Configuring S3 and Swift client connections

StorageGRID 11.5

NetApp
January 04, 2024

Table of Contents

Configuring S3 and Swift client connections

As a grid administrator, you manage the configuration options that control how S3 and Swift tenants can connect client applications to your StorageGRID system to store and retrieve data. There are a number of different options to meet different client and tenant requirements.

Client applications can store or retrieve objects by connecting to any of the following:

- The Load Balancer service on Admin Nodes or Gateway Nodes, or optionally, the virtual IP address of a high availability (HA) group of Admin Nodes or Gateway Nodes
- The CLB service on Gateway Nodes, or optionally, the virtual IP address of a high availability group of Gateway Nodes

> The CLB service is deprecated. Clients configured before the StorageGRID 11.3 release can continue to use the CLB service on Gateway Nodes. All other client applications that depend on StorageGRID to provide load balancing should connect using the Load Balancer service.

- Storage Nodes, with or without an external load balancer

You can optionally configure the following features on your StorageGRID system:

- **Load Balancer service**: You enable clients to use the Load Balancer service by creating load balancer endpoints for client connections. When creating a load balancer endpoint, you specify a port number, whether the endpoint accepts HTTP or HTTPS connections, the type of client (S3 or Swift) that will use the endpoint, and the certificate to be used for HTTPS connections (if applicable).
- **Untrusted Client Network**: You can make the Client Network more secure by configuring it as untrusted. When the Client Network is untrusted, clients can only connect using load balancer endpoints.
- **High availability groups**: You can create an HA group of Gateway Nodes or Admin Nodes to create an active-backup configuration, or you can use round-robin DNS or a third-party load balancer and multiple HA groups to achieve an active-active configuration. Client connections are made using the virtual IP addresses of HA groups.

You can also enable the use of HTTP for clients that connect to StorageGRID either directly to Storage Nodes or using the CLB service (deprecated), and you can configure S3 API endpoint domain names for S3 clients.

Summary: IP addresses and ports for client connections

Client applications can connect to StorageGRID using the IP address of a grid node and the port number of a service on that node. If high availability (HA) groups are configured, client applications can connect using the virtual IP address of the HA group.

About this task

This table summarizes the different ways that clients can connect to StorageGRID and the IP addresses and ports that are used for each type of connection. The instructions describe how to find this information in the Grid Manager if load balancer endpoints and high availability (HA) groups are already configured.

Where connection is made	Service that client connects to	IP address	Port
HA group	Load Balancer	Virtual IP address of an HA group	• Load balancer endpoint port
HA group	CLB **Note:** The CLB service is deprecated.	Virtual IP address of an HA group	Default S3 ports: • HTTPS: 8082 • HTTP: 8084 Default Swift ports: • HTTPS:8083 • HTTP:8085
Admin Node	Load Balancer	IP address of the Admin Node	• Load balancer endpoint port
Gateway Node	Load Balancer	IP address of the Gateway Node	• Load balancer endpoint port
Gateway Node	CLB **Note:** The CLB service is deprecated.	IP address of the Gateway Node **Note:** By default, HTTP ports for CLB and LDR are not enabled.	Default S3 ports: • HTTPS: 8082 • HTTP: 8084 Default Swift ports: • HTTPS:8083 • HTTP:8085
Storage Node	LDR	IP address of Storage Node	Default S3 ports: • HTTPS: 18082 • HTTP: 18084 Default Swift ports: • HTTPS: 18083 • HTTP:18085

Examples

To connect an S3 client to the Load Balancer endpoint of an HA group of Gateway Nodes, use a URL structured as shown below:

- `https://VIP-of-HA-group:LB-endpoint-port`

For example, if the virtual IP address of the HA group is 192.0.2.5 and the port number of an S3 Load Balancer endpoint is 10443, then an S3 client could use the following URL to connect to StorageGRID:

- `https://192.0.2.5:10443`

To connect a Swift client to the Load Balancer endpoint of an HA group of Gateway Nodes, use a URL structured as shown below:

- `https://`*`VIP-of-HA-group:LB-endpoint-port`*

For example, if the virtual IP address of the HA group is 192.0.2.6 and the port number of a Swift Load Balancer endpoint is 10444, then a Swift client could use the following URL to connect to StorageGRID:

- `https://192.0.2.6:10444`

It is possible to configure a DNS name for the IP address that clients use to connect to StorageGRID. Contact your local network administrator.

Steps

1. Sign in to the Grid Manager using a supported browser.
2. To find the IP address of a grid node:
   a. Select **Nodes**.
   b. Select the Admin Node, Gateway Node, or Storage Node to which you want to connect.
   c. Select the **Overview** tab.
   d. In the Node Information section, note the IP addresses for the node.
   e. Click **Show more** to view IPv6 addresses and interface mappings.

      You can establish connections from client applications to any of the IP addresses in the list:

      - **eth0:** Grid Network
      - **eth1:** Admin Network (optional)
      - **eth2:** Client Network (optional)

      > If you are viewing an Admin Node or a Gateway Node and it is the active node in a high availability group, the virtual IP address of the HA group is shown on eth2.
3. To find the virtual IP address of a high availability group:
   a. Select **Configuration** > **Network Settings** > **High Availability Groups**.
   b. In the table, note the virtual IP address of the HA group.
4. To find the port number of a Load Balancer endpoint:
   a. Select **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

      The Load Balancer Endpoints page appears, showing the list of endpoints that have already been configured.
   b. Select an endpoint, and click **Edit endpoint**.

      The Edit Endpoint window opens and displays additional details about the endpoint.

c. Confirm that the endpoint you have selected is configured for use with the correct protocol (S3 or Swift), then click **Cancel**.

d. Note the port number for the endpoint that you want to use for a client connection.

> ⓘ If the port number is 80 or 443, the endpoint is configured only on Gateway Nodes, since those ports are reserved on Admin Nodes. All other ports are configured on both Gateway Nodes and Admin Nodes.

Managing load balancing

You can use the StorageGRID load balancing functions to handle ingest and retrieval workloads from S3 and Swift clients. Load balancing maximizes speed and connection capacity by distributing the workloads and connections across multiple Storage Nodes.

You can achieve load balancing in your StorageGRID system in the following ways:

- Use the Load Balancer service, which is installed on Admin Nodes and Gateway Nodes. The Load Balancer service provides Layer 7 load balancing and performs TLS termination of client requests, inspects the requests, and establishes new secure connections to the Storage Nodes. This is the recommended load balancing mechanism.
- Use the Connection Load Balancer (CLB) service, which is installed on Gateway Nodes only. The CLB service provides Layer 4 load balancing and supports link costs.

  > ⓘ The CLB service is deprecated.

- Integrate a third-party load balancer. Contact your NetApp account representative for details.

How load balancing works - Load Balancer service

The Load Balancer service distributes incoming network connections from client applications to Storage Nodes. To enable load balancing, you must configure load balancer endpoints using the Grid Manager.

You can configure load balancer endpoints only for Admin Nodes or Gateway Nodes, since these node types contain the Load Balancer service. You cannot configure endpoints for Storage Nodes or Archive Nodes.

Each load balancer endpoint specifies a port, a protocol (HTTP or HTTPS), a service type (S3 or Swift), and a binding mode. HTTPS endpoints require a server certificate. Binding modes allow you to restrict the accessibility of endpoint ports to:

- Specific high availability (HA) virtual IP addresses (VIPs)
- Specific network interfaces of specific nodes

Port considerations

Clients can access any of the endpoints you configure on any node running the Load Balancer service, with two exceptions: ports 80 and 443 are reserved on Admin Nodes, so endpoints configured on these ports support load balancing operations only on Gateway Nodes.

If you have remapped any ports, you cannot use the same ports to configure load balancer endpoints. You can create endpoints using remapped ports, but those endpoints will be remapped to the original CLB ports and service, not the Load Balancer service. Follow the steps in the recovery and maintenance instructions for removing port remaps.

> The CLB service is deprecated.

CPU availability

The Load Balancer service on each Admin Node and Gateway Node operates independently when forwarding S3 or Swift traffic to the Storage Nodes. Through a weighting process, the Load Balancer service routes more requests to Storage Nodes with higher CPU availability. Node CPU load information is updated every few minutes, but weighting might be updated more frequently. All Storage Nodes are assigned a minimal base weight value, even if a node reports 100% utilization or fails to report its utilization.

In some cases, information about CPU availability is limited to the site where the Load Balancer service is located.

Related information

Maintain & recover

Configuring load balancer endpoints

You can create, edit, and remove load balancer endpoints.

Creating load balancer endpoints

Each load balancer endpoint specifies a port, a network protocol (HTTP or HTTPS), and a service type (S3 or Swift). If you create an HTTPS endpoint, you must upload or generate a server certificate.

What you'll need

- You must have the Root Access permission.
- You must be signed in to the Grid Manager using a supported browser.
- If you have previously remapped ports you intend to use for the Load Balancer service, you must have removed the remaps.

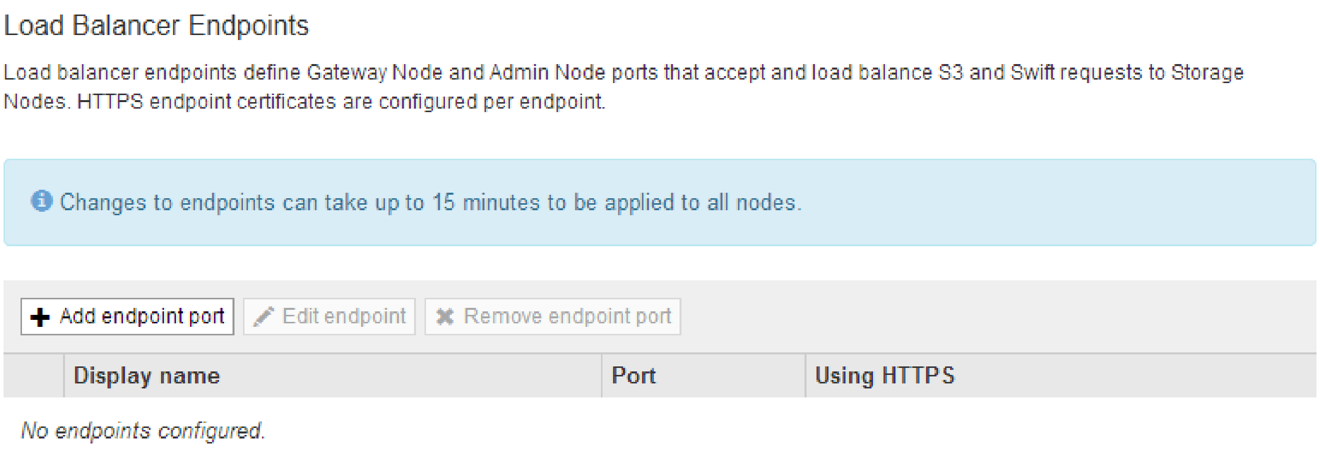
  > If you have remapped any ports, you cannot use the same ports to configure load balancer endpoints. You can create endpoints using remapped ports, but those endpoints will be remapped to the original CLB ports and service, not the Load Balancer service. Follow the steps in the recovery and maintenance instructions for removing port remaps.

  > The CLB service is deprecated.

Steps

1. Select **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   The Load Balancer Endpoints page appears.



Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

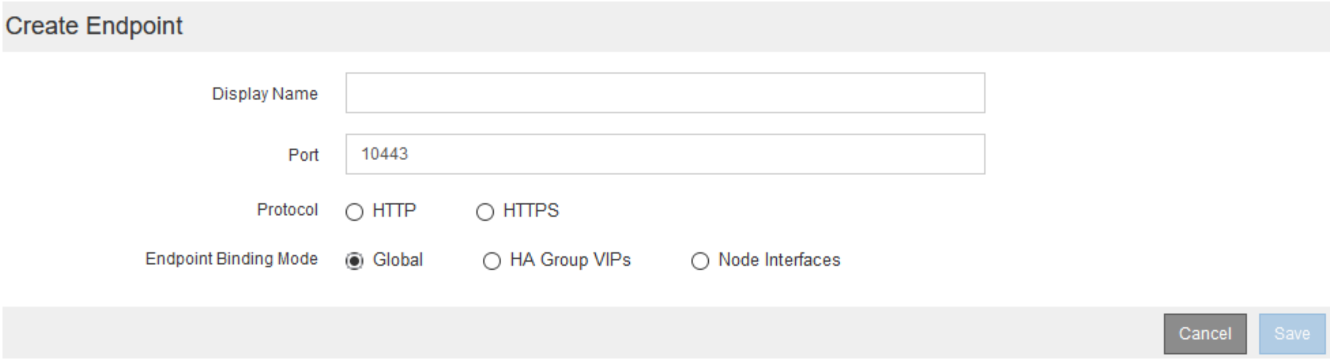
Changes to endpoints can take up to 15 minutes to be applied to all nodes.

Display name	Port	Using HTTPS

No endpoints configured.

2. Select **Add endpoint**.

   The Create Endpoint dialog box appears.



