Managing StorageGRID networks and connections

StorageGRID

Table of Contents

Managing StorageGRID networks and connections

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

See Configuring S3 and Swift client connections to learn how to connect S3 or Swift clients.

- Guidelines for StorageGRID networks
- Viewing IP addresses
- Supported ciphers for outgoing TLS connections
- Changing network transfer encryption
- Configuring server certificates
- Configuring Storage proxy settings
- Configuring Admin proxy settings
- Managing traffic classification policies
- What link costs are

Guidelines for StorageGRID networks

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

> ⓘ   To modify or add a network for a grid node, see the recovery and maintenance instructions. For more information about network topology, see the networking instructions.

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.

Related information

Maintain & recover

Network guidelines

Viewing 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 must be signed in to the Grid Manager using a supported browser.

About this task

For information on changing IP addresses, see the recovery and maintenance instructions.

Steps

1. Select **Nodes** > *grid node* > **Overview**.

2. Click **Show more** to the right of the IP Addresses title.

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

Related information

[Maintain & recover](#)

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

Changing 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 must be signed in to the Grid Manager using a supported browser.

- You must 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 Settings** > **Grid Options**.

2. In the Network Options section, change Network Transfer Encryption to **AES128-SHA** or **AES256-SHA** (default).

3. Click **Save**.

Configuring server certificates

You can customize the server certificates used by the StorageGRID system.

The StorageGRID system uses security certificates for multiple distinct purposes:

- Management Interface Server Certificates: Used to secure access to the Grid Manager, the Tenant Manager, the Grid Management API, and the Tenant Management API.
- Storage API Server Certificates: Used to secure access to the Storage Nodes and Gateway Nodes, which API client applications use to upload and download object data.

You can use the default certificates created during installation, or you can replace either, or both, of these default types of certificates with your own custom certificates.

Supported types of custom server certificate

The StorageGRID system supports custom server certificates encrypted with RSA or ECDSA (Elliptic Curve Digital Signature Algorithm).

For more information on how StorageGRID secures client connections for the REST API, see the S3 or Swift implementation guides.

Certificates for load balancer endpoints

StorageGRID manages the certificates used for load balancer endpoints separately. To configure load balancer certificates, see the instructions for configuring load balancer endpoints.

Related information

Use S3

Use Swift

Configuring load balancer endpoints

Configuring a custom server certificate for the Grid Manager and the Tenant Manager

You can replace the default StorageGRID server certificate with a single custom server certificate that allows users to access the Grid Manager and the Tenant Manager without encountering security warnings.

About this task

By default, every Admin Node is issued a certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom server certificate and corresponding private key.

Because a single custom server certificate is used for all Admin Nodes, you must specify the certificate as a wildcard or multi-domain certificate if clients need to verify the hostname when connecting to the Grid Manager and Tenant Manager. Define the custom certificate such that it matches all Admin Nodes in the grid.

You need to complete configuration on the server, and depending on the root Certificate Authority (CA) you are

using, users might also need to install the root CA certificate in the web browser they will use to access the Grid Manager and the Tenant Manager.

> (i) To ensure that operations are not disrupted by a failed server certificate, the **Expiration of server certificate for Management Interface** alert and the legacy Management Interface Certificate Expiry (MCEP) alarm are both triggered when this server certificate is about to expire. As required, you can view the number of days until the current service certificate expires by selecting **Support** > **Tools** > **Grid Topology**. Then, select *primary Admin Node* > **CMN** > **Resources**.

> (i) If you are accessing the Grid Manager or Tenant Manager using a domain name instead of an IP address, the browser shows a certificate error without an option to bypass if either of the following occurs:
>
> - Your custom management interface server certificate expires.
> - You revert from a custom management interface server certificate to the default server certificate.

Steps

1. Select **Configuration** > **Network Settings** > **Server Certificates**.

2. In the Management Interface Server Certificate section, click **Install Custom Certificate**.

3. Upload the required server certificate files:

   ◦ **Server Certificate**: The custom server certificate file (`.crt`).

