



Configurar las conexiones de clientes S3 y Swift

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

- Configurar las conexiones de clientes S3 y Swift 1
 - Resumen: Direcciones IP y puertos para conexiones cliente 1
 - Gestión del equilibrio de carga 4
 - Administración de redes de clientes que no son de confianza 14
 - Gestionar grupos de alta disponibilidad 17
 - Configurar nombres de dominio de extremo de API de S3 29
 - Habilitar HTTP para las comunicaciones del cliente 31
 - Controlar qué operaciones de cliente están permitidas 32

Configurar las conexiones de clientes S3 y Swift

Como administrador de grid, gestiona las opciones de configuración que controlan cómo los inquilinos S3 y Swift pueden conectar las aplicaciones cliente con el sistema StorageGRID para almacenar y recuperar datos. Hay una serie de opciones diferentes para responder a los distintos requisitos de cliente y cliente.

Las aplicaciones cliente pueden almacenar o recuperar objetos conectándose a cualquiera de los siguientes elementos:

- El servicio Load Balancer en los nodos de administrador o de puerta de enlace, o bien, de forma opcional, la dirección IP virtual de un grupo de alta disponibilidad (ha) de nodos de administración o nodos de puerta de enlace
- El servicio CLB en los nodos de puerta de enlace o, opcionalmente, la dirección IP virtual de un grupo de nodos de puerta de enlace de alta disponibilidad



El servicio CLB está obsoleto. Los clientes configurados antes de la versión StorageGRID 11.3 pueden seguir utilizando el servicio CLB en los nodos de puerta de enlace. El resto de aplicaciones cliente que dependen de StorageGRID para proporcionar equilibrio de carga se deben conectar mediante el servicio Load Balancer.

- Nodos de almacenamiento, con o sin un equilibrador de carga externo

Opcionalmente, puede configurar las siguientes funciones en el sistema StorageGRID:

- **Servicio de equilibrador de carga:** Permite a los clientes utilizar el servicio de equilibrador de carga mediante la creación de puntos finales de equilibrio de carga para las conexiones de cliente. Al crear un extremo de equilibrio de carga, especifica un número de puerto, si el extremo acepta conexiones HTTP o HTTPS, el tipo de cliente (S3 o Swift) que utilizará el extremo y el certificado que se utilizará para las conexiones HTTPS (si procede).
- **Red cliente no confiable:** Puede hacer que la Red cliente sea más segura configurándola como no confiable. Cuando la red de cliente no es de confianza, los clientes sólo pueden conectarse utilizando puntos finales de equilibrador de carga.
- **Grupos de alta disponibilidad:** Puede crear un grupo ha de nodos de puerta de enlace o nodos de administración para crear una configuración de copia de seguridad activa, o puede utilizar DNS round-robin o un equilibrador de carga de terceros y varios grupos ha para lograr una configuración activo-activo. Las conexiones de clientes se realizan mediante las direcciones IP virtuales de los grupos de alta disponibilidad.

También es posible habilitar el uso de HTTP para los clientes que se conectan a StorageGRID directamente a los nodos de almacenamiento o mediante el servicio CLB (obsoleto), y es posible configurar los nombres de dominio de extremo de la API de S3 para los clientes S3.

Resumen: Direcciones IP y puertos para conexiones cliente

Las aplicaciones cliente pueden conectarse a StorageGRID utilizando la dirección IP de un nodo de grid y el número de puerto de un servicio en ese nodo. Si se configuran los grupos de alta disponibilidad, las aplicaciones cliente se pueden conectar mediante la dirección IP virtual del grupo de alta disponibilidad.

Acerca de esta tarea

Esta tabla resume las distintas formas en que los clientes pueden conectarse a StorageGRID y las direcciones IP y los puertos que se utilizan para cada tipo de conexión. En las instrucciones se describe cómo encontrar esta información en Grid Manager si ya se han configurado puntos finales de equilibrador de carga y grupos de alta disponibilidad (ha).

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Grupo de ALTA DISPONIBILIDAD	Equilibrador de carga	La dirección IP virtual de un grupo de alta disponibilidad	<ul style="list-style-type: none">• Puerto de punto final del equilibrador de carga
Grupo de ALTA DISPONIBILIDAD	CLB Nota: el servicio CLB está en desuso.	La dirección IP virtual de un grupo de alta disponibilidad	Puertos S3 predeterminados: <ul style="list-style-type: none">• HTTPS: 8082• HTTP: 8084 Puertos Swift predeterminados: <ul style="list-style-type: none">• HTTPS:8083• HTTP: 8085
Nodo de administración	Equilibrador de carga	La dirección IP del nodo de administrador	<ul style="list-style-type: none">• Puerto de punto final del equilibrador de carga
Nodo de puerta de enlace	Equilibrador de carga	La dirección IP del nodo de puerta de enlace	<ul style="list-style-type: none">• Puerto de punto final del equilibrador de carga
Nodo de puerta de enlace	CLB Nota: el servicio CLB está en desuso.	La dirección IP del nodo de puerta de enlace Nota: de forma predeterminada, los puertos HTTP para CLB y LDR no están habilitados.	Puertos S3 predeterminados: <ul style="list-style-type: none">• HTTPS: 8082• HTTP: 8084 Puertos Swift predeterminados: <ul style="list-style-type: none">• HTTPS:8083• HTTP: 8085