Create Endpoint

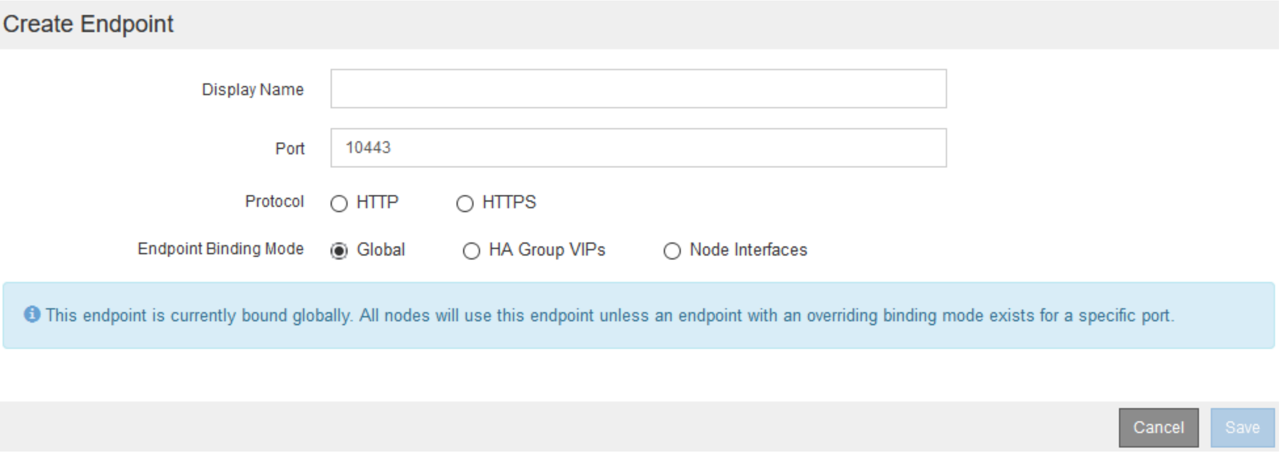
Display Name	
Port	10443
Protocol	○ HTTP ○ HTTPS
Endpoint Binding Mode	● Global ○ HA Group VIPs ○ Node Interfaces

3. Enter a display name for the endpoint, which will appear in the list on the Load Balancer Endpoints page.
4. Enter a port number, or leave the pre-filled port number as is.

   If you enter port number 80 or 443, the endpoint is configured only on Gateway Nodes, since these ports are reserved on Admin Nodes.

   > Ports used by other grid services are not permitted. See the networking guidelines for a list of ports used for internal and external communications.

5. Select **HTTP** or **HTTPS** to specify the network protocol for this endpoint.
6. Select an endpoint binding mode.
   - **Global** (default): The endpoint is accessible on all Gateway Nodes and Admin Nodes on the specified port number.

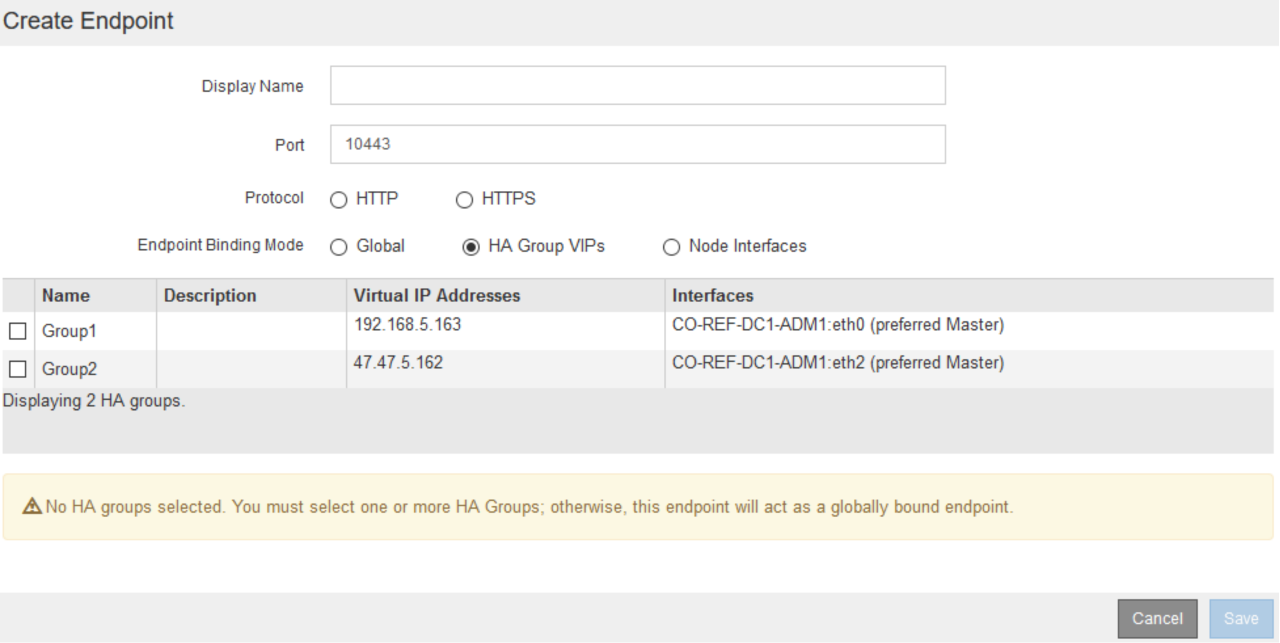

Create Endpoint

Display Name	
Port	10443
Protocol	○ HTTP ○ HTTPS
Endpoint Binding Mode	● Global ○ HA Group VIPs ○ Node Interfaces

This endpoint is currently bound globally. All nodes will use this endpoint unless an endpoint with an overriding binding mode exists for a specific port.

- **HA Group VIPs**: The endpoint is accessible only through the virtual IP addresses defined for the selected HA groups. Endpoints defined in this mode can reuse the same port number, as long as the HA groups defined by those endpoints do not overlap with each other.

  Select the HA groups with the virtual IP addresses where you want the endpoint to appear.


Create Endpoint

Display Name	
Port	10443
Protocol	○ HTTP ○ HTTPS
Endpoint Binding Mode	○ Global ● HA Group VIPs ○ Node Interfaces

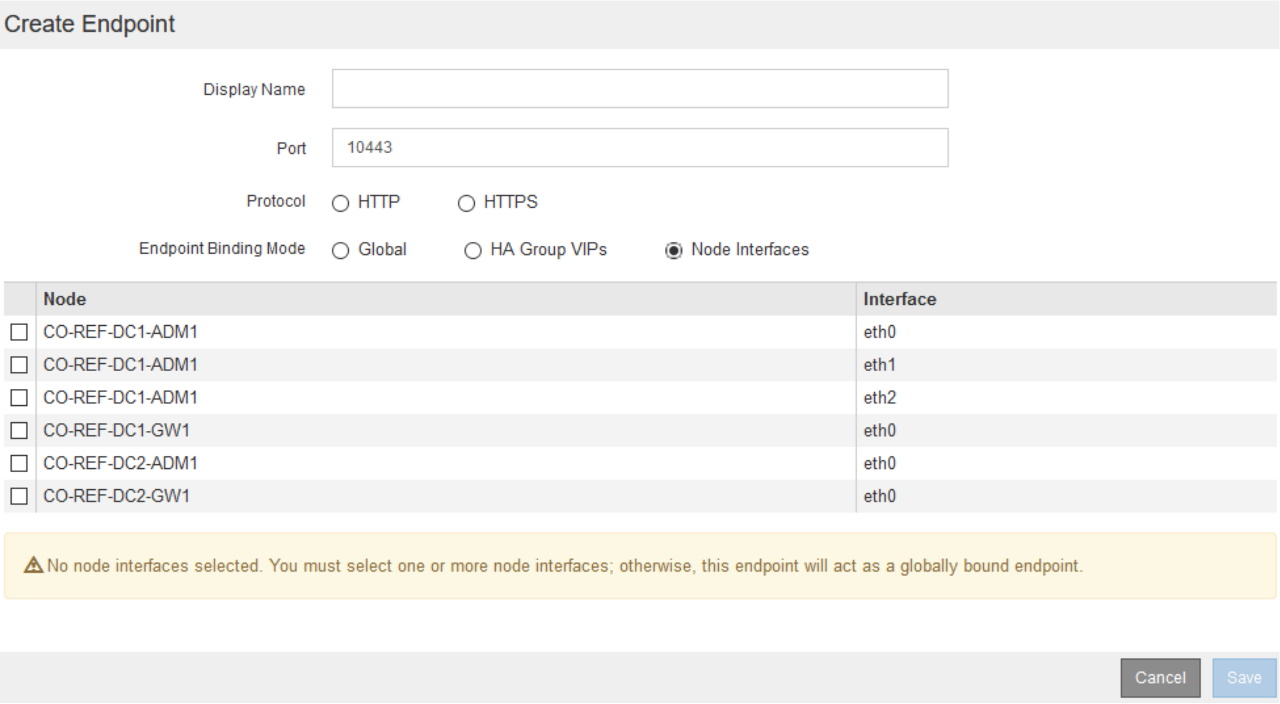
	Name	Description	Virtual IP Addresses	Interfaces
□	Group1		192.168.5.163	CO-REF-DC1-ADM1:eth0 (preferred Master)
□	Group2		47.47.5.162	CO-REF-DC1-ADM1:eth2 (preferred Master)

Displaying 2 HA groups.

⚠ No HA groups selected. You must select one or more HA Groups; otherwise, this endpoint will act as a globally bound endpoint.

- **Node Interfaces**: The endpoint is accessible only on the designated nodes and network interfaces. Endpoints defined in this mode can reuse the same port number as long as those interfaces do not overlap with each other.

  Select the node interfaces where you want the endpoint to appear.



Create Endpoint

Display Name

Port 10443

Protocol ○ HTTP ○ HTTPS

Endpoint Binding Mode ○ Global ○ HA Group VIPs ● Node Interfaces

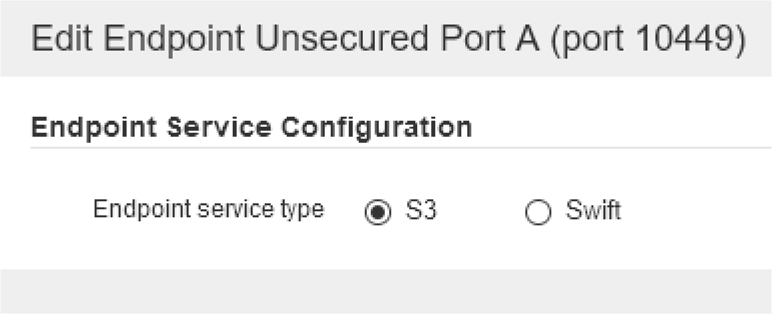
	Node	Interface
□	CO-REF-DC1-ADM1	eth0
□	CO-REF-DC1-ADM1	eth1
□	CO-REF-DC1-ADM1	eth2
□	CO-REF-DC1-GW1	eth0
□	CO-REF-DC2-ADM1	eth0
□	CO-REF-DC2-GW1	eth0

⚠ No node interfaces selected. You must select one or more node interfaces; otherwise, this endpoint will act as a globally bound endpoint.

7. Select **Save**.

   The Edit Endpoint dialog box appears.

8. Select **S3** or **Swift** to specify the type of traffic this endpoint will serve.



Edit Endpoint Unsecured Port A (port 10449)

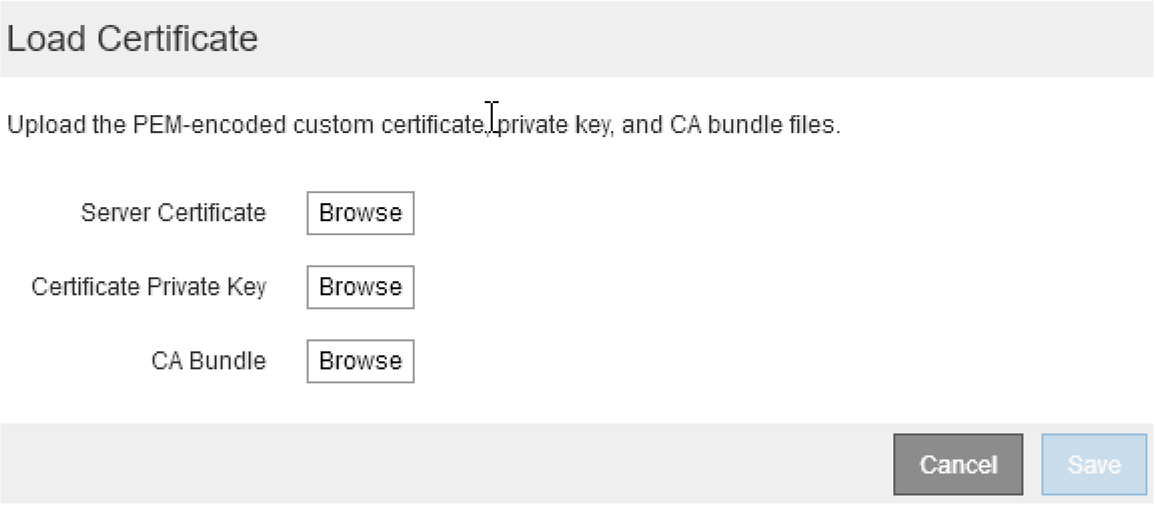
Endpoint Service Configuration

Endpoint service type ● S3 ○ Swift

9. If you selected **HTTP**, select **Save**.

   The unsecured endpoint is created. The table on the Load Balancer Endpoints page lists the endpoint’s display name, port number, protocol, and endpoint ID.