   ◦ **Server Certificate Private Key**: The custom server certificate private key file (`.key`).

   > (i) EC private keys must be 224 bits or larger. RSA private keys must be 2048 bits or larger.

   ◦ **CA Bundle**: A single file containing the certificates from each intermediate issuing Certificate Authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.

4. Click **Save**.

   The custom server certificates are used for all subsequent new client connections.

   Select a tab to display detailed information about the default StorageGRID server certificate or a CA signed certificate that was uploaded.

   > (i) After uploading a new certificate, allow up to one day for any related certificate expiration alerts (or legacy alarms) to clear.

5. Refresh the page to ensure the web browser is updated.

Restoring the default server certificates for the Grid Manager and the Tenant Manager

You can revert to using the default server certificates for the Grid Manager and the Tenant Manager.

Steps

1. Select **Configuration** > **Network Settings** > **Server Certificates**.

2. In the Manage Interface Server Certificate section, click **Use Default Certificates**.

3. Click **OK** in the confirmation dialog box.

   When you restore the default server certificates, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default server certificates are used for all subsequent new client connections.

4. Refresh the page to ensure the web browser is updated.

Configuring a custom server certificate for connections to the Storage Node or the CLB service

You can replace the server certificate that is used for S3 or Swift client connections to the Storage Node or to the CLB service (deprecated) on Gateway Node. The replacement custom server certificate is specific to your organization.

About this task

By default, every Storage Node is issued a X.509 server certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom server certificate and corresponding private key.

A single custom server certificate is used for all Storage Nodes, so you must specify the certificate as a wildcard or multi-domain certificate if clients need to verify the hostname when connecting to the storage endpoint. Define the custom certificate such that it matches all Storage Nodes in the grid.

After completing configuration on the server, users might also need to install the root CA certificate in the S3 or Swift API client they will use to access the system, depending on the root Certificate Authority (CA) you are using.

> (i) To ensure that operations are not disrupted by a failed server certificate, the **Expiration of server certificate for Storage API Endpoints** alert and the legacy Storage API Service Endpoints Certificate Expiry (SCEP) alarm are both triggered when the root server certificate is about to expire. As required, you can view the number of days until the current service certificate expires by selecting **Support** > **Tools** > **Grid Topology**. Then, select *primary Admin Node* > **CMN** > **Resources**.

The custom certificates are only used if clients connect to StorageGRID using the deprecated CLB service on Gateway Nodes, or if they connect directly to Storage Nodes. S3 or Swift clients that connect to StorageGRID using the Load Balancer service on Admin Nodes or Gateway Nodes use the certificate configured for the load balancer endpoint.

> (i) The **Expiration of load balancer endpoint certificate** alert is triggered for load balancer endpoints that will expire soon.

Steps

1. Select **Configuration** > **Network Settings** > **Server Certificates**.

2. In the Object Storage API Service Endpoints Server Certificate section, click **Install Custom Certificate**.

3. Upload the required server certificate files:

   ◦ **Server Certificate**: The custom server certificate file (`.crt`).

- **Server Certificate Private Key**: The custom server certificate private key file (`.key`).

  (i) EC private keys must be 224 bits or larger. RSA private keys must be 2048 bits or larger.

  - **CA Bundle**: A single file containing the certificates from each intermediate issuing Certificate Authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.

4. Click **Save**.

   The custom server certificate is used for all subsequent new API client connections.

   Select a tab to display detailed information about the default StorageGRID server certificate or a CA signed certificate that was uploaded.

   (i) After uploading a new certificate, allow up to one day for any related certificate expiration alerts (or legacy alarms) to clear.

5. Refresh the page to ensure the web browser is updated.

Related information

Use S3

Use Swift

Configuring S3 API endpoint domain names

Restoring the default server certificates for the S3 and Swift REST API endpoints

You can revert to using the default server certificates for the S3 and Swift REST API endpoints.

