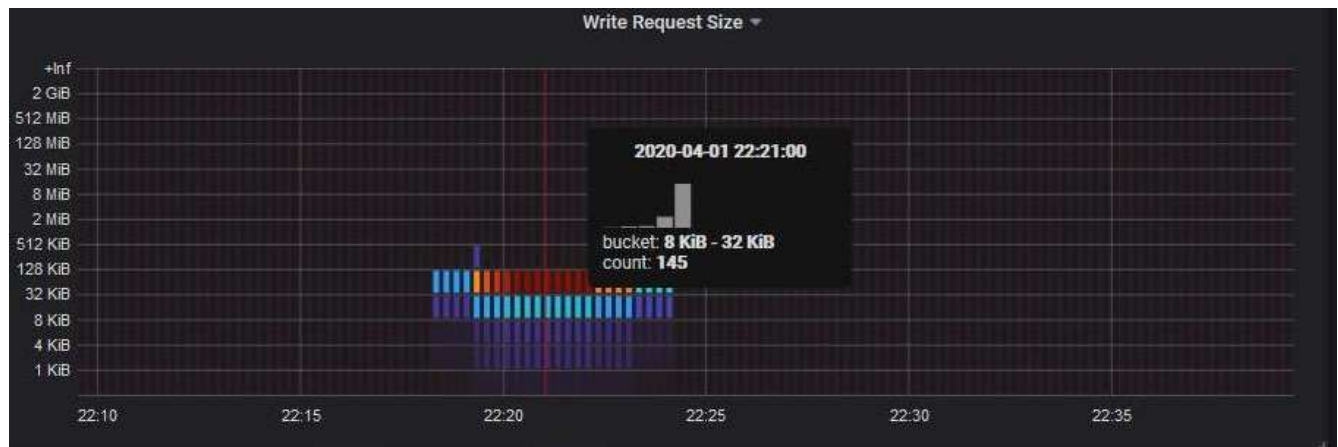
The following graphs are included on the web page.

- 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.

- Select **SUPPORT > Tools > Metrics**.
- In the **Grafana** section of the page, select **Traffic Classification Policy**.
- 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 and troubleshoot](#)

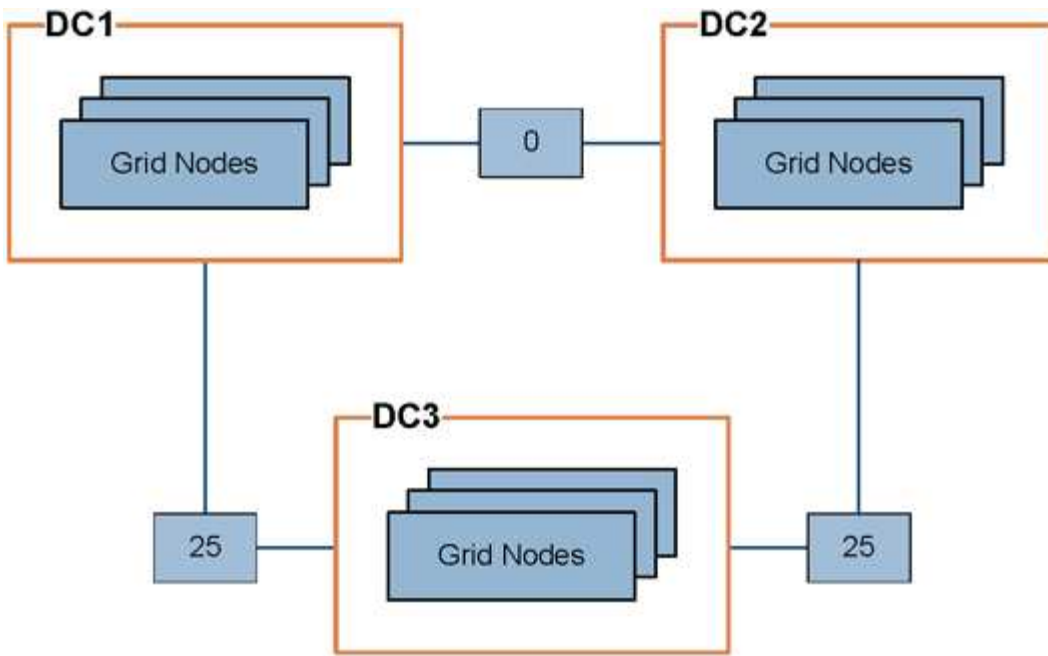
Manage link costs

What link costs are

Link costs let you prioritize which data center site provides a requested service when two or more data center sites exist. You can adjust link costs to reflect latency between sites.

- Link costs are used to prioritize which object copy is used to fulfill object retrievals.
- Link costs are used by the Grid Management API and the Tenant Management API to determine which internal StorageGRID services to use.
- Link costs are used by the deprecated Connection Load Balancer (CLB) service on Gateway Nodes to direct client connections. See [How load balancing works - CLB service](#).

The diagram shows a three site grid that has link costs configured between sites:



- The CLB service on Gateway Nodes equally distribute client connections to all Storage Nodes at the same data center site and to any data center sites with a link cost of 0.

In the example, a Gateway Node at data center site 1 (DC1) equally distributes client connections to Storage Nodes at DC1 and to Storage Nodes at DC2. A Gateway Node at DC3 sends client connections only to Storage Nodes at DC3.

- When retrieving an object that exists as multiple replicated copies, StorageGRID retrieves the copy at the data center that has the lowest link cost.

In the example, if a client application at DC2 retrieves an object that is stored both at DC1 and DC3, the object is retrieved from DC1, because the link cost from DC1 to D2 is 0, which is lower than the link cost from DC3 to DC2 (25).

Link costs are arbitrary relative numbers with no specific unit of measure. For example, a link cost of 50 is used less preferentially than a link cost of 25. The table shows commonly used link costs.

| Link | Link cost | Notes |
|---|--------------|--|
| Between physical data center sites | 25 (default) | Data centers connected by a WAN link. |
| Between logical data center sites at the same physical location | 0 | Logical data centers in the same physical building or campus connected by a LAN. |

Update link costs

You can update the link costs between data center sites to reflect latency between sites.


What you'll need

- You are signed in to the Grid Manager using a [supported web browser](#).

- You have the Grid Topology Page Configuration permission.


Steps



1. Select **CONFIGURATION** > **Network** > **Link cost**.



Link Cost


Updated: 2021-03-29 12:28:41 EDT


Site Names (1 - 2 of 2) 

| Site ID | Site Name | Actions |
|---------|---------------|---|
| 10 | Data Center 1 |  |
| 20 | Data Center 2 |  |

Show Records Per Page
Previous
« 1 » Next


Link Costs

| Link Source | Link Destination | Actions |
|--|------------------|---|
| <div> <div>10</div> <div>20</div> </div> | |  |



2. Select a site under **Link Source** and enter a cost value between 0 and 100 under **Link Destination**.

You cannot change the link cost if the source is the same as the destination.

To cancel changes, select  **Revert**.

3. Select **Apply Changes**.

Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.