10. If you selected **HTTPS** and you want to upload a certificate, select **Upload Certificate**.



Load Certificate

Upload the PEM-encoded custom certificate, private key, and CA bundle files.

a. Browse for the server certificate and the certificate private key.

   To enable S3 clients to connect using an S3 API endpoint domain name, use a multi-domain or wildcard certificate that matches all domain names that the client might use to connect to the grid. For example, the server certificate might use the domain name `*.`*`example`*`.com`.

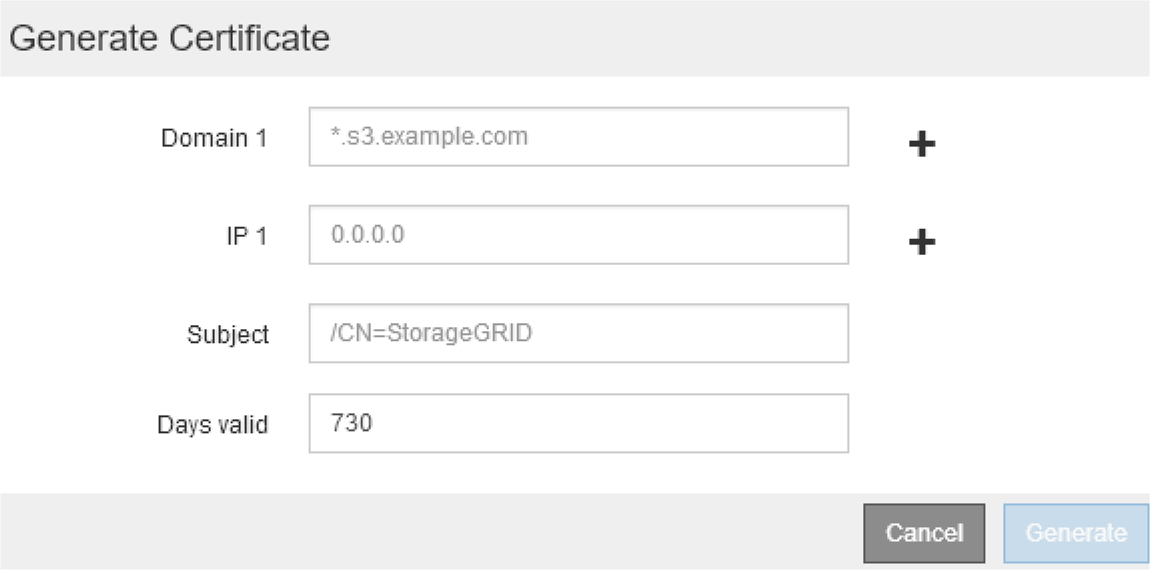
   Configuring S3 API endpoint domain names

b. Optionally browse for a CA bundle.

c. Select **Save**.

   The PEM-encoded certificate data for the endpoint appears.

11. If you selected **HTTPS** and you want to generate a certificate, select **Generate Certificate**.



Generate Certificate

Domain 1: *.s3.example.com

IP 1: 0.0.0.0

Subject: /CN=StorageGRID

Days valid: 730

a. Enter a domain name or an IP address.

   You can use wildcards to represent the fully qualified domain names of all Admin Nodes and Gateway Nodes running the Load Balancer service. For example, `*.sgws.foo.com` uses the * wildcard to represent `gn1.sgws.foo.com` and `gn2.sgws.foo.com`.

Configuring S3 API endpoint domain names

b. Select ➕ to add any other domain names or IP addresses.

   If you are using high availability (HA) groups, add the domain names and IP addresses of the HA virtual IPs.

c. Optionally, enter an X.509 subject, also referred to as the Distinguished Name (DN), to identify who owns the certificate.

d. Optionally, select the number of days the certificate is valid. The default is 730 days.

e. Select **Generate**.

   The certificate metadata and the PEM-encoded certificate data for the endpoint appear.

12. Click **Save**.

    The endpoint is created. The table on the Load Balancer Endpoints page lists the endpoint’s display name, port number, protocol, and endpoint ID.

Related information

Maintain & recover

Network guidelines

Managing high availability groups

Managing untrusted Client Networks

Editing load balancer endpoints

For an unsecured (HTTP) endpoint, you can change the endpoint service type between S3 and Swift. For a secured (HTTPS) endpoint, you can edit the endpoint service type and view or change the security certificate.

What you’ll need

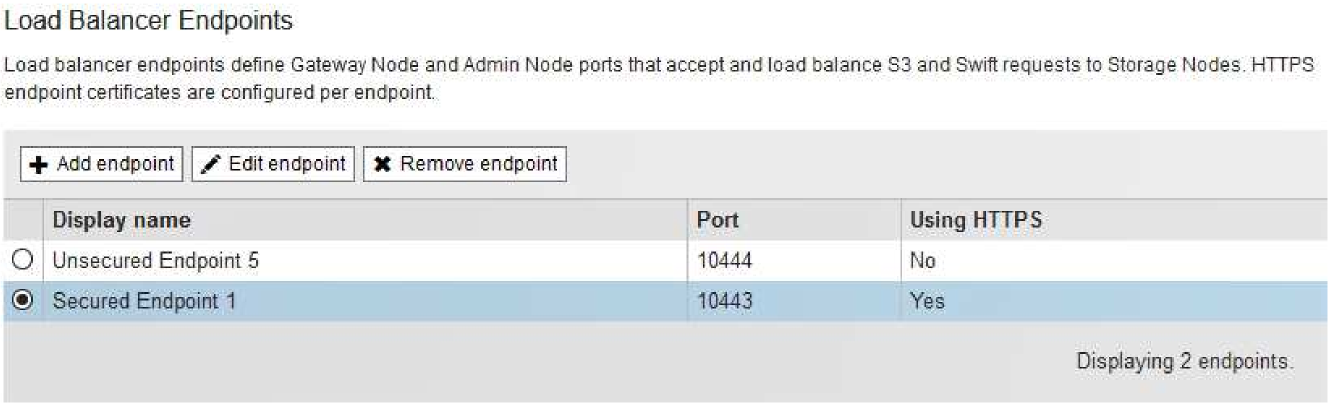
- You must have the Root Access permission.
- You must be signed in to the Grid Manager using a supported browser.

Steps

1. Select **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   The Load Balancer Endpoints page appears. The existing endpoints are listed in the table.

   Endpoints with certificates that will expire soon are identified in the table.



Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

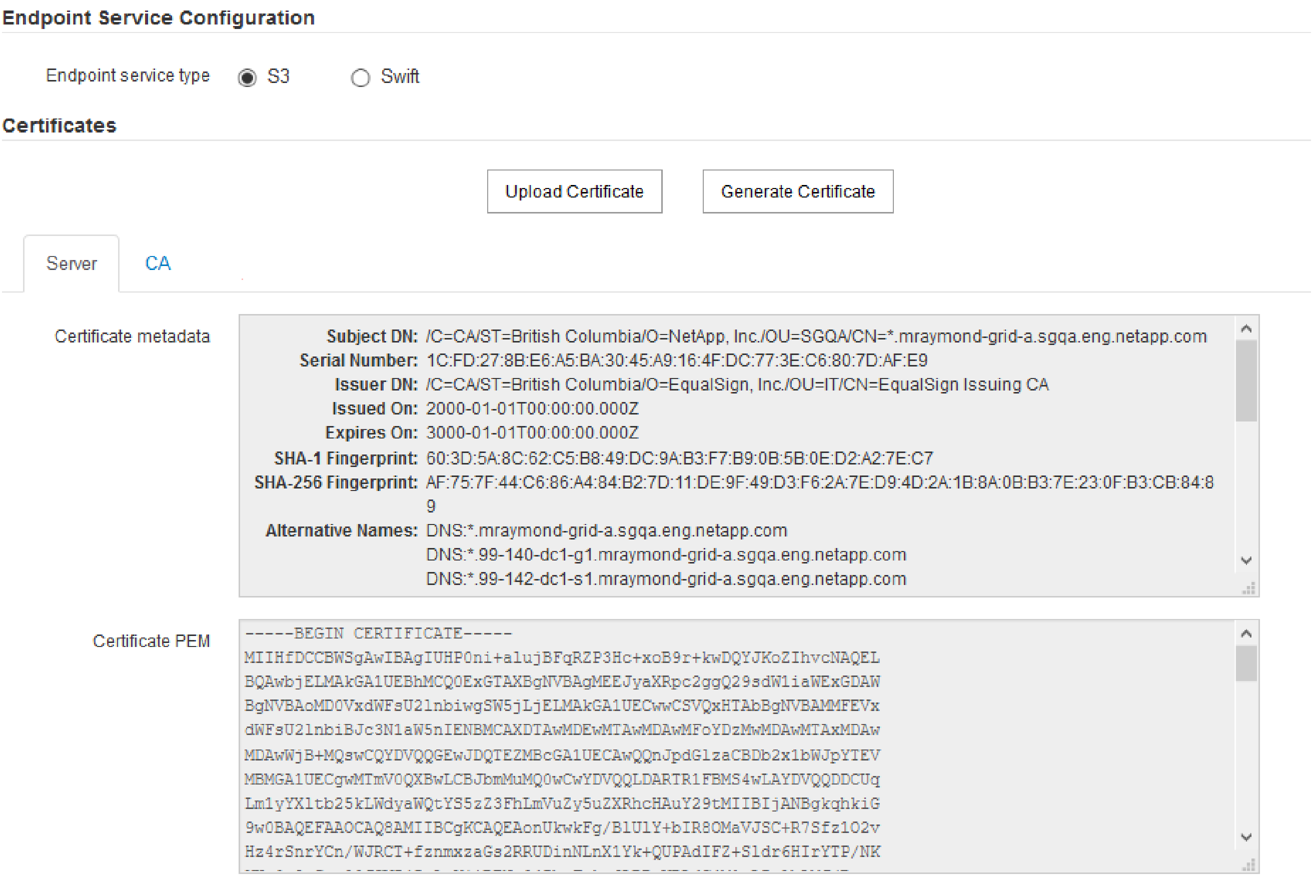
	Display name	Port	Using HTTPS
○	Unsecured Endpoint 5	10444	No
●	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

2. Select the endpoint you want to edit.
3. Click **Edit endpoint**.

   The Edit Endpoint dialog box appears.

   For an unsecured (HTTP) endpoint, only the Endpoint Service Configuration section of the dialog box appears. For a secured (HTTPS) endpoint, the Endpoint Service Configuration and the Certificates sections of the dialog box appear, as shown in the following example.



Endpoint Service Configuration

Endpoint service type ● S3 ○ Swift

Certificates

Certificate metadata

Subject DN:	/C=CA/ST=British Columbia/O=NetApp, Inc./OU=SGQA/CN=*.mraymond-grid-a.sgqa.eng.netapp.com
Serial Number:	1C:FD:27:8B:E6:A5:BA:30:45:A9:16:4F:DC:77:3E:C6:80:7D:AF:E9
Issuer DN:	/C=CA/ST=British Columbia/O=EqualSign, Inc./OU=IT/CN=EqualSign Issuing CA
Issued On:	2000-01-01T00:00:00.000Z
Expires On:	3000-01-01T00:00:00.000Z
SHA-1 Fingerprint:	60:3D:5A:8C:62:C5:B8:49:DC:9A:B3:F7:B9:0B:5B:0E:D2:A2:7E:C7
SHA-256 Fingerprint:	AF:75:7F:44:C6:86:A4:84:B2:7D:11:DE:9F:49:D3:F6:2A:7E:D9:4D:2A:1B:8A:0B:B3:7E:23:0F:B3:CB:84:89
Alternative Names:	DNS:*.mraymond-grid-a.sgqa.eng.netapp.com DNS:*.99-140-dc1-g1.mraymond-grid-a.sgqa.eng.netapp.com DNS:*.99-142-dc1-s1.mraymond-grid-a.sgqa.eng.netapp.com

Certificate PEM

```
-----BEGIN CERTIFICATE-----
MIIHfDCCBWSgAwIBAgIUHP0ni+alujBFqRZP3Hc+xoB9r+kwDQYJKoZIhvcNAQEL
BQAwbjELMAkGA1UEBhMCQ0ExGTAXBgNVBAgMEEJyaXRpc2ggQ29sdW1iaWExGDAW
BgNVBAoMD0VxdWFsU2lnbiwgSW5jLjELMAkGA1UECwwCSVQxHTAbBgNVBAMMFEVx
dWFsU2lnbiBJc3N1aW5nIENBMCAXDTAwMDEwMTAwMDAwMFoYDzMwMDAwMTAxMDAw
MDAwWjB+MQswCQYDVQQGEwJDQTEZMBcGA1UECAwQQnJpdGlzaCBDb2x1bWJpYTEV
MBMGA1UECgwMTmV0QXBwLCBJbmMuMQ0wCwYDVQQLDARTR1FBMS4wLAYDVQQDDCUq
Lm1yYXltb25kLWdyaWQtYS5zZ3FhLmVuZy5uZXRhcHAuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAonUkwkFg/B1U1Y+bIR8OMaVJSC+R7Sfz1O2v
Hz4rSnrYCn/WJRCT+fznmxzaGs2RRUDinNLnX1Yk+QUPAdIFZ+Sldr6HIrYTP/NK
```

4. Make the desired changes to the endpoint.

   For an unsecured (HTTP) endpoint, you can:

   - Change the endpoint service type between S3 and Swift.