Steps

1. Select **Configuration** > **Network Settings** > **Server Certificates**.
2. In the Object Storage API Service Endpoints Server Certificate section, click **Use Default Certificates**.
3. Click **OK** in the confirmation dialog box.

   When you restore the default server certificates for the object storage API endpoints, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default server certificates are used for all subsequent new API client connections.

4. Refresh the page to ensure the web browser is updated.

Copying the StorageGRID system's CA certificate

StorageGRID uses an internal Certificate Authority (CA) to secure internal traffic. This certificate does not change if you upload your own certificates.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have specific access permissions.

About this task

If a custom server certificate has been configured, client applications should verify the server using the custom server certificate. They should not copy the CA certificate from the StorageGRID system.

Steps

1. Select **Configuration** > **Network Settings** > **Server Certificates**.

2. In the **Internal CA Certificate** section, select all of the certificate text.

   You must include `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` in your selection.
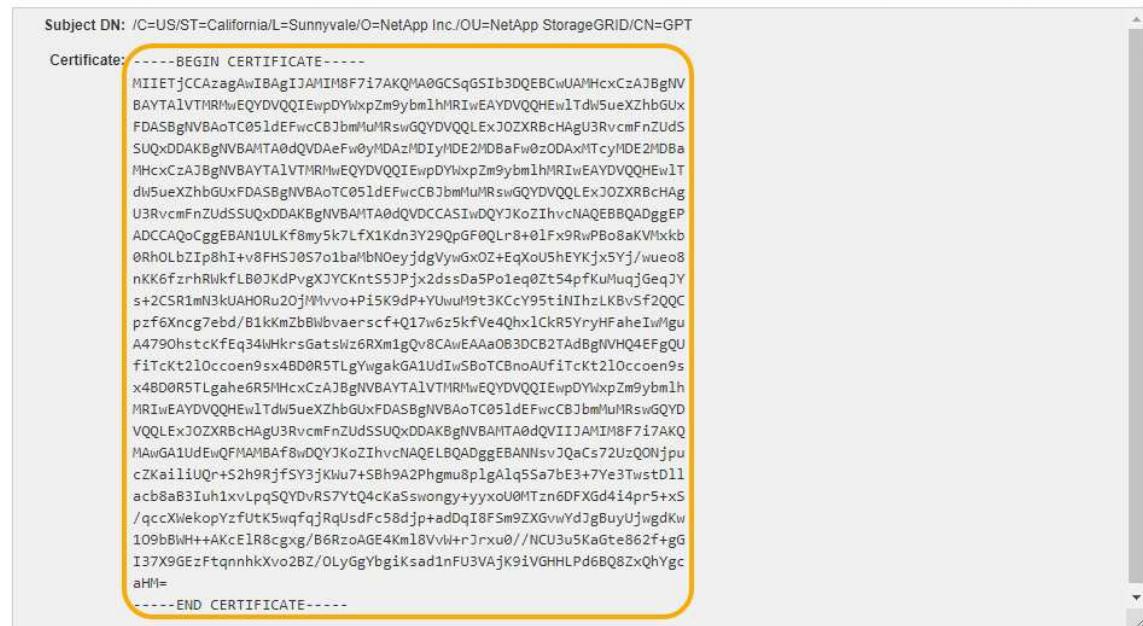
3. Right-click the selected text, and select **Copy**.

4. Paste the copied certificate into a text editor.

5. Save the file with the extension `.pem`.

   For example: `storagegrid_certificate.pem`

Configuring StorageGRID certificates for FabricPool

For S3 clients that perform strict hostname validation and do not support disabling strict hostname validation, such as ONTAP clients using FabricPool, you can generate or upload a server certificate when you configure the load balancer endpoint.

What you'll need

- You must have specific access permissions.
- You must be signed in to the Grid Manager using a supported browser.

About this task

When you create a load balancer endpoint, you can generate a self-signed server certificate or upload a certificate that is signed by a known Certificate Authority (CA). In production environments, you should use a certificate that is signed by a known CA. Certificates signed by a CA can be rotated non-disruptively. They are also more secure because they provide better protection against man-in-the-middle attacks.