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Nodo de almacenamiento	LDR	La dirección IP del nodo de almacenamiento	Puertos S3 predeterminados: <ul style="list-style-type: none"> • HTTPS: 18082 • HTTP: 18084 Puertos Swift predeterminados: <ul style="list-style-type: none"> • HTTPS: 18083 • HTTP: 18085

Ejemplos

Para conectar un cliente S3 al extremo de equilibrio de carga de un grupo ha de nodos de puerta de enlace, utilice una URL estructurada como se muestra a continuación:

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

Por ejemplo, si la dirección IP virtual del grupo de alta disponibilidad es 192.0.2.5 y el número de puerto de un extremo de equilibrio de carga de S3 es 10443, un cliente de S3 puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.5:10443`

Para conectar un cliente Swift al extremo Load Balancer de un grupo de ha de nodos de Gateway, utilice una URL estructurada como se muestra a continuación:

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

Por ejemplo, si la dirección IP virtual del grupo de alta disponibilidad es 192.0.2.6 y el número de puerto de un extremo de equilibrio de carga de Swift es 10444, un cliente de Swift puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.6:10444`

Es posible configurar un nombre DNS para la dirección IP que utilizan los clientes para conectarse a StorageGRID. Póngase en contacto con el administrador de red local.

Pasos

1. Inicie sesión en Grid Manager con un navegador compatible.
2. Para encontrar la dirección IP de un nodo de grid:
 - a. Seleccione **Nodes**.
 - b. Seleccione el nodo de administrador, Gateway Node o Storage Node al que desea conectarse.
 - c. Seleccione la ficha **Descripción general**.
 - d. En la sección Node Information, tenga en cuenta las direcciones IP del nodo.
 - e. Haga clic en **Mostrar más** para ver las direcciones IPv6 y las asignaciones de interfaz.

Puede establecer conexiones desde aplicaciones cliente a cualquiera de las direcciones IP de la lista:

- **Eth0:** Red Grid
- **Eth1:** Red de administración (opcional)
- **Eth2:** Red cliente (opcional)



Si va a ver un nodo de administrador o un nodo de puerta de enlace y es el nodo activo de un grupo de alta disponibilidad, en eth2 se muestra la dirección IP virtual del grupo de alta disponibilidad.

3. Para buscar la dirección IP virtual de un grupo de alta disponibilidad:

- a. Seleccione **Configuración > Configuración de red > grupos de alta disponibilidad**.
- b. En la tabla, tenga en cuenta la dirección IP virtual del grupo ha.

4. Para buscar el número de puerto de un extremo Load Balancer:

- a. Seleccione **Configuración > Configuración de red > parámetros de equilibrio de carga**.

Aparece la página Load Balancer Endpoints, donde se muestra la lista de puntos finales que ya se han configurado.

- b. Seleccione un punto final y haga clic en **Editar punto final**.

Se abre la ventana Edit Endpoint y se muestran detalles adicionales sobre el extremo.

- c. Confirme que el extremo que ha seleccionado está configurado para su uso con el protocolo correcto (S3 o Swift) y, a continuación, haga clic en **Cancelar**.
- d. Tenga en cuenta el número de puerto del extremo que desea utilizar para una conexión de cliente.



Si el número de puerto es 80 o 443, el extremo se configura únicamente en los nodos de puerta de enlace, ya que esos puertos están reservados en los nodos de administración. Todos los demás puertos están configurados tanto en los nodos de puerta de enlace como en los de administración.

Gestión del equilibrio de carga

Las funciones de equilibrio de carga de StorageGRID se pueden usar para manejar cargas de trabajo de procesamiento y recuperación de los clientes S3 y Swift. El equilibrio de carga maximiza la velocidad y la capacidad de conexión distribuyendo las cargas de trabajo y las conexiones entre varios nodos de almacenamiento.