    - Change the endpoint binding mode. For a secured (HTTPS) endpoint, you can:
    - Change the endpoint service type between S3 and Swift.
    - Change the endpoint binding mode.
    - View the security certificate.
    - Upload or generate a new security certificate when the current certificate is expired or about to expire.

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

> ⓘ To change the protocol for an existing endpoint, for example from HTTP to HTTPS, you must create a new endpoint. Follow the instructions for creating load balancer endpoints, and select the desired protocol.

5. Click **Save**.

Related information

Creating load balancer endpoints

Removing load balancer endpoints

If you no longer need a load balancer endpoint, you can remove it.

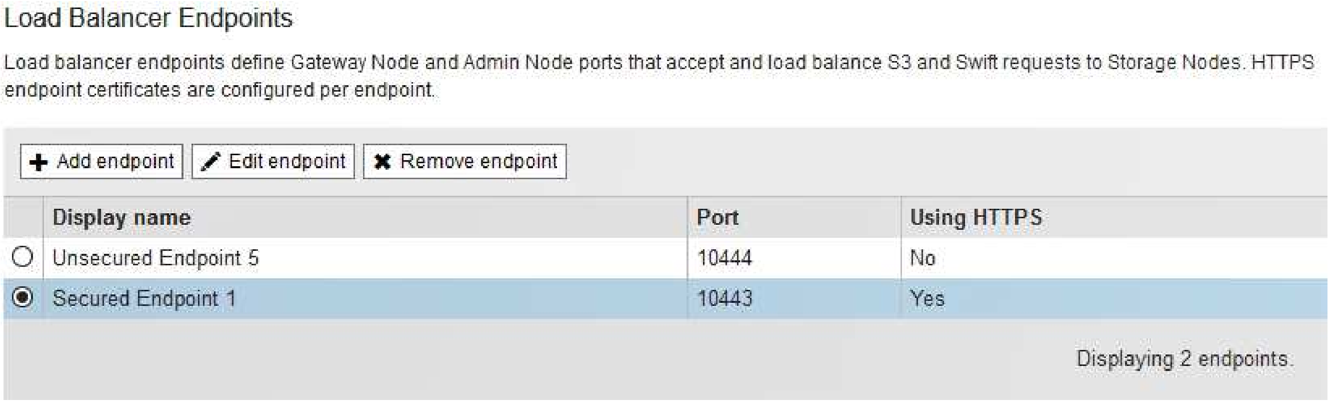
What you'll need

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

Steps

1. Select **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   The Load Balancer Endpoints page appears. The existing endpoints are listed in the table.



Load Balancer Endpoints

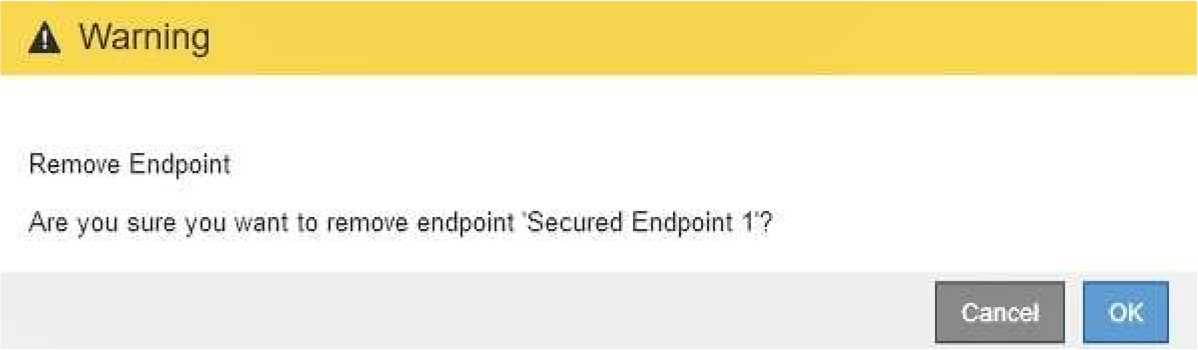
Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

	Display name	Port	Using HTTPS
○	Unsecured Endpoint 5	10444	No
●	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

2. Select the radio button to the left of the endpoint you want to remove.
3. Click **Remove endpoint**.

   A confirmation dialog box appears.



Remove Endpoint

Are you sure you want to remove endpoint 'Secured Endpoint 1'?

4. Click **OK**.

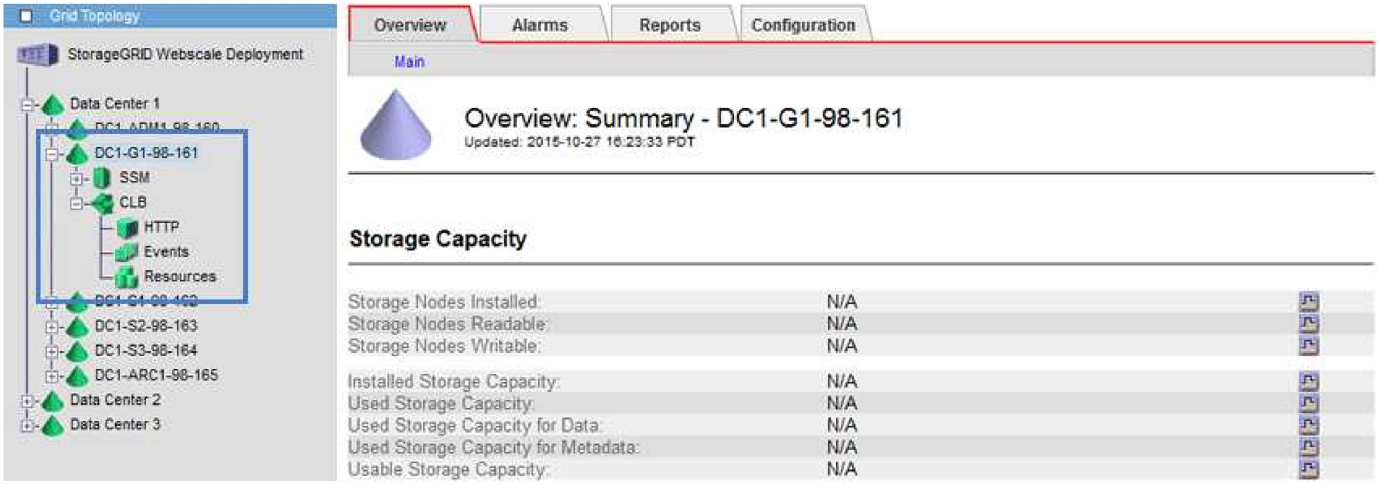
   The endpoint is removed.

How load balancing works - CLB service

The Connection Load Balancer (CLB) service on Gateway Nodes is deprecated. The Load Balancer service is now the recommended load balancing mechanism.

The CLB service uses Layer 4 load balancing to distribute incoming TCP network connections from client applications to the optimal Storage Node based on availability, system load, and the administrator-configured link cost. When the optimal Storage Node is chosen, the CLB service establishes a two-way network connection and forwards the traffic to and from the chosen node. The CLB does not consider the Grid Network configuration when directing incoming network connections.

To view information about the CLB service, select **Support** > **Tools** > **Grid Topology**, and then expand a Gateway Node until you can select **CLB** and the options below it.



Overview: Summary - DC1-G1-98-161

Updated: 2015-10-27 16:23:33 PDT

Storage Capacity

Storage Nodes Installed:	N/A
Storage Nodes Readable:	N/A
Storage Nodes Writable:	N/A
Installed Storage Capacity:	N/A
Used Storage Capacity:	N/A
Used Storage Capacity for Data:	N/A
Used Storage Capacity for Metadata:	N/A
Usable Storage Capacity:	N/A

If you choose to use the CLB service, you should consider configuring link costs for your StorageGRID system.

Related information

What link costs are

Updating link costs

Managing untrusted Client Networks

If you are using a Client Network, you can help secure StorageGRID from hostile attacks by accepting inbound client traffic only on explicitly configured endpoints.

By default, the Client Network on each grid node is *trusted*. That is, by default, StorageGRID trusts inbound connections to each grid node on all available external ports (see the information about external communications in the network guidelines).

You can reduce the threat of hostile attacks on your StorageGRID system by specifying that the Client Network on each node be *untrusted*. If a node's Client Network is untrusted, the node only accepts inbound connections on ports explicitly configured as load balancer endpoints.

Example 1: Gateway Node only accepts HTTPS S3 requests

Suppose you want a Gateway Node to refuse all inbound traffic on the Client Network except for HTTPS S3 requests. You would perform these general steps:

1. From the Load Balancer Endpoints page, configure a load balancer endpoint for S3 over HTTPS on port 443.
2. From the Untrusted Client Networks page, specify that the Client Network on the Gateway Node is untrusted.

After you save your configuration, all inbound traffic on the Gateway Node's Client Network is dropped except for HTTPS S3 requests on port 443 and ICMP echo (ping) requests.

Example 2: Storage Node sends S3 platform services requests

Suppose you want to enable outbound S3 platform service traffic from a Storage Node, but you want to prevent any inbound connections to that Storage Node on the Client Network. You would perform this general step:

- From the Untrusted Client Networks page, indicate that the Client Network on the Storage Node is untrusted.

After you save your configuration, the Storage Node no longer accepts any incoming traffic on the Client Network, but it continues to allow outbound requests to Amazon Web Services.

Related information

Network guidelines

Configuring load balancer endpoints

Specifying a node's Client Network is untrusted

If you are using a Client Network, you can specify whether each node's Client Network is trusted or untrusted. You can also specify the default setting for new nodes added in an expansion.

What you'll need

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

- If you want an Admin Node or Gateway Node to accept inbound traffic only on explicitly configured endpoints, you have defined the load balancer endpoints.

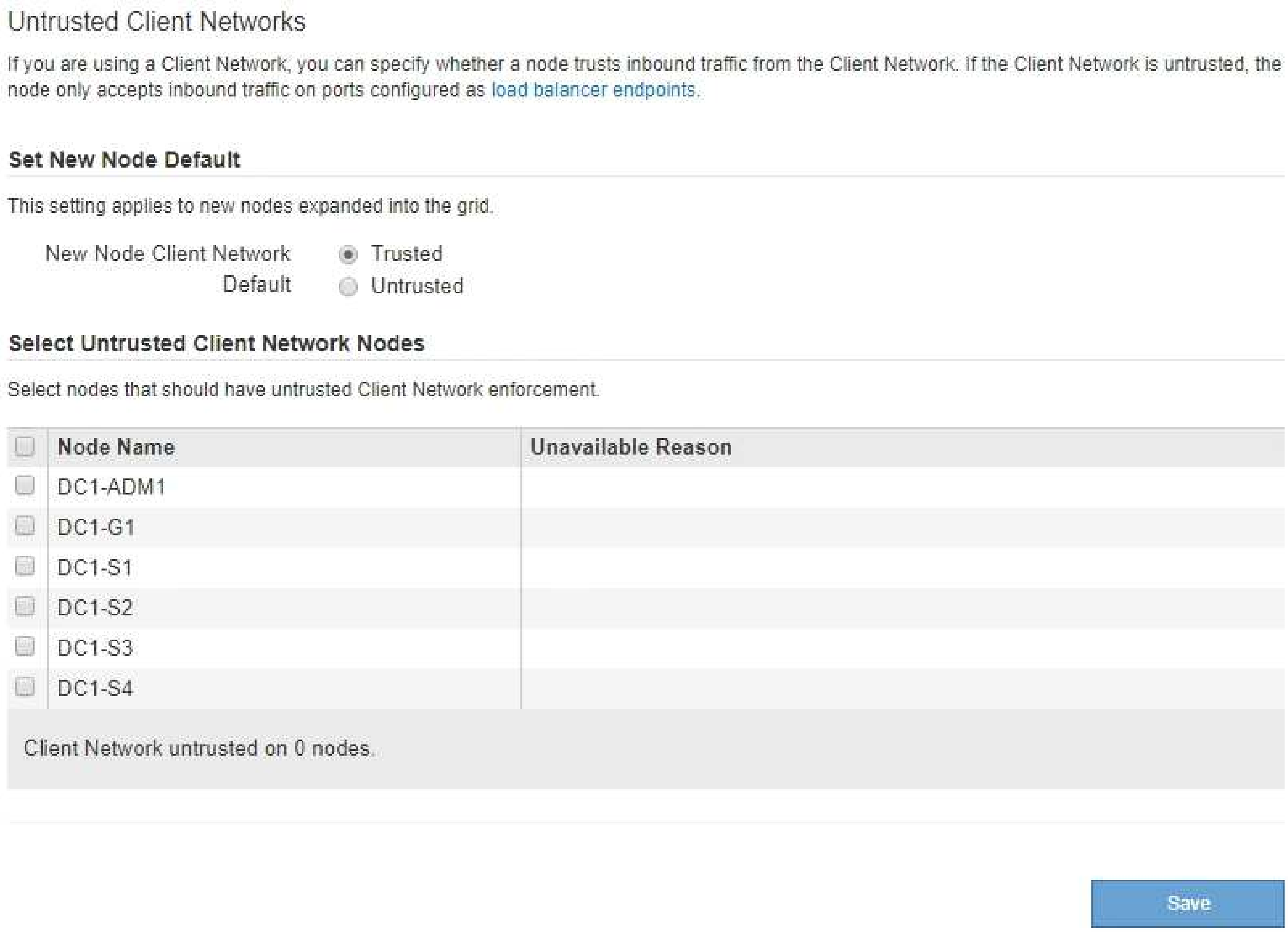
> Existing client connections might fail if load balancer endpoints have not been configured.

