Managing load balancing

StorageGRID 11.5

NetApp
January 04, 2024

Table of Contents

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.

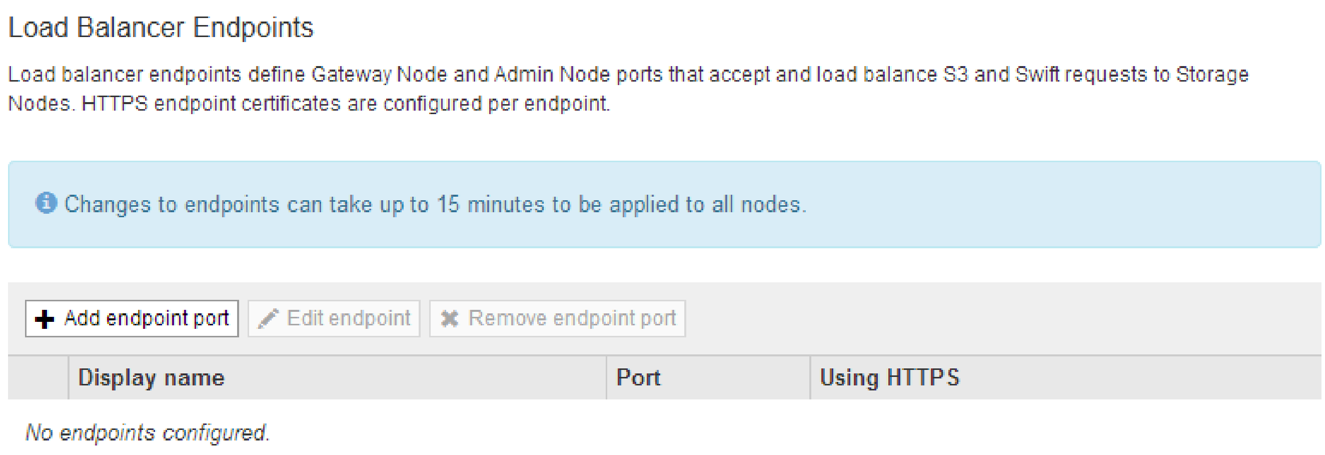
  > ⓘ If you have remapped any ports, you cannot use the same ports to configure load balancer endpoints. You can create endpoints using remapped ports, but those endpoints will be remapped to the original CLB ports and service, not the Load Balancer service. Follow the steps in the recovery and maintenance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

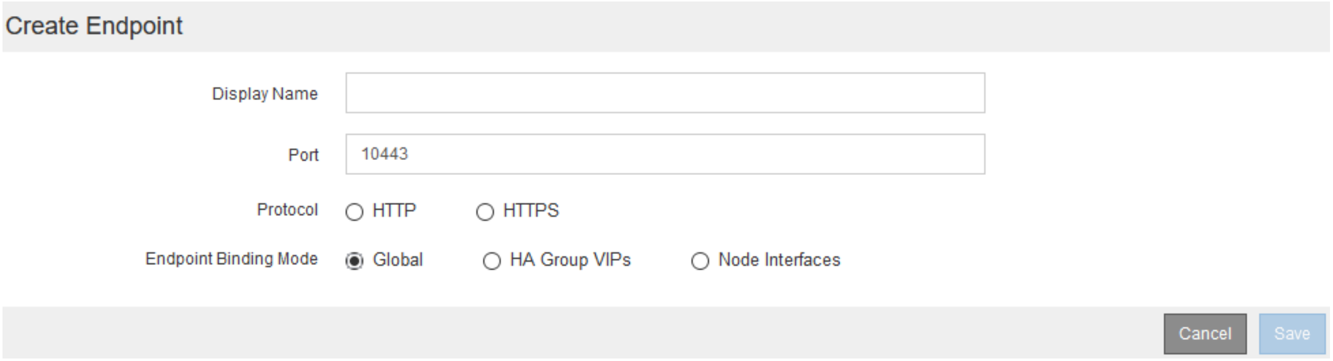
Changes to endpoints can take up to 15 minutes to be applied to all nodes.