Puede lograr el equilibrio de carga en el sistema StorageGRID de las siguientes maneras:

- Use el servicio Load Balancer, que se instala en los nodos de administrador y de puerta de enlace. El servicio Load Balancer proporciona equilibrio de carga de capa 7 y realiza terminación TLS de solicitudes de cliente, inspecciona las solicitudes y establece nuevas conexiones seguras a los nodos de almacenamiento. Este es el mecanismo de equilibrio de carga recomendado.
- Utilice el servicio Connection Load Balancer (CLB), que se instala sólo en nodos Gateway. El servicio CLB proporciona equilibrio de carga de capa 4 y soporta costes de enlace.



El servicio CLB está obsoleto.

- Integre un equilibrador de carga de terceros. Si desea obtener más información, póngase en contacto con el representante de cuenta de NetApp.

Cómo funciona el equilibrio de carga: Servicio de equilibrio de carga

El servicio Load Balancer distribuye conexiones de red entrantes desde aplicaciones cliente hasta nodos de almacenamiento. Para habilitar el equilibrio de carga, debe configurar los extremos del equilibrador de carga mediante el Administrador de grid.

Puede configurar extremos de equilibrador de carga solo para nodos de administración o nodos de puerta de enlace, ya que estos tipos de nodos contienen el servicio Load Balancer. No se pueden configurar extremos para nodos de almacenamiento ni nodos de archivado.

Cada extremo de equilibrio de carga especifica un puerto, un protocolo (HTTP o HTTPS), un tipo de servicio (S3 o Swift) y un modo de enlace. Los extremos HTTPS requieren un certificado de servidor. Los modos de enlace permiten restringir la accesibilidad de los puertos de extremo a:

- Direcciones IP virtuales de alta disponibilidad (ha) específicas
- Interfaces de red específicas de nodos específicos

Consideraciones sobre el puerto

Los clientes pueden acceder a cualquiera de los extremos que configure en cualquier nodo que ejecute el servicio Load Balancer, con dos excepciones: Los puertos 80 y 443 están reservados en nodos de administrador, de modo que los extremos configurados en estos puertos admiten operaciones de balanceo de carga solo en nodos de puerta de enlace.

Si ha reasignado algún puerto, no puede utilizar los mismos puertos para configurar los extremos de equilibrador de carga. Puede crear puntos finales mediante puertos reasignados, pero esos puntos finales se volverán a asignar a los puertos y servicios de CLB originales, no al servicio Load Balancer. Siga los pasos de las instrucciones de recuperación y mantenimiento para eliminar las reasignaciones de puertos.



El servicio CLB está obsoleto.

Disponibilidad de CPU

El servicio Load Balancer en cada nodo de administración y nodo de puerta de enlace funciona de forma independiente cuando se reenvía tráfico de S3 o Swift a los nodos de almacenamiento. Mediante un proceso de ponderación, el servicio Load Balancer envía más solicitudes a los nodos de almacenamiento con una mayor disponibilidad de CPU. La información de carga de CPU del nodo se actualiza cada pocos minutos, pero es posible que la ponderación se actualice con mayor frecuencia. A todos los nodos de almacenamiento se les asigna un valor de peso base mínimo, incluso si un nodo informa de un uso del 100 % o no informa de su uso.

En algunos casos, la información acerca de la disponibilidad de CPU se limita al sitio donde se encuentra el servicio Load Balancer.

Información relacionada

["Mantener recuperar"](#)

Configuración de los extremos del equilibrador de carga

Puede crear, editar y eliminar puntos finales del equilibrador de carga.

Creación de puntos finales del equilibrador de carga

Cada extremo de equilibrio de carga especifica un puerto, un protocolo de red (HTTP o HTTPS) y un tipo de servicio (S3 o Swift). Si se crea un extremo de HTTPS, se debe cargar o generar un certificado de servidor.

Lo que necesitará

- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Si ha reasignado previamente puertos que pretende utilizar para el servicio Load Balancer, debe haber eliminado las reasignaciones.



Si ha reasignado algún puerto, no puede utilizar los mismos puertos para configurar los extremos de equilibrador de carga. Puede crear puntos finales mediante puertos reasignados, pero esos puntos finales se volverán a asignar a los puertos y servicios de CLB originales, no al servicio Load Balancer. Siga los pasos de las instrucciones de recuperación y mantenimiento para eliminar las reasignaciones de puertos.



El servicio CLB está obsoleto.

Pasos

1. Seleccione **Configuración > Configuración de red > parámetros de equilibrio de carga**.

Aparece la página Load Balancer Endpoints.

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.

Add endpoint port Edit endpoint Remove endpoint port

Display name	Port	Using HTTPS
--------------	------	-------------

No endpoints configured.

2. Seleccione **Agregar punto final**.

Se muestra el cuadro de diálogo Create Endpoint.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Cancel Save

- Introduzca un nombre para mostrar para el extremo, que aparecerá en la lista de la página Load Balancer Endpoints.
- Introduzca un número de puerto o deje el número de puerto relleno previamente como está.