Steps

1. Select **Configuration** > **Network Settings** > **Untrusted Client Network**.

   The Untrusted Client Networks page appears.

   This page lists all nodes in your StorageGRID system. The Unavailable Reason column includes an entry if the Client Network on the node must be trusted.



Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as load balancer endpoints.

Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network Default: ● Trusted ○ Untrusted

Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

□	Node Name	Unavailable Reason
□	DC1-ADM1	
□	DC1-G1	
□	DC1-S1	
□	DC1-S2	
□	DC1-S3	
□	DC1-S4	

Client Network untrusted on 0 nodes.

2. In the **Set New Node Default** section, specify what the default setting should be when new nodes are added to the grid in an expansion procedure.

   - **Trusted**: When a node is added in an expansion, its Client Network is trusted.
   - **Untrusted**: When a node is added in an expansion, its Client Network is untrusted. As required, you can return to this page to change the setting for a specific new node.

   > This setting does not affect the existing nodes in your StorageGRID system.

3. In the **Select Untrusted Client Network Nodes** section, select the nodes that should allow client connections only on explicitly configured load balancer endpoints.

You can select or unselect the check box in the title to select or unselect all nodes.

4. Click **Save**.

   The new firewall rules are immediately added and enforced. Existing client connections might fail if load balancer endpoints have not been configured.

Related information

Configuring load balancer endpoints

Managing high availability groups

High availability (HA) groups can be used to provide highly available data connections for S3 and Swift clients. HA groups can also be used to provide highly available connections to the Grid Manager and the Tenant Manager.

- What an HA group is
- How HA groups are used
- Configuration options for HA groups
- Creating a high availability group
- Editing a high availability group
- Removing a high availability group

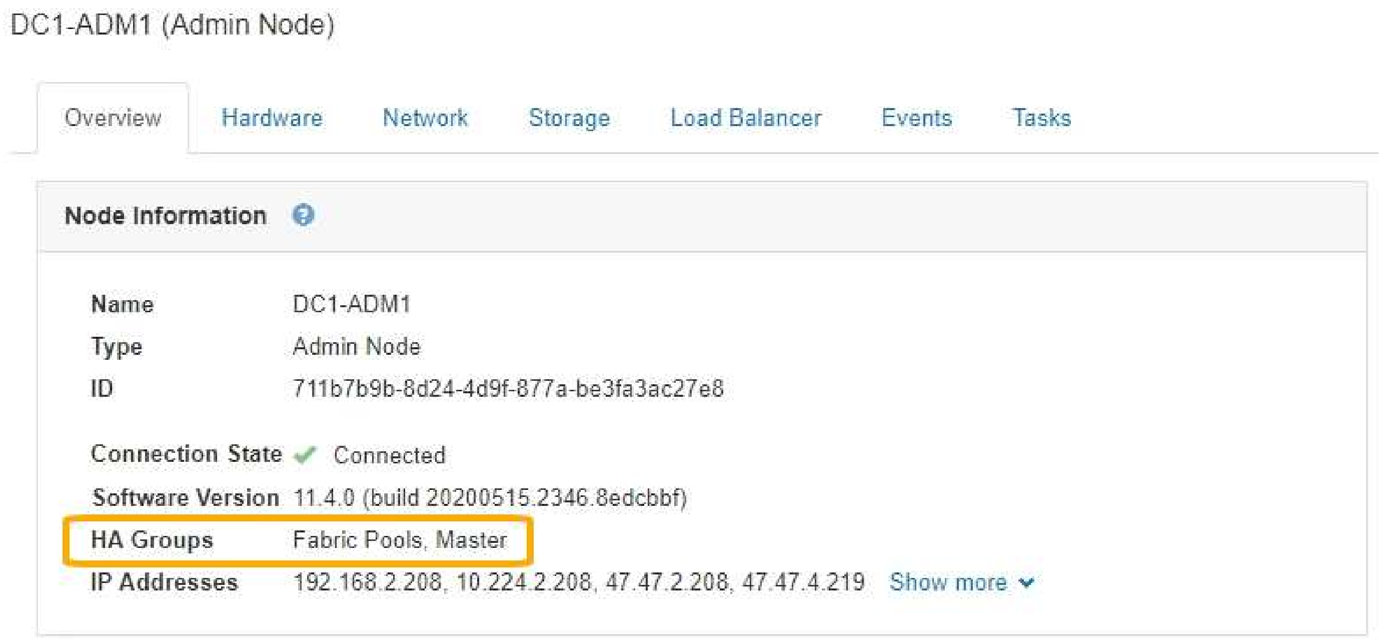
What an HA group is

High availability groups use virtual IP addresses (VIPs) to provide active-backup access to Gateway Node or Admin Node services.

An HA group consists of one or more network interfaces on Admin Nodes and Gateway Nodes. When creating an HA group, you select network interfaces belonging to the Grid Network (eth0) or the Client Network (eth2). All interfaces in an HA group must be within the same network subnet.

An HA group maintains one or more virtual IP addresses that are added to the active interface in the group. If the active interface becomes unavailable, the virtual IP addresses are moved to another interface. This failover process generally takes only a few seconds and is fast enough that client applications should experience little impact and can rely on normal retry behaviors to continue operation.

The active interface in an HA group is designated as the Master. All other interfaces are designated as Backup. To view these designations, select **Nodes** > ***node*** > **Overview**.



DC1-ADM1 (Admin Node)

Node Information

Name DC1-ADM1
Type Admin Node
ID 711b7b9b-8d24-4d9f-877a-be3fa3ac27e8

Connection State ✓ Connected
Software Version 11.4.0 (build 20200515.2346.8edcbbf)
HA Groups Fabric Pools, Master
IP Addresses 192.168.2.208, 10.224.2.208, 47.47.2.208, 47.47.4.219

When creating an HA group, you specify one interface to be the preferred Master. The preferred Master is the active interface unless a failure occurs that causes the VIP addresses to be reassigned to a Backup interface. When the failure is resolved, the VIP addresses are automatically moved back to the preferred Master.

Failover can be triggered for any of these reasons:

- The node on which the interface is configured goes down.
- The node on which the interface is configured loses connectivity to all other nodes for at least 2 minutes
- The active interface goes down.
- The Load Balancer service stops.
- The High Availability service stops.

Failover might not be triggered by network failures external to the node that hosts the active interface. Similarly, failover is not triggered by the failure of the CLB service (deprecated) or services for the Grid Manager or the Tenant Manager.

If the HA group includes interfaces from more than two nodes, the active interface might move to any other node's interface during failover.

How HA groups are used

You might want to use high availability (HA) groups for several reasons.

- An HA group can provide highly available administrative connections to the Grid Manager or the Tenant Manager.
- An HA group can provide highly available data connections for S3 and Swift clients.
- An HA group that contains only one interface allows you to provide many VIP addresses and to explicitly set IPv6 addresses.

An HA group can provide high availability only if all nodes included in the group provide the same services. When you create an HA group, add interfaces from the types of nodes that provide the services you require.

- **Admin Nodes**: Include the Load Balancer service and enable access to the Grid Manager or the Tenant Manager.
- **Gateway Nodes**: Include the Load Balancer service and the CLB service (deprecated).

Purpose of HA group	Add nodes of this type to the HA group
Access to Grid Manager	• Primary Admin Node (**preferred Master**) • Non-primary Admin Nodes **Note:** The primary Admin Node must be the preferred Master. Some maintenance procedures can only be performed from the primary Admin Node.
Access to Tenant Manager only	• Primary or non-primary Admin Nodes
S3 or Swift client access — Load Balancer service	• Admin Nodes • Gateway Nodes
S3 or Swift client access — CLB service **Note:** The CLB service is deprecated.	• Gateway Nodes

Limitations of using HA groups with Grid Manager or Tenant Manager

The failure of services for the Grid Manager or the Tenant Manager does not trigger failover within the HA group.

If you are signed in to the Grid Manager or the Tenant Manager when failover occurs, you are signed out and must sign in again to resume your task.

Some maintenance procedures cannot be performed when the primary Admin Node is unavailable. During failover, you can use the Grid Manager to monitor your StorageGRID system.

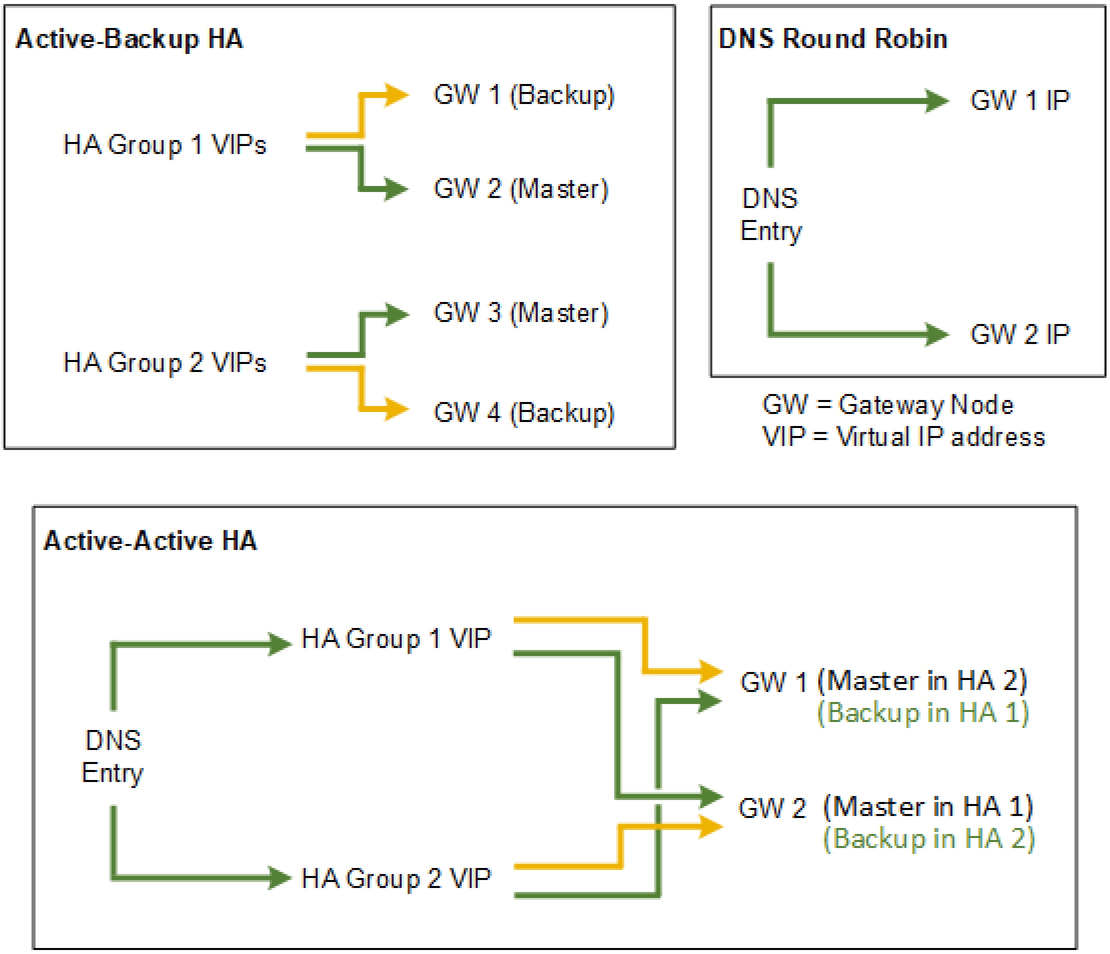
Limitations of using HA groups with the CLB service

The failure of the CLB service does not trigger failover within the HA group.

ⓘ The CLB service is deprecated.

Configuration options for HA groups

The following diagrams provide examples of different ways you can configure HA groups. Each option has advantages and disadvantages.



When creating multiple overlapping HA groups as shown in the Active-Active HA example, the total throughput scales with the number of nodes and HA groups. With three or more nodes and three or more HA groups, you also gain the ability to continue operations using any of the VIPs even during maintenance procedures that require you to take a node offline.

The table summarizes the benefits of each HA configuration shown in the diagram.

Configuration	Advantages	Disadvantages
Active-Backup HA	• Managed by StorageGRID with no external dependencies. • Fast failover.	• Only one node in an HA group is active. At least one node per HA group will be idle.
DNS Round Robin	• Increased aggregate throughput. • No idle hosts.	• Slow failover, which could depend on client behavior. • Requires configuration of hardware outside of StorageGRID. • Needs a customer-implemented health check.

Configuration	Advantages	Disadvantages
Active-Active	• Traffic is distributed across multiple HA groups. • High aggregate throughput that scales with the number of HA groups. • Fast failover.	• More complex to configure. • Requires configuration of hardware outside of StorageGRID. • Needs a customer-implemented health check.

Creating a high availability group

You can create one or more high availability (HA) groups to provide highly available access to the services on Admin Nodes or Gateway Nodes.