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

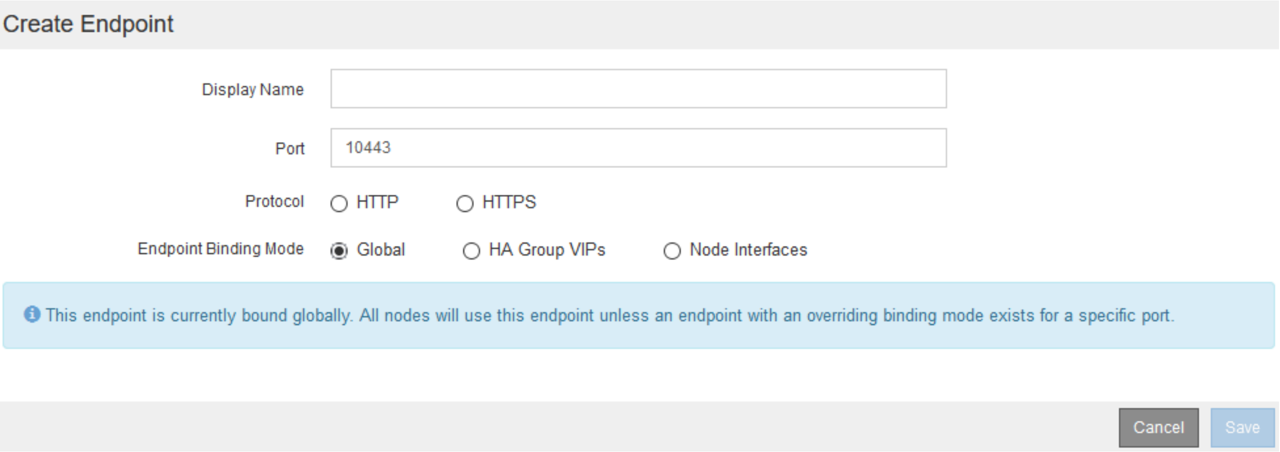
Endpoint Binding Mode: ● Global ○ HA Group VIPs ○ Node Interfaces

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.