Si introduce el número de puerto 80 o 443, el extremo se configura únicamente en los nodos de puerta de enlace, ya que estos puertos están reservados en los nodos de administración.



Los puertos utilizados por otros servicios de red no están permitidos. Consulte las directrices de red para obtener una lista de los puertos utilizados para las comunicaciones internas y externas.

- Seleccione **HTTP** o **HTTPS** para especificar el protocolo de red para este extremo.
- Seleccione un modo de enlace de extremo.
 - Global** (predeterminado): El punto final es accesible en todos los nodos Gateway y Admin en el número de puerto especificado.

Create Endpoint

Display Name

Port

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.

Cancel Save

- VIPS de grupo de alta disponibilidad:** Sólo se puede acceder al terminal a través de las direcciones IP virtuales definidas para los grupos de alta disponibilidad seleccionados. Los extremos definidos en este modo pueden reutilizar el mismo número de puerto, siempre que los grupos de alta disponibilidad definidos por dichos extremos no se superpongan entre sí.

Seleccione los grupos de alta disponibilidad con las direcciones IP virtuales donde desee que aparezca el extremo.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Name	Description	Virtual IP Addresses	Interfaces
<input type="checkbox"/> Group1		192.168.5.163	CO-REF-DC1-ADM1:eth0 (preferred Master)
<input type="checkbox"/> 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.

- **Interfaces de nodo:** Sólo se puede acceder al extremo en los nodos designados y en las interfaces de red. Los extremos definidos en este modo pueden reutilizar el mismo número de puerto siempre que estas interfaces no se superpongan entre sí.

Seleccione las interfaces de nodo en las que desea que aparezca el extremo.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Node	Interface
<input type="checkbox"/> CO-REF-DC1-ADM1	eth0
<input type="checkbox"/> CO-REF-DC1-ADM1	eth1
<input type="checkbox"/> CO-REF-DC1-ADM1	eth2
<input type="checkbox"/> CO-REF-DC1-GW1	eth0
<input type="checkbox"/> CO-REF-DC2-ADM1	eth0
<input type="checkbox"/> 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. Seleccione **Guardar**.

Se muestra el cuadro de diálogo Edit Endpoint.

8. Seleccione **S3** o **Swift** para especificar el tipo de tráfico que servirá este extremo.

Edit Endpoint Unsecured Port A (port 10449)

Endpoint Service Configuration

Endpoint service type S3 Swift

9. Si ha seleccionado **HTTP**, seleccione **Guardar**.

Se crea el extremo no seguro. En la tabla de la página Load Balancer Endpoints se muestra el nombre para mostrar, el número de puerto, el protocolo y el ID de extremo del extremo.

10. Si ha seleccionado **HTTPS** y desea cargar un certificado, seleccione **cargar certificado**.

Load Certificate

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

Server Certificate

Certificate Private Key

CA Bundle

Cancel

Save

- a. Busque el certificado de servidor y la clave privada de certificado.

Para habilitar que los clientes S3 se conecten mediante un nombre de dominio de extremo de API S3, use un certificado comodín o de varios dominios que coincida con todos los nombres de dominio que el cliente podría usar para conectarse al grid. Por ejemplo, el certificado de servidor puede utilizar el nombre de dominio `*.example.com`.

"Configurar nombres de dominio de extremo de API de S3"

- a. Opcionalmente, busque un paquete de CA.
- b. Seleccione **Guardar**.

Aparece los datos de certificado codificados con PEM para el extremo.

11. Si ha seleccionado **HTTPS** y desea generar un certificado, seleccione **generar certificado**.

Generate Certificate

Domain 1	<input type="text" value="*.s3.example.com"/>	+
IP 1	<input type="text" value="0.0.0.0"/>	+
Subject	<input type="text" value="/CN=StorageGRID"/>	
Days valid	<input type="text" value="730"/>	

- a. Introduzca un nombre de dominio o una dirección IP.

Puede usar caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración y de puerta de enlace que ejecutan el servicio Load Balancer. Por ejemplo: `*.sgws.foo.com` utiliza el comodín `*` que se va a representar `gn1.sgws.foo.com` y `gn2.sgws.foo.com`.

"Configurar nombres de dominio de extremo de API de S3"

- a. Seleccione **+** Para agregar otros nombres de dominio o direcciones IP.

Si está usando grupos de alta disponibilidad (ha), añada los nombres de dominio y las direcciones IP de las IP virtuales de alta disponibilidad.

- b. Opcionalmente, introduzca un sujeto X.509, también denominado Nombre distintivo (DN), para identificar quién posee el certificado.
- c. De manera opcional, seleccione el número de días en los que el certificado es válido. El valor predeterminado es 730 días.
- d. Seleccione **generar**.