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

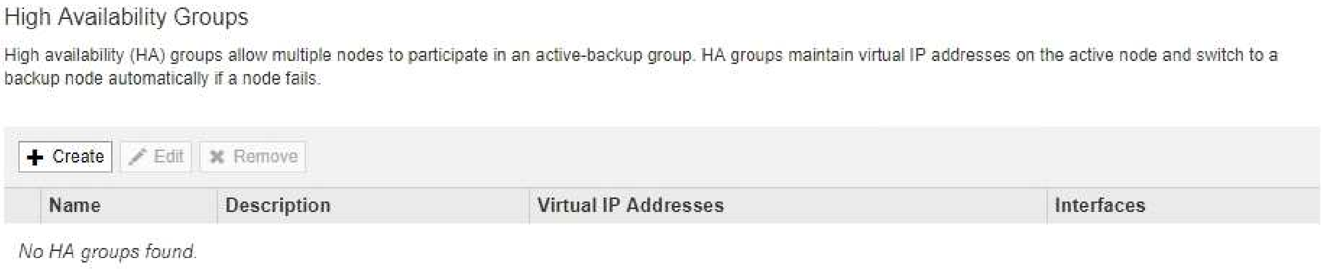
An interface must meet the following conditions to be included in an HA group:

- The interface must be for a Gateway Node or an Admin Node.
- The interface must belong to the Grid Network (eth0) or the Client Network (eth2).
- The interface must be configured with fixed or static IP addressing, not with DHCP.

Steps

1. Select **Configuration** > **Network Settings** > **High Availability Groups**.

   The High Availability Groups page appears.



High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

Name	Description	Virtual IP Addresses	Interfaces

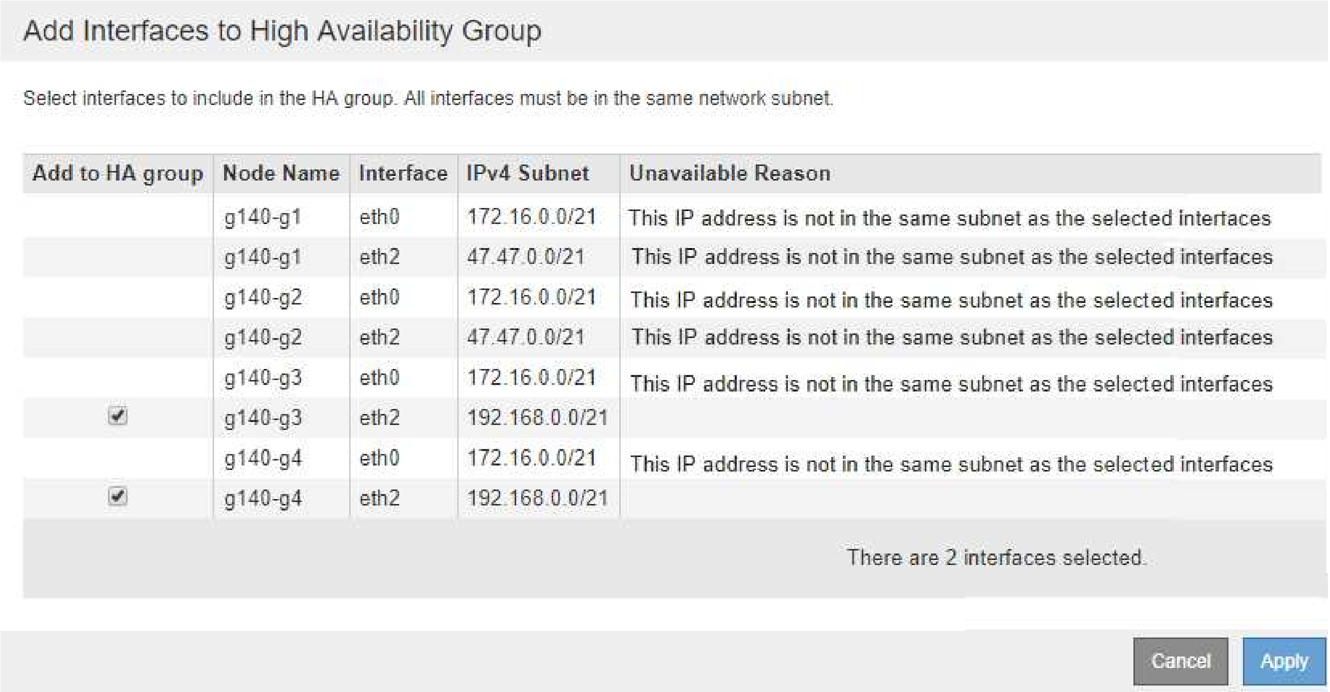
No HA groups found.

2. Click **Create**.

   The Create High Availability Group dialog box appears.

3. Type a name and, if desired, a description for the HA group.
4. Click **Select Interfaces**.

   The Add Interfaces to High Availability Group dialog box appears. The table lists eligible nodes, interfaces, and IPv4 subnets.



Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
☑	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
☑	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

An interface does not appear in the list if its IP address is assigned by DHCP.

5. In the **Add to HA group** column, select the check box for the interface you want to add to the HA group.

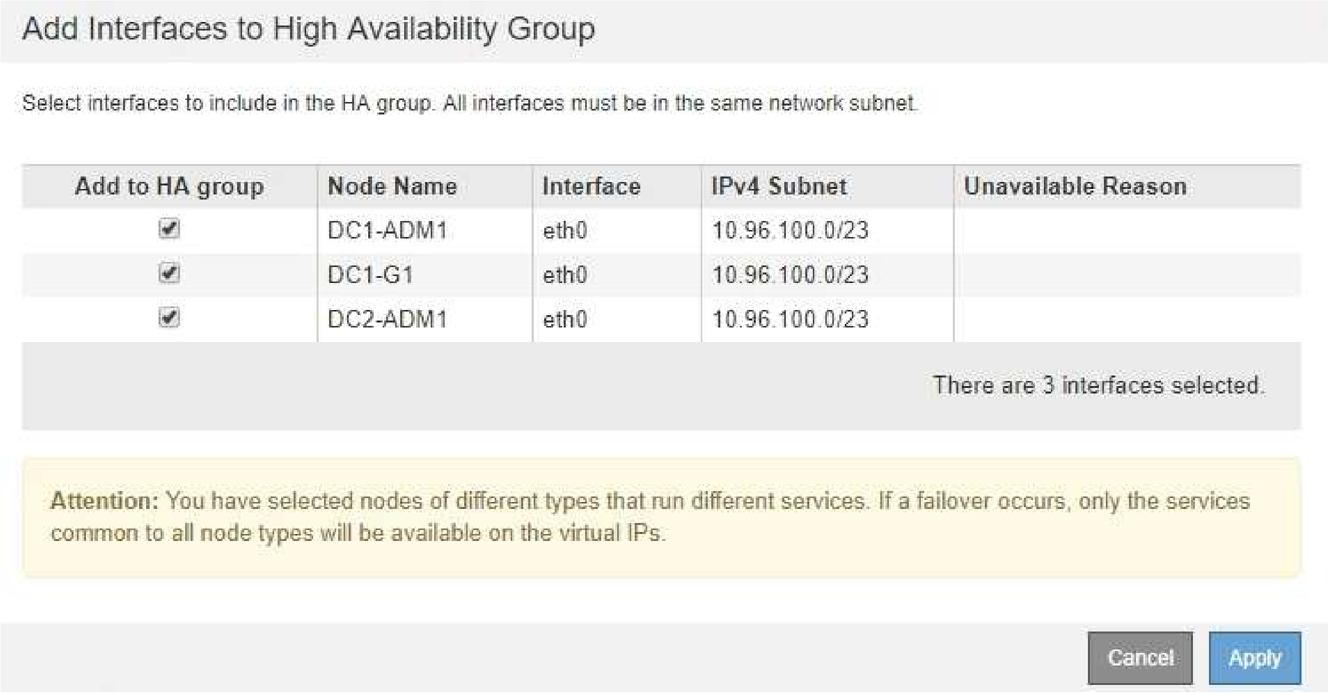
   Note the following guidelines for selecting interfaces:

   - You must select at least one interface.
   - If you select more than one interface, all of the interfaces must be on either the Grid Network (eth0) or on the Client Network (eth2).
   - All interfaces must be in the same subnet or in subnets with a common prefix.

     IP addresses will be restricted to the smallest subnet (the one with the largest prefix).

   - If you select interfaces on different types of nodes, and a failover occurs, only the services common to the selected nodes will be available on the virtual IPs.
     - Select two or more Admin Nodes for HA protection of the Grid Manager or the Tenant Manager.
     - Select two or more Admin Nodes, Gateway Nodes, or both for HA protection of the Load Balancer service.
     - Select two or more Gateway Nodes for HA protection of the CLB service.

       The CLB service is deprecated.



Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

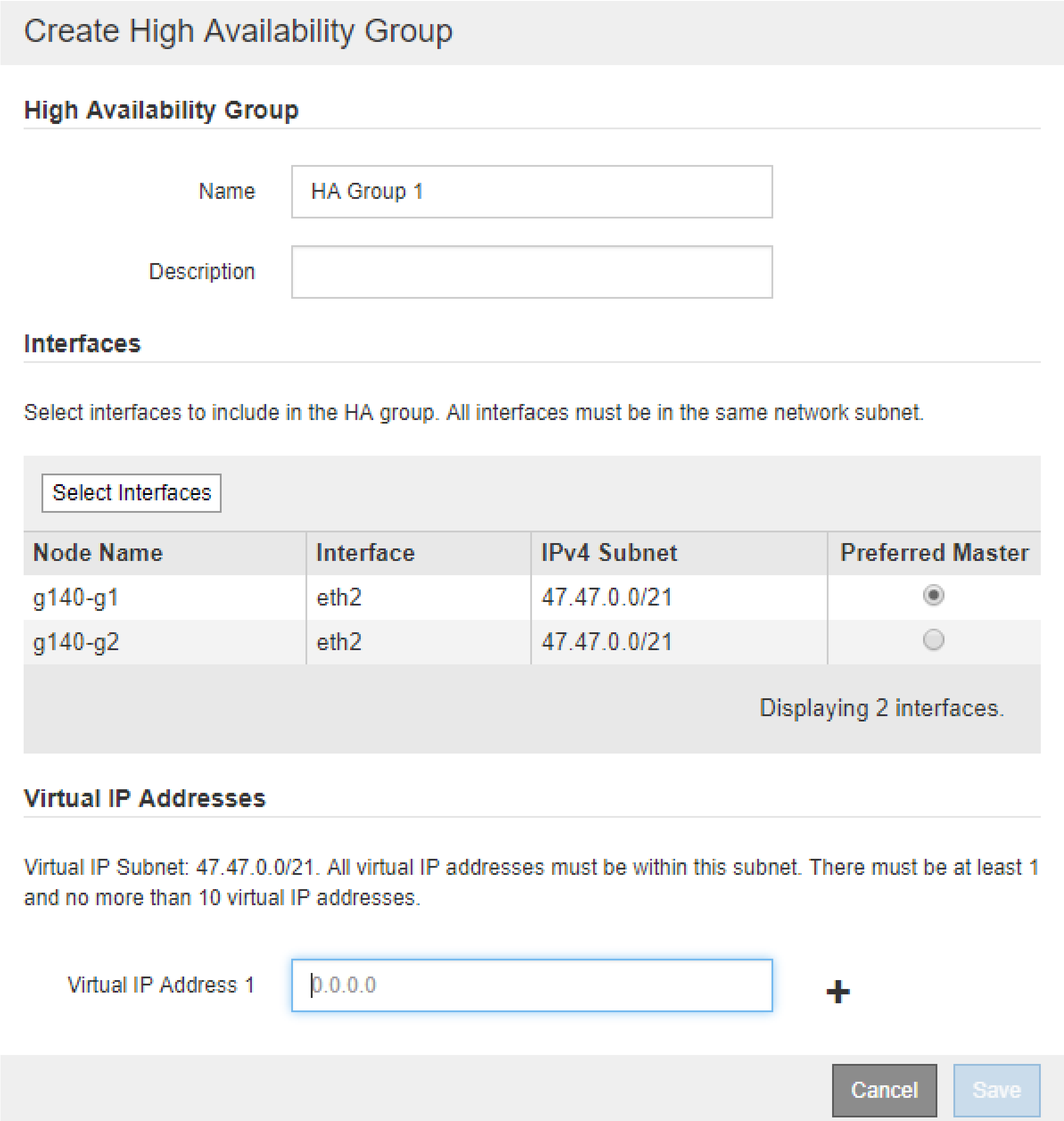
Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
☑	DC1-ADM1	eth0	10.96.100.0/23	
☑	DC1-G1	eth0	10.96.100.0/23	
☑	DC2-ADM1	eth0	10.96.100.0/23	

There are 3 interfaces selected.

Attention: You have selected nodes of different types that run different services. If a failover occurs, only the services common to all node types will be available on the virtual IPs.

6. Click **Apply**.

   The interfaces you selected are listed in the Interfaces section of the Create High Availability Group page. By default, the first interface in the list is selected as the Preferred Master.



Create High Availability Group

High Availability Group

Name	HA Group 1
Description	

Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Node Name	Interface	IPv4 Subnet	Preferred Master
g140-g1	eth2	47.47.0.0/21	●
g140-g2	eth2	47.47.0.0/21	○

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 47.47.0.0/21. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1	0.0.0.0

7. If you want a different interface to be the preferred Master, select that interface in the **Preferred Master** column.