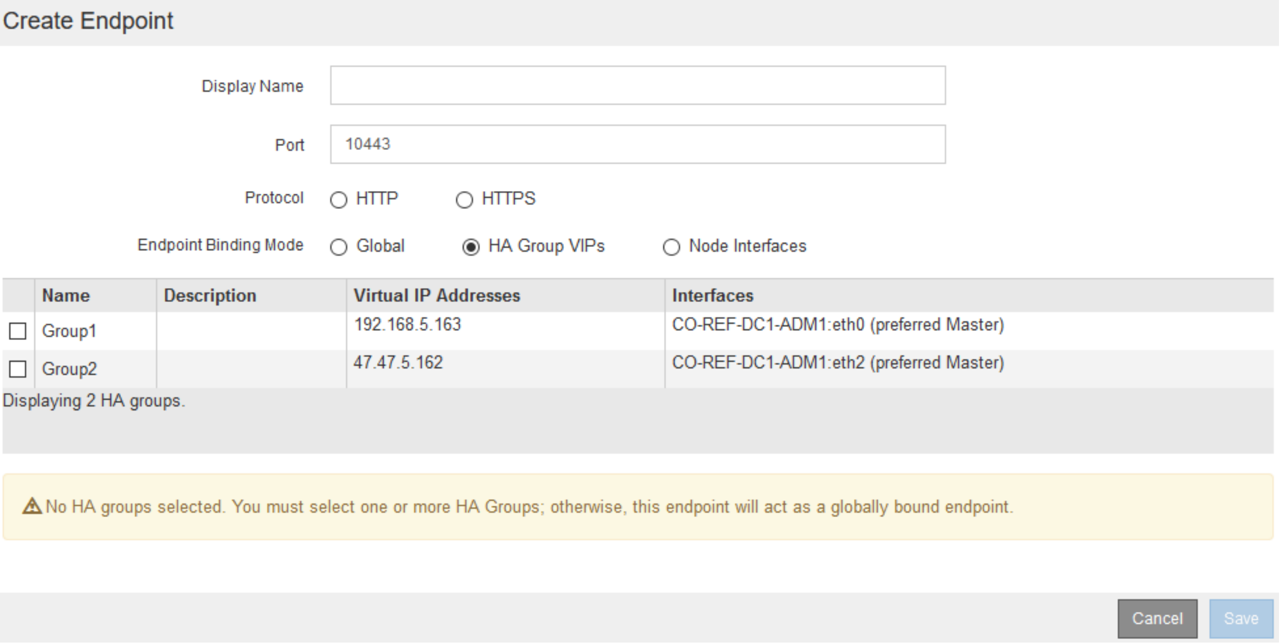
Create Endpoint

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

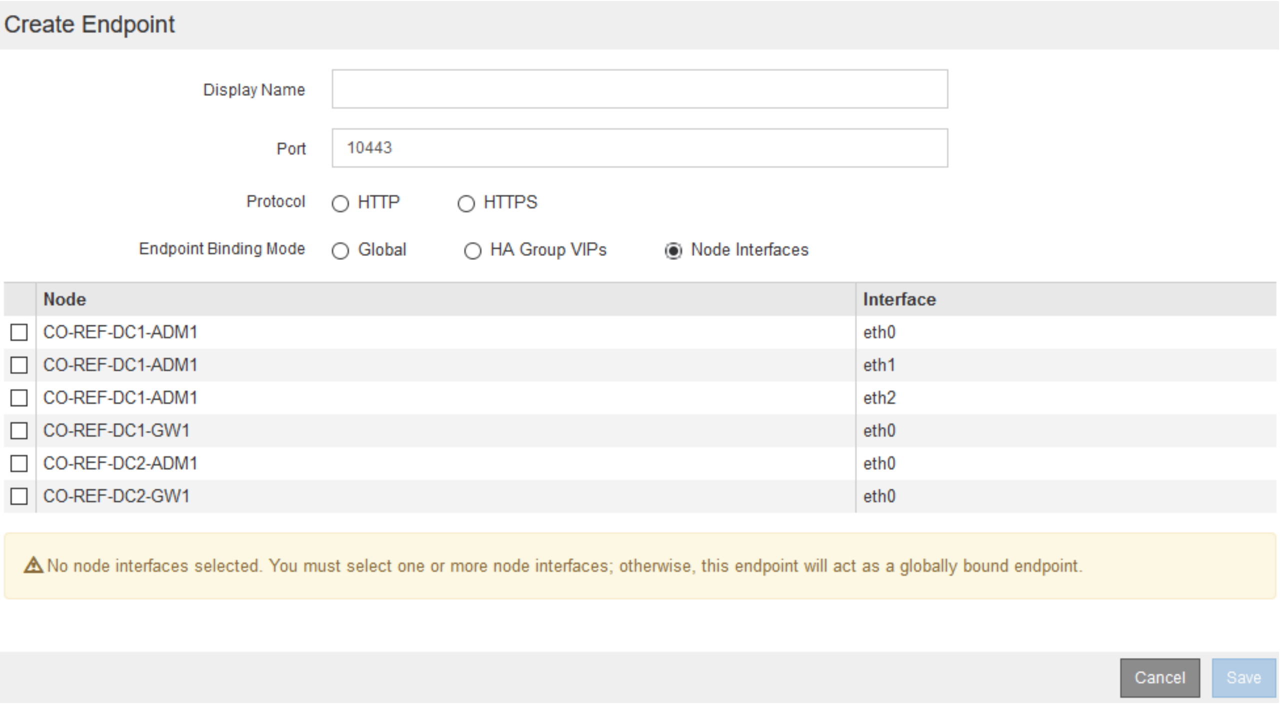
	Name	Description	Virtual IP Addresses	Interfaces
□	Group1		192.168.5.163	CO-REF-DC1-ADM1:eth0 (preferred Master)
□	Group2		47.47.5.162	CO-REF-DC1-ADM1:eth2 (preferred Master)