Se muestran los metadatos del certificado y los datos de certificado codificados con PEM para el extremo.

12. Haga clic en **Guardar**.

Se crea el extremo. En la tabla de la página Load Balancer Endpoints se muestra el nombre para mostrar, el número de puerto, el protocolo y el ID de extremo del extremo.

Información relacionada

["Mantener recuperar"](#)

["Directrices de red"](#)

["Gestionar grupos de alta disponibilidad"](#)

["Administración de redes de clientes que no son de confianza"](#)

Edición de puntos finales del equilibrador de carga

Para un extremo no seguro (HTTP), puede cambiar el tipo de servicio de extremo entre S3 y Swift. En el caso de un extremo protegido (HTTPS), puede editar el tipo de servicio de extremo y ver o cambiar el certificado de seguridad.

Lo que necesitará

- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Pasos

1. Seleccione **Configuración > Configuración de red > parámetros de equilibrio de carga**.

Aparece la página Load Balancer Endpoints. Los extremos existentes se muestran en la tabla.

Los extremos con certificados que caducarán pronto se identifican en la tabla.

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.

<input type="button" value="+ Add endpoint"/> <input type="button" value="✎ Edit endpoint"/> <input type="button" value="✕ Remove endpoint"/>			
	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

2. Seleccione el extremo que desea editar.
3. Haga clic en **Editar punto final**.

Se muestra el cuadro de diálogo Edit Endpoint.

En el caso de un extremo no seguro (HTTP), sólo aparece la sección Configuración del servicio de extremo del cuadro de diálogo. En el caso de un extremo protegido (HTTPS), aparecen las secciones Configuración de Endpoint Service y certificados del cuadro de diálogo, como se muestra en el siguiente ejemplo.