   The preferred Master is the active interface unless a failure occurs that causes the VIP addresses to be reassigned to a Backup interface.

   > If the HA group provides access to the Grid Manager, you must select an interface on the primary Admin Node to be the preferred Master. Some maintenance procedures can only be performed from the primary Admin Node.

8. In the Virtual IP Addresses section of the page, enter one to 10 virtual IP addresses for the HA group. Click the plus sign (+) to add multiple IP addresses.

   You must provide at least one IPv4 address. Optionally, you can specify additional IPv4 and IPv6 addresses.

   IPv4 addresses must be within the IPv4 subnet shared by all of the member interfaces.

9. Click **Save**.

   The HA Group is created, and you can now use the configured virtual IP addresses.

Related information

Install Red Hat Enterprise Linux or CentOS

Install VMware

Install Ubuntu or Debian

Managing load balancing

Editing a high availability group

You can edit a high availability (HA) group to change its name and description, add or remove interfaces, or add or update a virtual IP address.

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

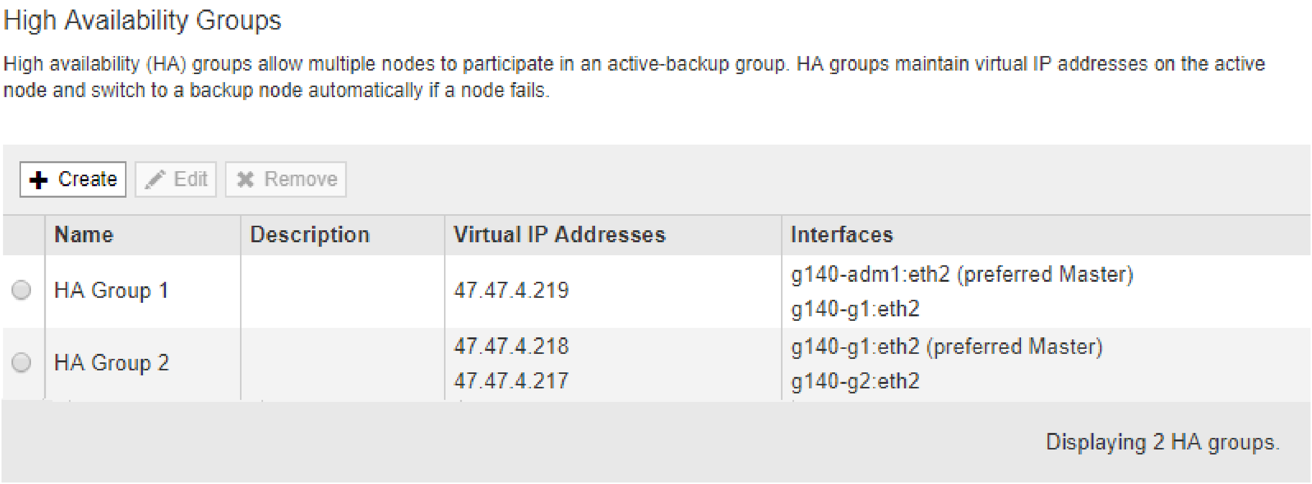
Some of the reasons for editing an HA group include the following:

- Adding an interface to an existing group. The interface IP address must be within the same subnet as other interfaces already assigned to the group.
- Removing an interface from an HA group. For example, you cannot start a site or node decommission procedure if a node's interface for the Grid Network or the Client Network is used in an HA group.

Steps

1. Select **Configuration** > **Network Settings** > **High Availability Groups**.

   The High Availability Groups page appears.



High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

	Name	Description	Virtual IP Addresses	Interfaces
○	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
○	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

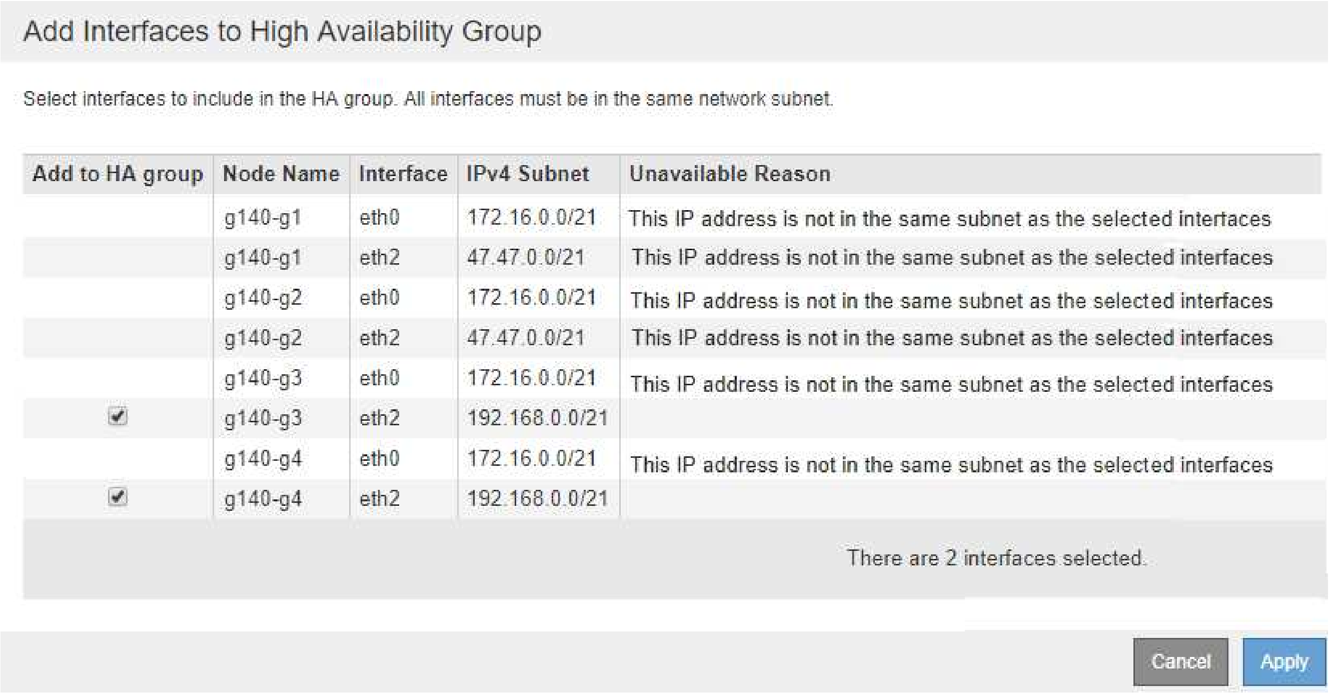
Displaying 2 HA groups.

2. Select the HA group you want to edit, and click **Edit**.

The Edit High Availability Group dialog box appears.

3. Optionally, update the group’s name or description.
4. Optionally, click **Select Interfaces** to change the interfaces for the HA Group.

   The Add Interfaces to High Availability Group dialog box appears.



Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
☑	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
☑	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

   An interface does not appear in the list if its IP address is assigned by DHCP.

5. Select or unselect the check boxes to add or remove interfaces.

   Note the following guidelines for selecting interfaces:

   - You must select at least one interface.
   - If you select more than one interface, all of the interfaces must be on either the Grid Network (eth0) or on the Client Network (eth2).
   - All interfaces must be in the same subnet or in subnets with a common prefix.

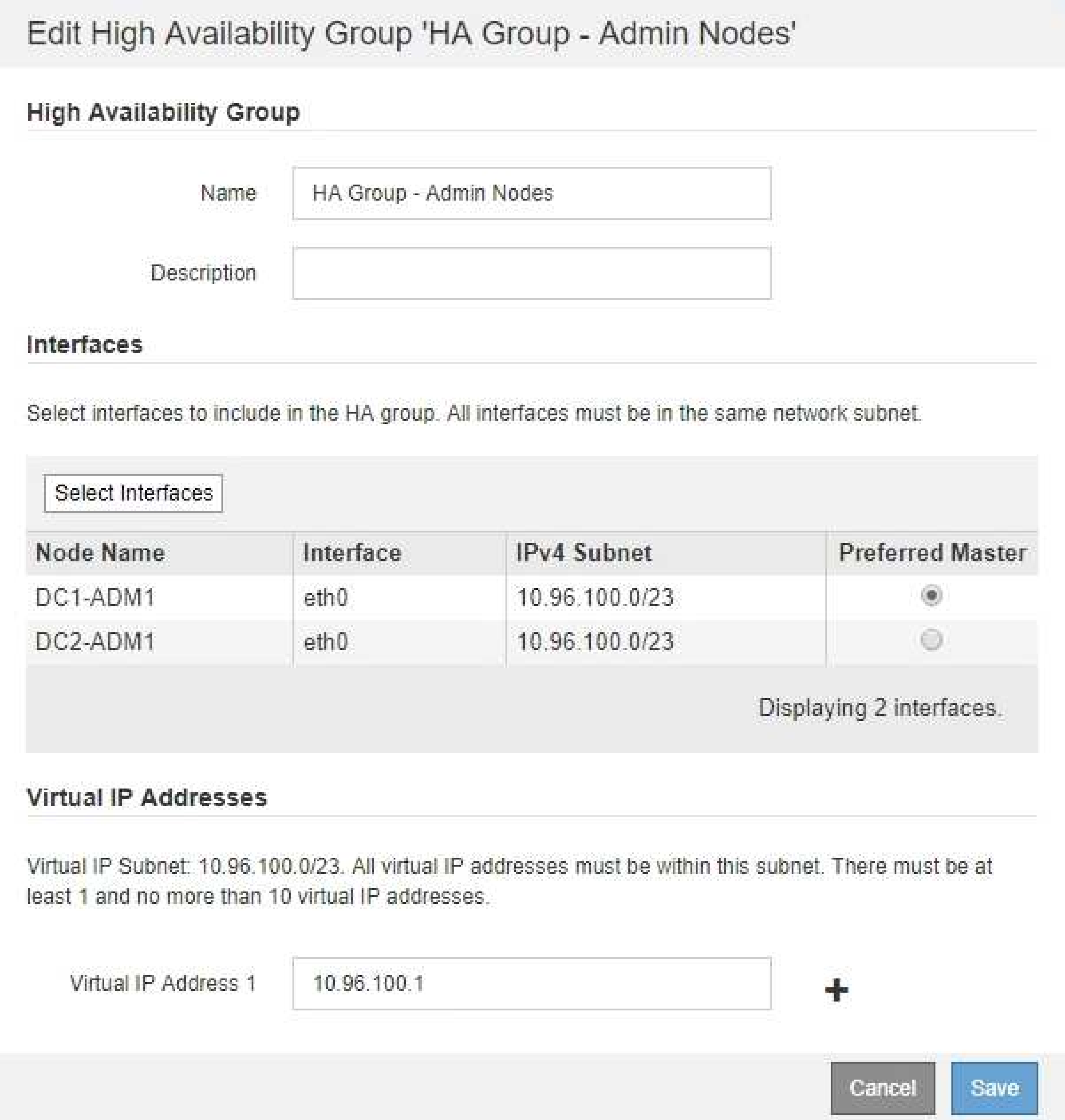
     IP addresses will be restricted to the smallest subnet (the one with the largest prefix).

   - If you select interfaces on different types of nodes, and a failover occurs, only the services common to the selected nodes will be available on the virtual IPs.
     - Select two or more Admin Nodes for HA protection of the Grid Manager or the Tenant Manager.
     - Select two or more Admin Nodes, Gateway Nodes, or both for HA protection of the Load Balancer service.
     - Select two or more Gateway Nodes for HA protection of the CLB service.

       ⓘ The CLB service is deprecated.

6. Click **Apply**.

The interfaces you selected are listed in the Interfaces section of the page. By default, the first interface in the list is selected as the Preferred Master.



Edit High Availability Group 'HA Group - Admin Nodes'

High Availability Group

Name	HA Group - Admin Nodes
Description	

Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Node Name	Interface	IPv4 Subnet	Preferred Master
DC1-ADM1	eth0	10.96.100.0/23	●
DC2-ADM1	eth0	10.96.100.0/23	○

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 10.96.100.0/23. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1	10.96.100.1

7. If you want a different interface to be the preferred Master, select that interface in the **Preferred Master** column.

   The preferred Master is the active interface unless a failure occurs that causes the VIP addresses to be reassigned to a Backup interface.

   > If the HA group provides access to the Grid Manager, you must select an interface on the primary Admin Node to be the preferred Master. Some maintenance procedures can only be performed from the primary Admin Node.

8. Optionally, update the virtual IP addresses for the HA group.

   You must provide at least one IPv4 address. Optionally, you can specify additional IPv4 and IPv6 addresses.

IPv4 addresses must be within the IPv4 subnet shared by all of the member interfaces.

9. Click **Save**.

   The HA Group is updated.

Removing a high availability group

You can remove a high availability (HA) group that you are no longer using.