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

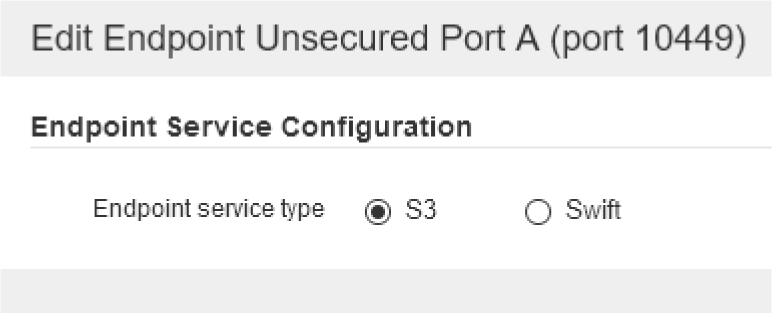
	Node	Interface
□	CO-REF-DC1-ADM1	eth0
□	CO-REF-DC1-ADM1	eth1
□	CO-REF-DC1-ADM1	eth2
□	CO-REF-DC1-GW1	eth0
□	CO-REF-DC2-ADM1	eth0
□	CO-REF-DC2-GW1	eth0

⚠ 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)

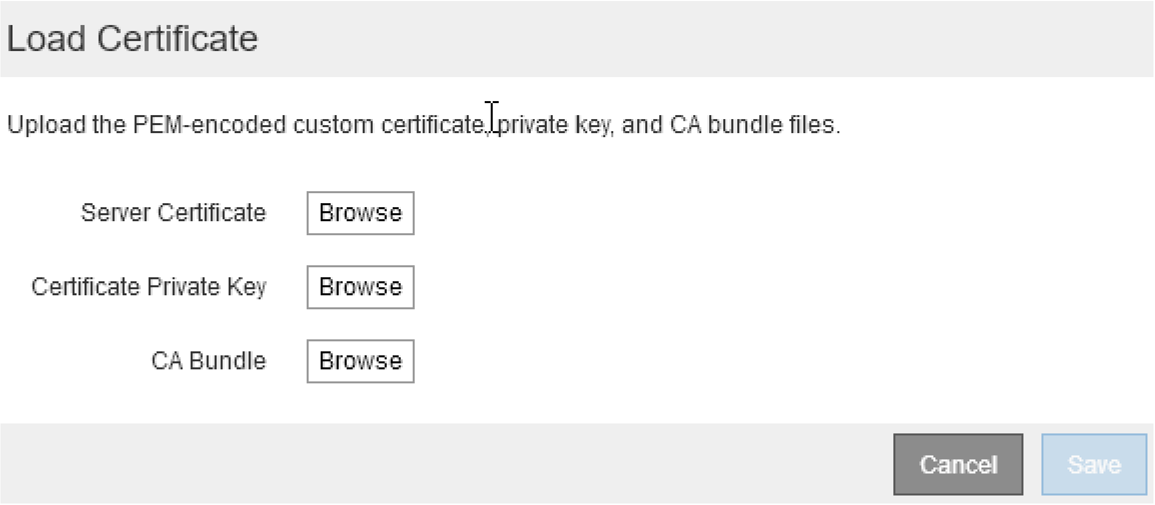
Endpoint Service Configuration

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.

Server Certificate: Browse

Certificate Private Key: Browse

CA Bundle: Browse

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`.

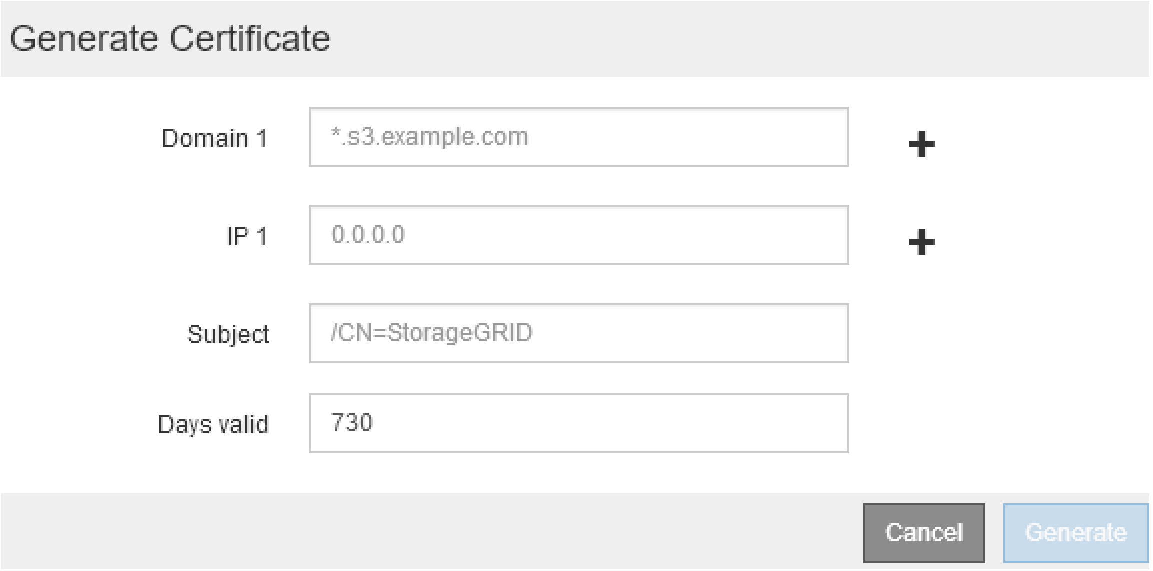
   Configuring S3 API endpoint domain names