The following steps provide general guidelines for S3 clients that use FabricPool. For more detailed information and procedures, see the instructions for configuring StorageGRID for FabricPool.

> ⓘ The separate Connection Load Balancer (CLB) service on Gateway Nodes is deprecated and no longer recommended for use with FabricPool.

Steps

1. Optionally, configure a high availability (HA) group for FabricPool to use.

2. Create an S3 load balancer endpoint for FabricPool to use.

   When you create an HTTPS load balancer endpoint, you are prompted to upload your server certificate, certificate private key, and CA bundle.

3. Attach StorageGRID as a cloud tier in ONTAP.

   Specify the load balancer endpoint port and the fully qualified domain name used in the CA certificate you uploaded. Then, provide the CA certificate.

   > ⓘ If an intermediate CA issued the StorageGRID certificate, you must provide the intermediate CA certificate. If the StorageGRID certificate was issued directly by the Root CA, you must provide the Root CA certificate.

Related information

Configure StorageGRID for FabricPool

Generating a self-signed server certificate for the management interface

You can use a script to generate a self-signed server certificate for management API clients that require strict hostname validation.

What you'll need

- You must have specific access permissions.
- You must have the `Passwords.txt` file.

About this task

In production environments, you should use a certificate that is signed by a known Certificate Authority (CA). Certificates signed by a CA can be rotated non-disruptively. They are also more secure because they provide better protection against man-in-the-middle attacks.

Steps

1. Obtain the fully qualified domain name (FQDN) of each Admin Node.

2. Log in to the primary Admin Node:

   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

c. Enter the following command to switch to root: `su -`

d. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

3. Configure StorageGRID with a new self-signed certificate.

   `$ sudo make-certificate --domains` *wildcard-admin-node-fqdn* `--type management`

   ○ For `--domains`, use wildcards to represent the fully qualified domain names of all Admin Nodes. For example, `*.ui.storagegrid.example.com` uses the `*` wildcard to represent `admin1.ui.storagegrid.example.com` and `admin2.ui.storagegrid.example.com`.

   ○ Set `--type` to `management` to configure the certificate used by Grid Manager and Tenant Manager.

   ○ By default, generated certificates are valid for one year (365 days) and must be recreated before they expire. You can use the `--days` argument to override the default validity period.

   > ⓘ A certificate's validity period begins when `make-certificate` is run. You must ensure the management API client is synchronized to the same time source as StorageGRID; otherwise, the client might reject the certificate.

   ```
   $ sudo make-certificate --domains *.ui.storagegrid.example.com --type
   management --days 365
   ```

   The resulting output contains the public certificate needed by your management API client.

4. Select and copy the certificate.

   Include the BEGIN and the END tags in your selection.

5. Log out of the command shell. `$ exit`

6. Confirm the certificate was configured:

   a. Access the Grid Manager.

   b. Select **Configuration** > **Server Certificates** > **Management Interface Server Certificate**.

7. Configure your management API client to use the public certificate you copied. Include the BEGIN and END tags.

Configuring Storage proxy settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy between Storage Nodes and the external S3 endpoints. For example, you might need a non-transparent proxy to allow platform services messages to be sent to external endpoints, such as an endpoint on the internet.

What you'll need
- You must have specific access permissions.

- You must be signed in to the Grid Manager using a supported browser.

About this task

You can configure the settings for a single Storage proxy.

Steps

1. Select **Configuration** > **Network Settings** > **Proxy Settings**.

   The Storage Proxy Settings page appears. By default, **Storage** is selected in the sidebar menu.

   Proxy Settings
Storage
Admin
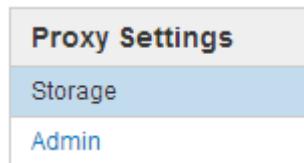
2. Select the **Enable Storage Proxy** check box.

   The fields for configuring a Storage proxy appear.