Endpoint Service Configuration

Endpoint service type S3 Swift

Certificates

Upload Certificate

Generate Certificate

Server

CA

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-----
MIIEHfDCCBWSgAwIBAgIUHP0ni+a1ujBFgRZP3Hc+xcB9r+kWdQYJKoZIhvcNAQEL
BQAwbjELMAkGA1UEBhMCQ0ExGTAXBgNVBAgMEEJyaXRpc2ggQ29sdWliaWExGDAW
BgNVBAoMD0VxdWFeU2lnbiwgSW5jLjELMAkGA1UECwwCSVQxHTAbBgNVBAMMFVx
dWFeU2lnbiBjc3N1aW5nIENBMCAxDTAwMDEwMTAwMDAwMDAwMDAwMDAwMDAwMDAw
MDAwWjB+MQswCQYDVQQGEwJDQTEZMBcGA1UECAwQcnJpdG1zaCBDb2x1bWpYTEV
MEMGA1UECgwMTmV0QXBwLCBjb250aW50aW50aW50aW50aW50aW50aW50aW50aW50
LmlyYX1tb25kLWdyYWQtYS5zZ3FhLmVuz3FhLmVuz3FhLmVuz3FhLmVuz3FhLmVuz3
9w0BAQEFAAOCAQ8AMIIBCgKCAQEaonUkwkFg/B1U1Y+bIR80MaVJSC+R7Sfz102v
Hz4rSnrYCh/WJRCT+fznmzxaGz2RRUDinNlnX1Yk+QUPAdIFZ+Sldr6HirYTE/NK
-----
```

4. Realice los cambios deseados en el extremo.

En el caso de un extremo no seguro (HTTP), puede:

- Cambie el tipo de servicio de extremo entre S3 y Swift.
- Cambie el modo de enlace de punto final. Para un extremo protegido (HTTPS), puede:
- Cambie el tipo de servicio de extremo entre S3 y Swift.
- Cambie el modo de enlace de punto final.
- Vea el certificado de seguridad.
- Cargue o genere un nuevo certificado de seguridad cuando el certificado actual haya caducado o esté a punto de caducar.

Seleccione una pestaña para mostrar información detallada sobre el certificado de servidor StorageGRID predeterminado o un certificado firmado de CA que se cargó.



Para cambiar el protocolo de un extremo existente, por ejemplo de HTTP a HTTPS, debe crear un extremo nuevo. Siga las instrucciones para crear puntos finales del equilibrador de carga y seleccione el protocolo deseado.

5. Haga clic en **Guardar**.

Información relacionada

[Creación de puntos finales del equilibrador de carga](#)

Retirada de los extremos del equilibrador de carga

Si ya no necesita un extremo de equilibrador de carga, puede eliminarlo.

Lo que necesitará

- Debe tener el permiso acceso raíz.
- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Pasos

1. Seleccione **Configuración > Configuración de red > parámetros de equilibrio de carga**.

Aparece la página Load Balancer Endpoints. Los extremos existentes se muestran en la tabla.

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.

<input type="button" value="+ Add endpoint"/> <input type="button" value="✎ Edit endpoint"/> <input type="button" value="✕ Remove endpoint"/>			
	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

2. Seleccione el botón de opción situado a la izquierda del extremo que desea eliminar.
3. Haga clic en **Quitar punto final**.

Se muestra un cuadro de diálogo de confirmación.



4. Haga clic en **Aceptar**.

El punto final se elimina.

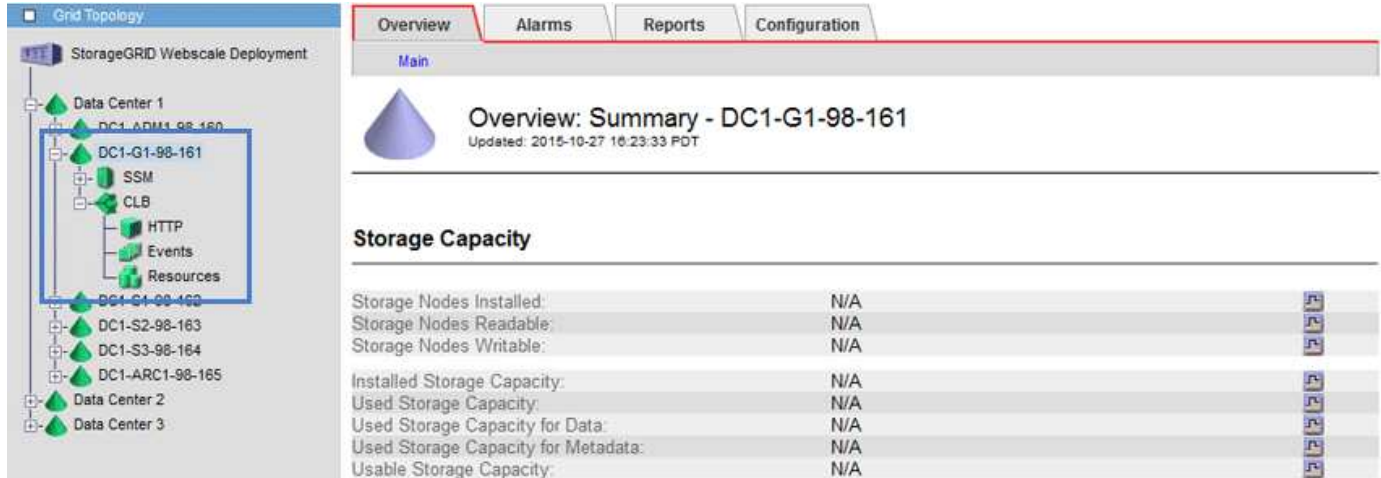
Cómo funciona el equilibrio de carga: Servicio CLB

El servicio Connection Load Balancer (CLB) en los nodos de Gateway queda obsoleto. El servicio Load Balancer es ahora el mecanismo de equilibrio de carga recomendado.

El servicio CLB utiliza el equilibrio de carga de capa 4 para distribuir las conexiones de red TCP entrantes de las aplicaciones cliente al nodo de almacenamiento óptimo en función de la disponibilidad, la carga del

sistema y el coste de enlace configurado por el administrador. Cuando se elige el nodo de almacenamiento óptimo, el servicio CLB establece una conexión de red bidireccional y reenvía el tráfico hacia y desde el nodo elegido. El CLB no considera la configuración de red de red de cuadrícula al dirigir las conexiones de red entrantes.

Para ver información acerca del servicio CLB, seleccione **Soporte > Herramientas > Topología de cuadrícula** y, a continuación, expanda un nodo de puerta de enlace hasta que pueda seleccionar **CLB** y las opciones que aparecen debajo de él.



The screenshot shows the StorageGRID Webconsole interface. On the left, the 'Grid Topology' tree is expanded to show 'Data Center 1' and its nodes, with 'DC1-G1-98-161' selected. The main panel displays the 'Overview: Summary - DC1-G1-98-161' page, which includes a 'Storage Capacity' table.

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

Si decide utilizar el servicio CLB, debe considerar la configuración de los costes de enlace para su sistema StorageGRID.

Información relacionada

["¿Cuáles son los costes de enlace"](#)

["Actualizando costes de enlace"](#)

Administración de redes de clientes que no son de confianza

Si está utilizando una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles aceptando tráfico de cliente entrante sólo en puntos finales configurados explícitamente.

De forma predeterminada, la red de cliente de cada nodo de cuadrícula es *Trusted*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de cuadrícula en todos los puertos externos disponibles (consulte la información acerca de las comunicaciones externas en las directrices de red).