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

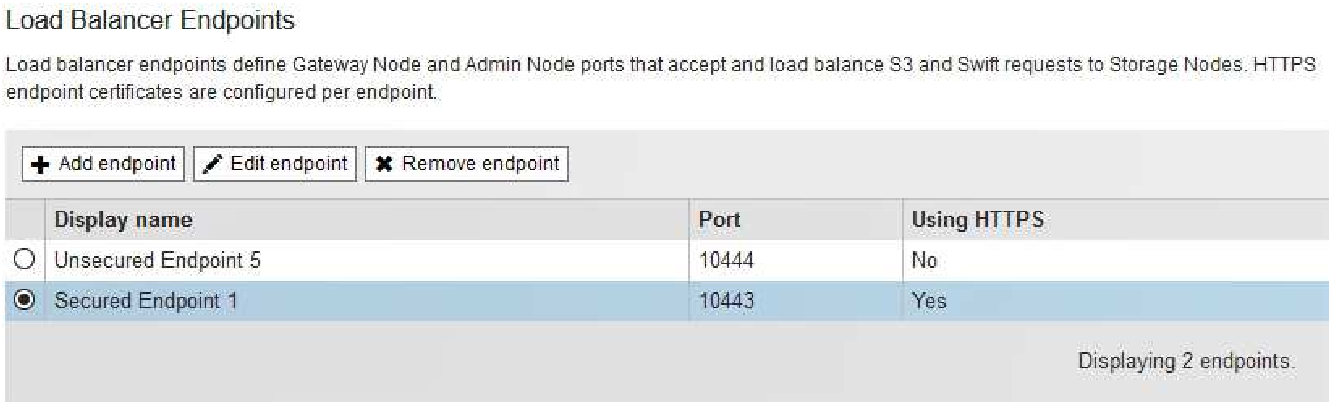
- You must have the Root Access permission.
- You must be signed in to the Grid Manager using a supported browser.

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.