   Storage Proxy Settings
   If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy	☑
Protocol	○ HTTP ○ SOCKS5
Hostname	
Port (optional)	

   Save

3. Select the protocol for the non-transparent Storage proxy.

4. Enter the hostname or IP address of the proxy server.

5. Optionally, enter the port used to connect to the proxy server.

   You can leave this field blank if you use the default port for the protocol: 80 for HTTP or 1080 for SOCKS5.

6. Click **Save**.

   After the Storage proxy is saved, new endpoints for platform services or Cloud Storage Pools can be configured and tested.

   > ⓘ Proxy changes can take up to 10 minutes to take effect.

7. Check the settings of your proxy server to ensure that platform service-related messages from StorageGRID will not be blocked.

After you finish

If you need to disable a Storage proxy, deselect the **Enable Storage Proxy** check box, and click **Save**.

Configuring Admin proxy settings

If you send AutoSupport messages using HTTP or HTTPS, you can configure a non-transparent proxy server between Admin Nodes and technical support (AutoSupport).

What you'll need
- You must have specific access permissions.
- You must be signed in to the Grid Manager using a supported browser.

About this task

You can configure the settings for a single Admin proxy.

Steps

1. Select **Configuration** > **Network Settings** > **Proxy Settings**.

   The Admin Proxy Settings page appears. By default, **Storage** is selected in the sidebar menu.

2. From the sidebar menu, select **Admin**.

   Proxy Settings

Storage
Admin
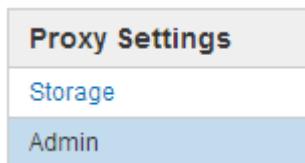
3. Select the **Enable Admin Proxy** check box.

   Admin Proxy Settings

   If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy	☑
Hostname	myproxy.example.com
Port	8080
Username (optional)	root
Password (optional)	••••••••
	Save

4. Enter the hostname or IP address of the proxy server.

5. Enter the port used to connect to the proxy server.

6. Optionally, enter the proxy username.

   Leave this field blank if your proxy server does not require a username.

7. Optionally, enter the proxy password.

   Leave this field blank if your proxy server does not require a password.

8. Click **Save**.

   After the Admin proxy is saved, the proxy server between Admin Nodes and technical support is configured.

   > ℹ️ Proxy changes can take up to 10 minutes to take effect.

9. If you need to disable the proxy, deselect the **Enable Admin Proxy** check box, and click **Save**.

Related information

Specifying the protocol for AutoSupport messages

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.

   Traffic Classification Policies

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

+ Create	✏ Edit	✖ Remove	ᐧ�障 Metrics

Name	Description	ID

   No policies found.

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

      The Create Matching Rule dialog box appears.

Create Matching Rule

Matching Rules

Type ❓ | -- Choose One -- ⌄
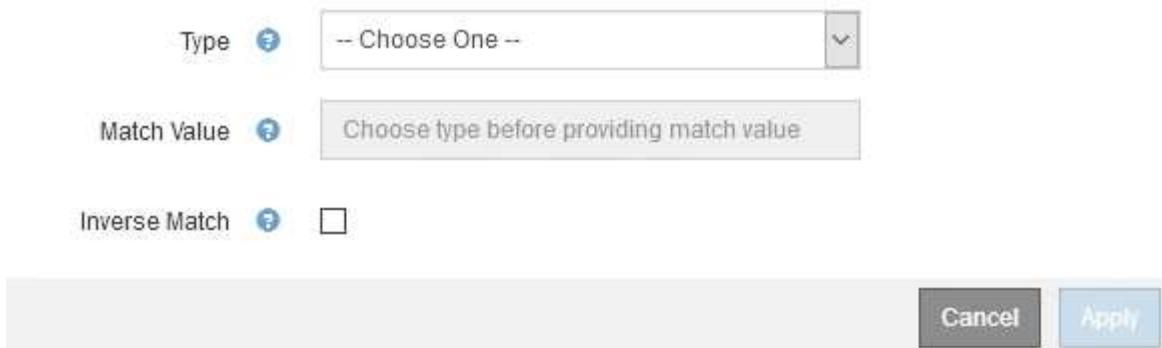
Match Value ❓ | Choose type before providing match value

Inverse Match ❓ ☐

Cancel   Apply

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.