Puede reducir la amenaza de ataques hostiles en su sistema StorageGRID especificando que la red cliente de cada nodo sea *no confiable*. Si la red de cliente de un nodo no es de confianza, el nodo sólo acepta conexiones entrantes en los puertos configurados explícitamente como puntos finales de equilibrador de carga.

Ejemplo 1: Gateway Node solo acepta solicitudes HTTPS S3

Supongamos que desea que un nodo de puerta de enlace rechace todo el tráfico entrante en la red cliente excepto las solicitudes HTTPS S3. Debe realizar estos pasos generales:

1. En la página Load Balancer Endpoints, configure un extremo de equilibrador de carga para S3 a través de HTTPS en el puerto 443.
2. En la página redes de cliente no fiables, especifique que la red de cliente del nodo de puerta de enlace no sea de confianza.

Después de guardar la configuración, se descarta todo el tráfico entrante en la red cliente del nodo de puerta de enlace, excepto las solicitudes HTTPS S3 en el puerto 443 y las solicitudes ICMP echo (ping).

Ejemplo 2: El nodo de almacenamiento envía solicitudes de servicios de plataforma S3

Supongamos que desea habilitar el tráfico saliente del servicio de la plataforma S3 desde un nodo de almacenamiento, pero desea impedir las conexiones entrantes a ese nodo de almacenamiento en la red cliente. Debe realizar este paso general:

- En la página redes de cliente no fiables, indique que la red de clientes del nodo de almacenamiento no es de confianza.

Después de guardar la configuración, el nodo de almacenamiento ya no acepta ningún tráfico entrante en la red cliente, pero continúa permitiendo solicitudes salientes a Amazon Web Services.

Información relacionada

["Directrices de red"](#)

["Configuración de los extremos del equilibrador de carga"](#)

La especificación de la red de cliente de un nodo no es de confianza

Si utiliza una red de cliente, puede especificar si la red de cliente de cada nodo es de confianza o no es de confianza. También puede especificar la configuración predeterminada para los nuevos nodos agregados en una ampliación.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.
- Si desea que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante sólo en puntos finales configurados explícitamente, ha definido los puntos finales del equilibrador de carga.



Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Pasos

1. Seleccione **Configuración > Configuración de red > Red de cliente no confiable**.

Aparece la página redes de cliente no fiables.

Esta página muestra todos los nodos del sistema StorageGRID. La columna motivo no disponible incluye una entrada si la red de cliente del nodo debe ser de confianza.

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.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

- En la sección **establecer nuevo nodo predeterminado**, especifique cuál debe ser la configuración predeterminada cuando se agregan nuevos nodos a la cuadrícula en un procedimiento de expansión.
 - Trusted:** Cuando se agrega un nodo en una expansión, su red de cliente es de confianza.
 - No fiable:** Cuando se agrega un nodo en una expansión, su red cliente no es de confianza. Según sea necesario, puede volver a esta página para cambiar la configuración de un nuevo nodo concreto.



Esta configuración no afecta a los nodos existentes del sistema StorageGRID.

- En la sección **Seleccionar nodos de red de cliente no confiable**, seleccione los nodos que deben permitir conexiones de cliente sólo en puntos finales de equilibrador de carga configurados explícitamente.

Puede seleccionar o anular la selección de la casilla de comprobación en el título para seleccionar o anular la selección de todos los nodos.

- Haga clic en **Guardar**.

Las nuevas reglas de firewall se agregan y aplican inmediatamente. Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Información relacionada

["Configuración de los extremos del equilibrador de carga"](#)

Gestionar grupos de alta disponibilidad

Los grupos de alta disponibilidad pueden usarse para proporcionar conexiones de datos altamente disponibles para clientes S3 y Swift. Los grupos DE ALTA DISPONIBILIDAD también se pueden utilizar para proporcionar conexiones de alta disponibilidad al administrador de grid y al administrador de inquilinos.

- ["Qué es un grupo de alta disponibilidad"](#)
- ["Cómo se utilizan los grupos de alta disponibilidad"](#)
- ["Opciones de configuración para grupos de alta disponibilidad"](#)
- ["Crear un grupo de alta disponibilidad"](#)
- ["Edición de un grupo de alta disponibilidad"](#)
- ["Eliminar un grupo de alta disponibilidad"](#)

Qué es un grupo de alta disponibilidad

Los grupos de alta disponibilidad usan direcciones IP virtuales (VIP) para proporcionar acceso de backup activo a los servicios Gateway Node o Admin Node.