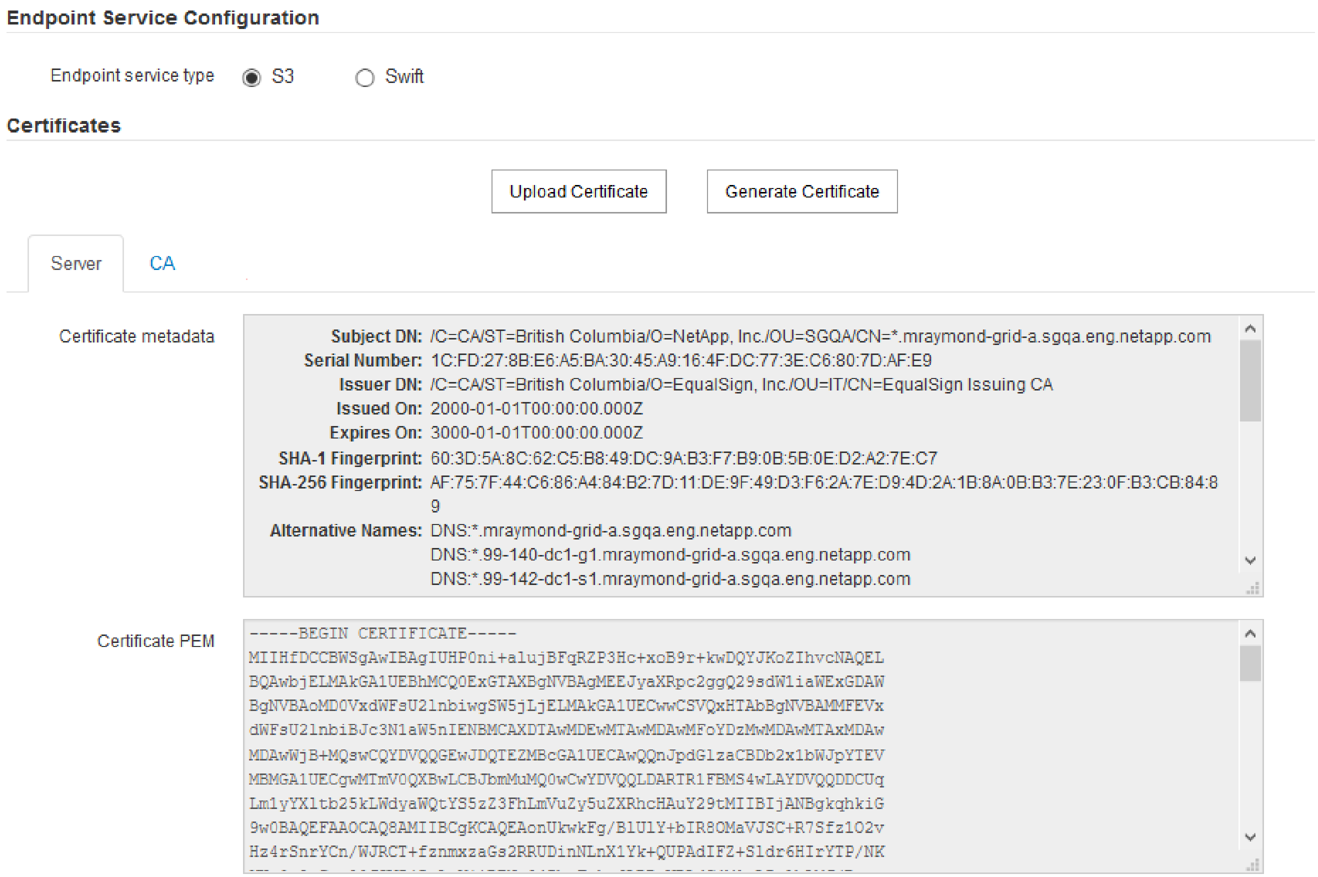
	Display name	Port	Using HTTPS
○	Unsecured Endpoint 5	10444	No
●	Secured Endpoint 1	10443	Yes

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:84:8
                       9
   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.