What you’ll need

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

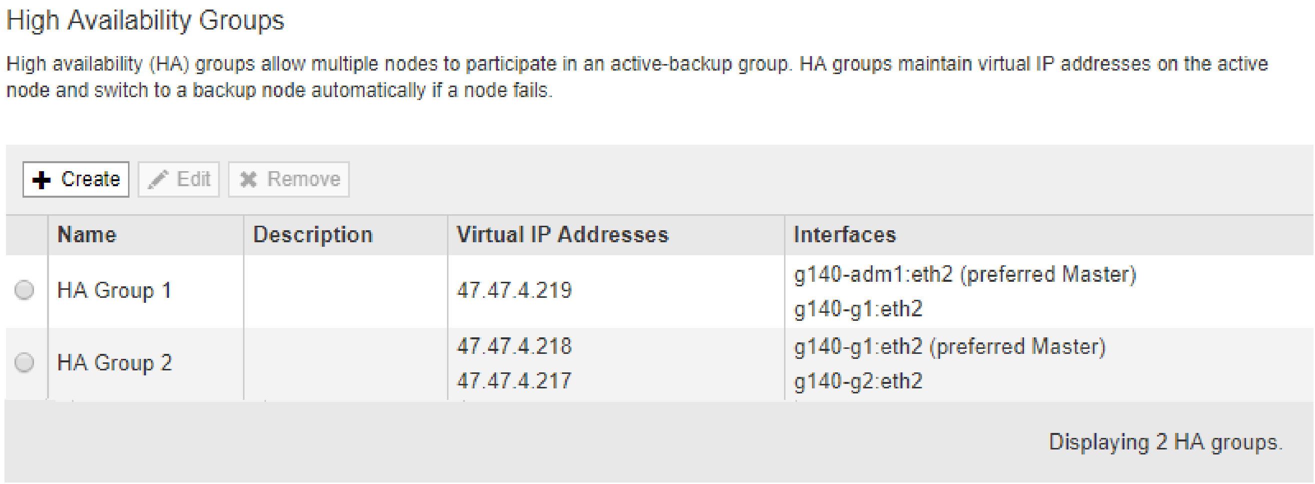
Aboout this task

If you remove an HA group, any S3 or Swift clients that are configured to use one of the group’s virtual IP addresses will no longer be able to connect to StorageGRID. To prevent client disruptions, you should update all affected S3 or Swift client applications before you remove an HA group. Update each client to connect using another IP address, for example, the virtual IP address of a different HA group or the IP address that was configured for an interface during installation or using DHCP.

Steps

1. Select **Configuration** > **Network Settings** > **High Availability Groups**.

   The High Availability Groups page appears.



High Availability Groups

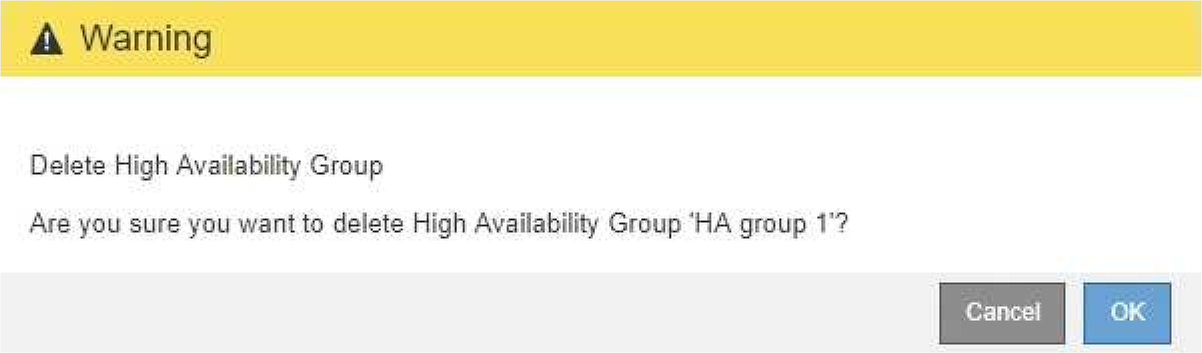
High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

	Name	Description	Virtual IP Addresses	Interfaces
○	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
○	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. Select the HA group you want to remove, and click **Remove**.

   The Delete High Availability Group warning appears.



Delete High Availability Group

Are you sure you want to delete High Availability Group 'HA group 1'?

3. Click **OK**.

   The HA group is removed.

Configuring S3 API endpoint domain names

To support S3 virtual hosted-style requests, you must use the Grid Manager to configure the list of endpoint domain names that S3 clients connect to.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have specific access permissions.
- You must have confirmed that a grid upgrade is not in progress.

> ! Do not make any changes to the domain name configuration when a grid upgrade is in progress.

About this task

To enable clients to use S3 endpoint domain names, you must do all of the following tasks:

- Use the Grid Manager to add the S3 endpoint domain names to the StorageGRID system.
- Ensure that the certificate the client uses for HTTPS connections to StorageGRID is signed for all domain names that the client requires.

  For example, if the endpoint is `s3.company.com`, you must ensure that the certificate used for HTTPS connections includes the `s3.company.com` endpoint and the endpoint's wildcard Subject Alternative Name (SAN): `*.s3.company.com`.

- Configure the DNS server used by the client. Include DNS records for the IP addresses that clients use to make connections, and ensure that the records reference all required endpoint domain names, including any wildcard names.

> i Clients can connect to StorageGRID using the IP address of a Gateway Node, an Admin Node, or a Storage Node, or by connecting to the virtual IP address of a high availability group. You should understand how client applications connect to the grid so you include the correct IP addresses in the DNS records.

The certificate a client uses for HTTPS connections depends on how the client connects to the grid:

- If a client connects using the Load Balancer service, it uses the certificate for a specific load balancer endpoint.

  > Each load balancer endpoint has its own certificate, and each endpoint can be configured to recognize different endpoint domain names.

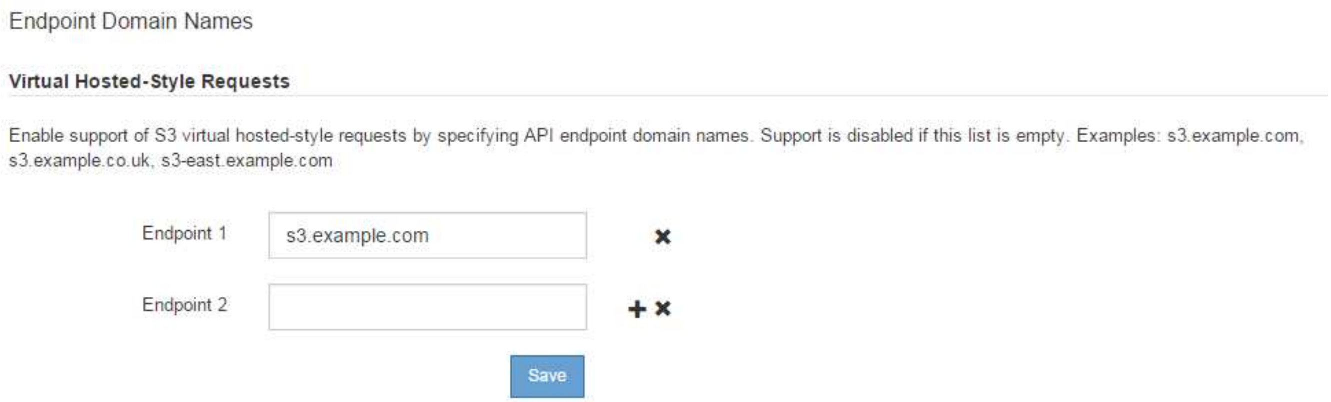
- If the client connects to a Storage Node or to the CLB service on a Gateway Node, the client uses a grid custom server certificate that has been updated to include all required endpoint domain names.

  > The CLB service is deprecated.

Steps

1. Select **Configuration** > **Network Settings** > **Domain Names**.

   The Endpoint Domain Names page appears.

   Endpoint Domain Names

   Virtual Hosted-Style Requests

   Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: s3.example.com, s3.example.co.uk, s3-east.example.com

   Endpoint 1: s3.example.com

   Endpoint 2:

2. Using the (+) icon to add additional fields, enter the list of S3 API endpoint domain names in the **Endpoint** fields.

   If this list is empty, support for S3 virtual hosted-style requests is disabled.

3. Click **Save**.
4. Ensure that the server certificates that clients use match the required endpoint domain names.
   - For clients that use the Load Balancer service, update the certificate associated with the load balancer endpoint that the client connects to.
   - For clients that connect directly to Storage Nodes or that use the CLB service on Gateway Nodes, update the custom server certificate for the grid.
5. Add the DNS records required to ensure that endpoint domain name requests can be resolved.

Result

Now, when clients use the endpoint `bucket.s3.company.com`, the DNS server resolves to the correct endpoint and the certificate authenticates the endpoint as expected.

Related information

Use S3

Viewing IP addresses

Creating a high availability group

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

Configuring load balancer endpoints

Enabling HTTP for client communications

By default, client applications use the HTTPS network protocol for all connections to Storage Nodes or to the deprecated CLB service on Gateway Nodes. You can optionally enable HTTP for these connections, for example, when testing a non-production grid.

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

Complete this task only if S3 and Swift clients need to make HTTP connections directly to Storage Nodes or to the deprecated CLB service on Gateway Nodes.

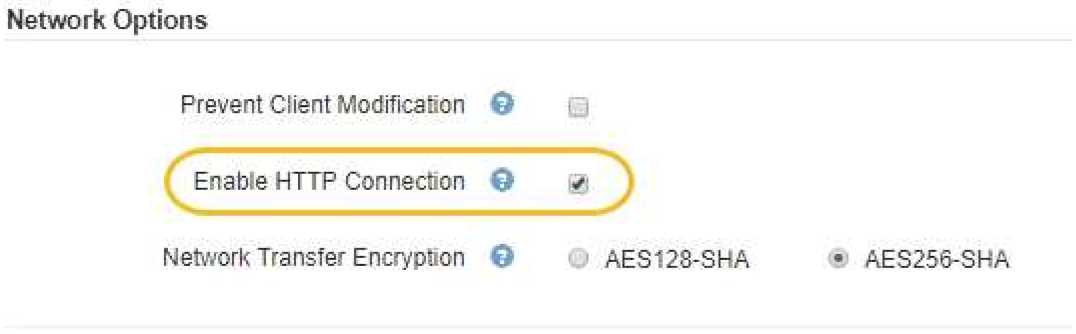
You do not need to complete this task for clients that only use HTTPS connections or for clients that connect to the Load Balancer service (because you can configure each Load Balancer endpoint to use either HTTP or HTTPS). See the information on configuring load balancer endpoints for more information.

See Summary: IP addresses and ports for client connections to learn which ports S3 and Swift clients use when connecting to Storage Nodes or to the deprecated CLB service using HTTP or HTTPS

> Be careful when enabling HTTP for a production grid because requests will be sent unencrypted.

Steps

1. Select **Configuration** > **System Settings** > **Grid Options**.
2. In the Network Options section, select the **Enable HTTP Connection** check box.



Network Options

Prevent Client Modification □

Enable HTTP Connection ☑

Network Transfer Encryption ○ AES128-SHA ● AES256-SHA

3. Click **Save**.

Related information

Configuring load balancer endpoints

Use S3

Controlling which client operations are permitted

You can select the Prevent Client Modification grid option to deny specific HTTP client operations.

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

Prevent Client Modification is a system wide setting. When the Prevent Client Modification option is selected, the following requests are denied:

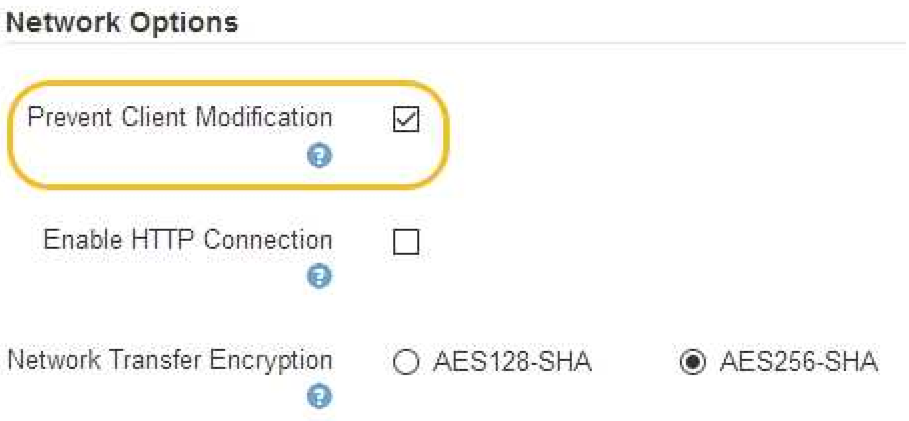
- **S3 REST API**
  - Delete Bucket requests
  - Any requests to modify an existing object's data, user-defined metadata, or S3 object tagging

    > ⓘ This setting does not apply to buckets with versioning enabled. Versioning already prevents modifications to object data, user-defined metadata, and object tagging.

- **Swift REST API**
  - Delete Container requests
  - Requests to modify any existing object. For example, the following operations are denied: Put Overwrite, Delete, Metadata Update, and so on.

Steps

1. Select **Configuration** > **System Settings** > **Grid Options**.
2. In the Network Options section, select the **Prevent Client Modification** check box.



Network Options

Prevent Client Modification ☑

Enable HTTP Connection □

Network Transfer Encryption ○ AES128-SHA ● AES256-SHA

3. Click **Save**.

Copyright information

Trademark information