    (i)   Traffic that matches any rule is handled by the policy.

6. Optionally, create limits for the policy.

    (i)   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.

> (i) 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.

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.

	Type	Inverse Match	Match Value
⦿	CIDR		10.10.152.0/24

Displaying 1 matching rule.

Limits (Optional)

Type	Value	Units

No limits found.

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.

   Traffic Classification Policies

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

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

   A Warning dialog box appears.

   ⚠ Warning

   Delete Policy

   Are you sure you want to delete the policy "Fabric Pools"?

   Cancel   OK

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.
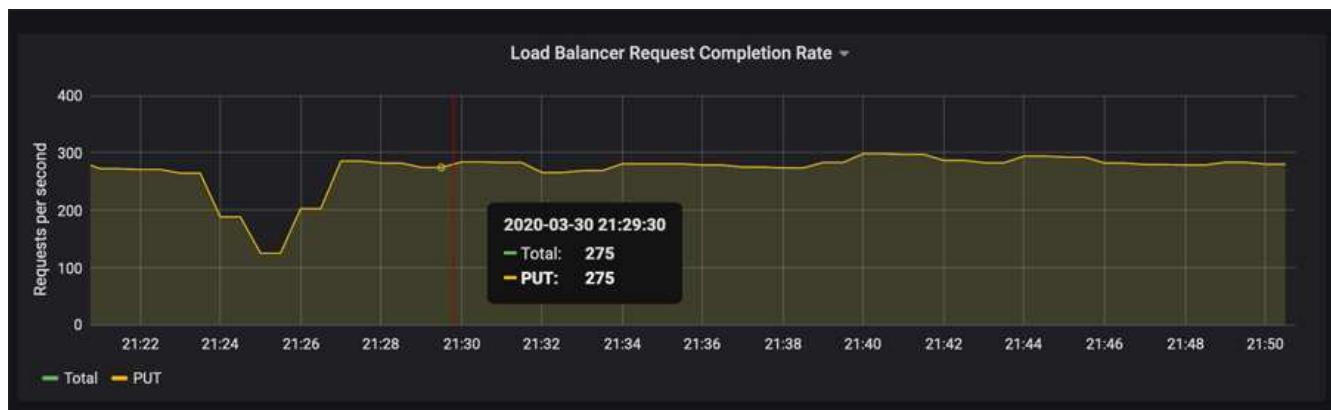
5. Hover the cursor over a heatmap to see a pop-up that shows the date and time of the sample, object sizes that are aggregated into the count, and the number of requests per second during that time period.
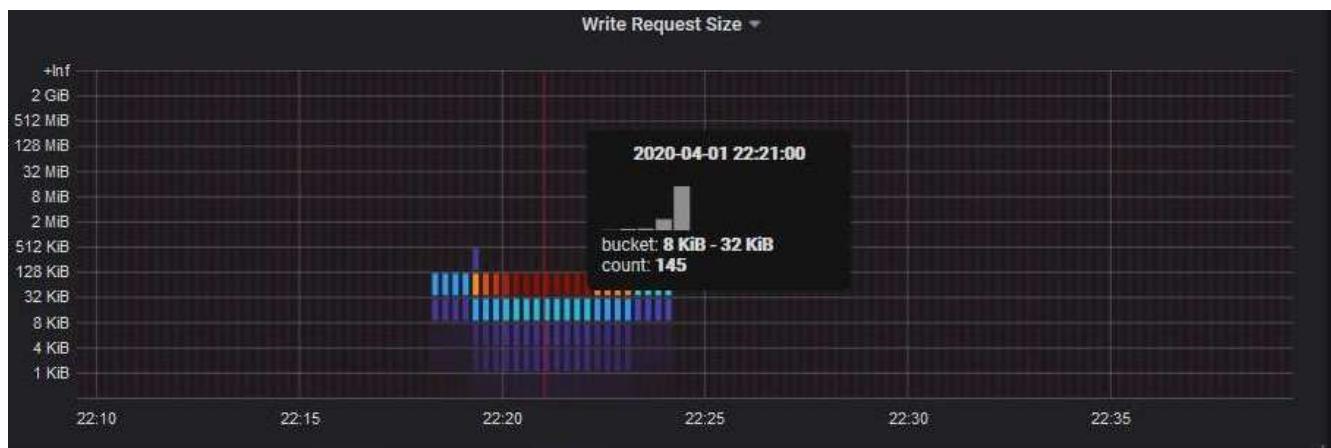
6. Use the **Policy** pull-down in the upper left to select a different policy.