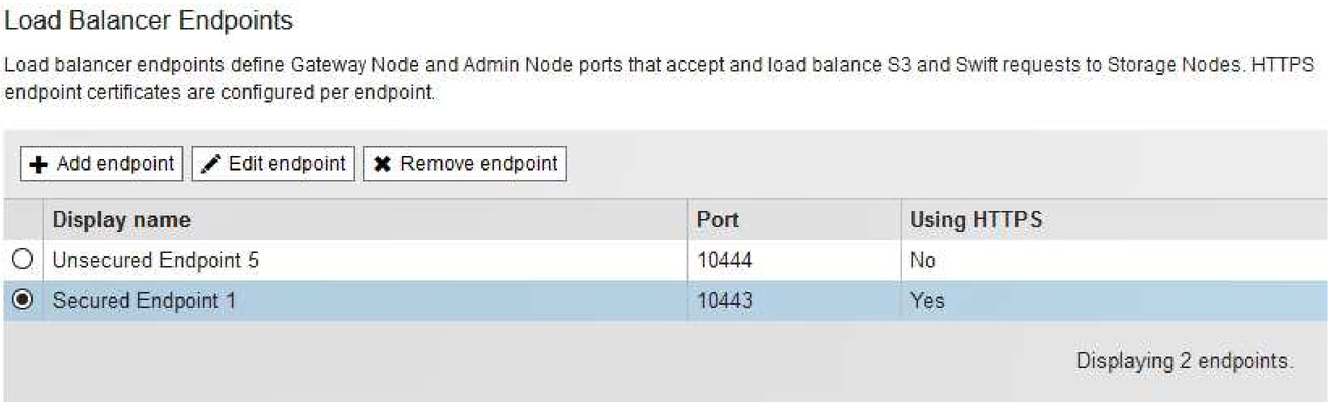
What you'll need

- 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

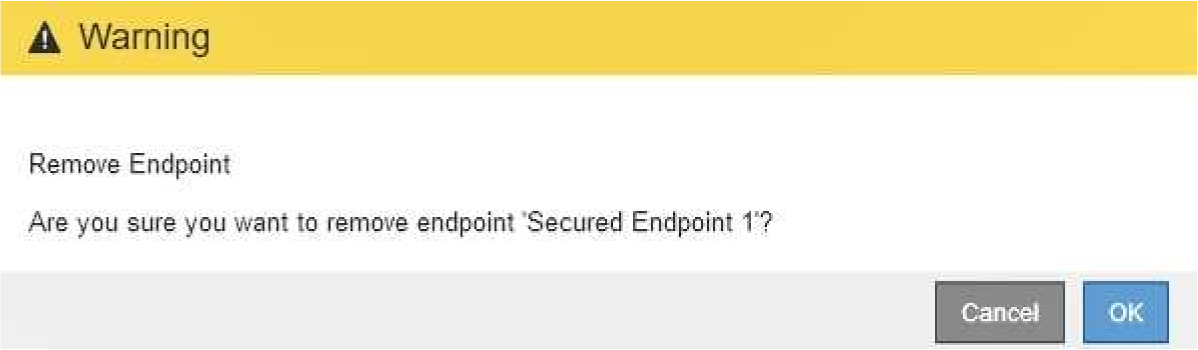
Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

	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.



⚠ Warning

Remove Endpoint

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

4. Click **OK**.

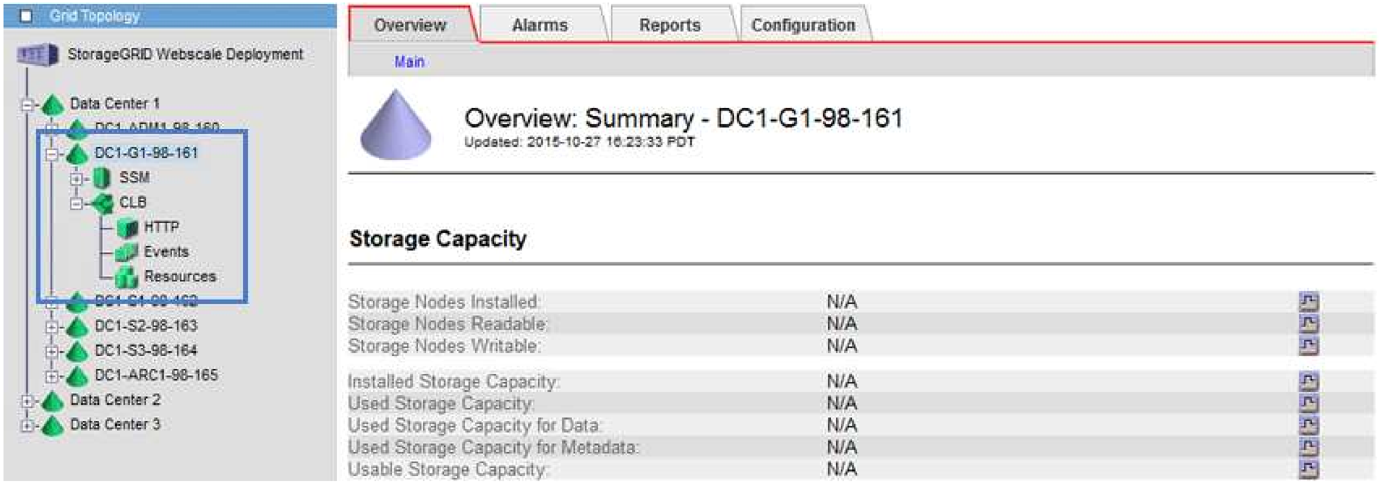
   The endpoint is removed.

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

Copyright information

Trademark information