   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

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 CLB service on Gateway Nodes to direct client connections.

  ⓘ   The CLB service is deprecated.

The diagram shows a three site grid that has link costs configured between sites:
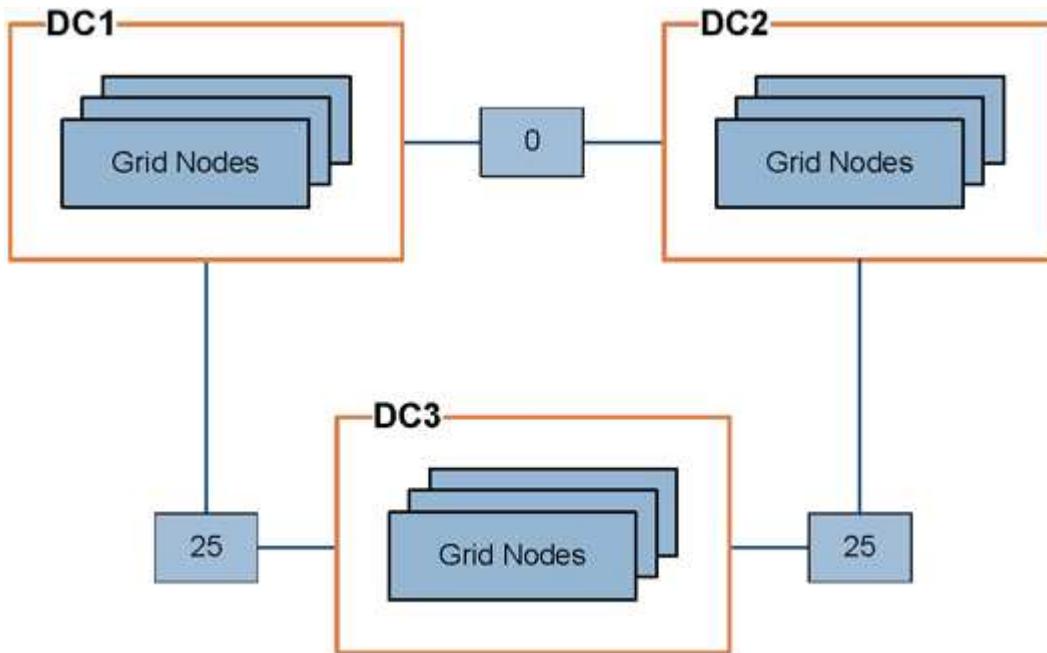
- The CLB service on Gateway Nodes equally distribute client connections to all Storage Nodes at the same data center site and to any data center sites with a link cost of 0.

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.

Related information

How load balancing works - CLB service

Updating link costs

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

What you'll need

• You must be signed in to the Grid Manager using a supported browser.

• You must have the Grid Topology Page Configuration permission.

Steps

1. Select **Configuration** > **Network Settings** > **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 50 ▼ Records Per Page   Refresh   Previous   « 1 » Next

Link Costs

| Link Source | Link Destination | | Actions |
	10	20	
▼			↺

Apply Changes ➡

---

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, click ↺ **Revert**.

3. Click **Apply Changes**.