Un grupo de alta disponibilidad consta de una o varias interfaces de red en los nodos de administración y de pasarela. Al crear un grupo ha, se seleccionan las interfaces de red que pertenecen a la red de cuadrícula (eth0) o a la red de cliente (eth2). Todas las interfaces de un grupo de alta disponibilidad deben estar en la misma subred de red.

Un grupo de alta disponibilidad mantiene una o varias direcciones IP virtuales que se han añadido a la interfaz activa en el grupo. Si la interfaz activa deja de estar disponible, las direcciones IP virtuales se mueven a otra interfaz. Por lo general, este proceso de conmutación por error solo se realiza en unos pocos segundos y es lo suficientemente rápido como para que las aplicaciones cliente tengan un impacto escaso y puedan confiar en los comportamientos normales de reintento para continuar con el funcionamiento.

La interfaz activa de un grupo de alta disponibilidad se designa como maestro. El resto de las interfaces se designan como copia de seguridad. Para ver estas designaciones, seleccione **Nodes > node > Descripción general**.

Overview

Hardware

Network



Storage

Load Balancer

Events

Tasks

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 Show more 

Al crear un grupo de alta disponibilidad, se especifica una interfaz para que sea el maestro preferido. El principal preferido es la interfaz activa a menos que se produzca un fallo que haga que las direcciones VIP se reasignan a una interfaz de copia de seguridad. Cuando se resuelve el fallo, las direcciones VIP se vuelven automáticamente al maestro preferido.

La conmutación por error puede activarse por cualquiera de estas razones:

- El nodo en el que se configura la interfaz se desactiva.
- El nodo en el que se configura la interfaz pierde la conectividad con los demás nodos durante al menos 2 minutos
- La interfaz activa se desactiva.
- El servicio Load Balancer se detiene.
- El servicio de alta disponibilidad se detiene.



Es posible que la conmutación al respaldo no se active por errores de red externos al nodo que aloja la interfaz activa. Del mismo modo, la conmutación por error no se activa con el fallo del servicio CLB (obsoleto) o los servicios para el administrador de grid o el administrador de inquilinos.

Si el grupo de alta disponibilidad incluye interfaces de más de dos nodos, la interfaz activa podría moverse a la interfaz de cualquier otro nodo durante la conmutación por error.

Cómo se utilizan los grupos de alta disponibilidad

Puede que quiera utilizar grupos de alta disponibilidad por varios motivos.

- Un grupo de alta disponibilidad puede proporcionar conexiones administrativas de alta disponibilidad al administrador de grid o al administrador de inquilinos.
- Un grupo de alta disponibilidad puede proporcionar conexiones de datos de alta disponibilidad para clientes S3 y Swift.
- Un grupo de alta disponibilidad que contiene una sola interfaz le permite proporcionar muchas direcciones

VIP y establecer explícitamente direcciones IPv6.

Un grupo de alta disponibilidad solo puede proporcionar alta disponibilidad si todos los nodos incluidos en el grupo proporcionan los mismos servicios. Cuando crea un grupo de alta disponibilidad, añada interfaces desde los tipos de nodos que proporcionan los servicios necesarios.

- **Admin Nodes:** Incluye el servicio Load Balancer y permite el acceso al Grid Manager o al arrendatario Manager.
- **Nodos de puerta de enlace:** Incluye el servicio Load Balancer y el servicio CLB (obsoleto).

Objetivo del grupo de alta disponibilidad	Añada nodos de este tipo al grupo de alta disponibilidad
Acceso a Grid Manager	<ul style="list-style-type: none">• Nodo de administración principal (Master preferido)• Nodos de administrador no primario <p>Nota: el nodo de administración principal debe ser el Master preferido. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.</p>
Acceso solo al administrador de inquilinos	<ul style="list-style-type: none">• Nodos de administrador primario o no primario
Acceso al cliente de S3 o Swift: Servicio Load Balancer	<ul style="list-style-type: none">• Nodos de administración• Nodos de puerta de enlace
Acceso al cliente S3 o Swift: Servicio CLB Nota: el servicio CLB está en desuso.	<ul style="list-style-type: none">• Nodos de puerta de enlace

Limitaciones en el uso de grupos de alta disponibilidad con Grid Manager o Intenant Manager

El fallo de los servicios del administrador de grid o del administrador de inquilinos no activa la conmutación por error dentro del grupo de alta disponibilidad.

Si ha iniciado sesión en Grid Manager o en el arrendatario Manager cuando se produce la conmutación por error, ha cerrado sesión y debe volver a iniciar sesión para reanudar la tarea.

No se pueden realizar algunos procedimientos de mantenimiento cuando el nodo administrador principal no está disponible. Durante la conmutación por error, puede utilizar Grid Manager para supervisar el sistema StorageGRID.

Limitaciones del uso de grupos de alta disponibilidad con el servicio CLB

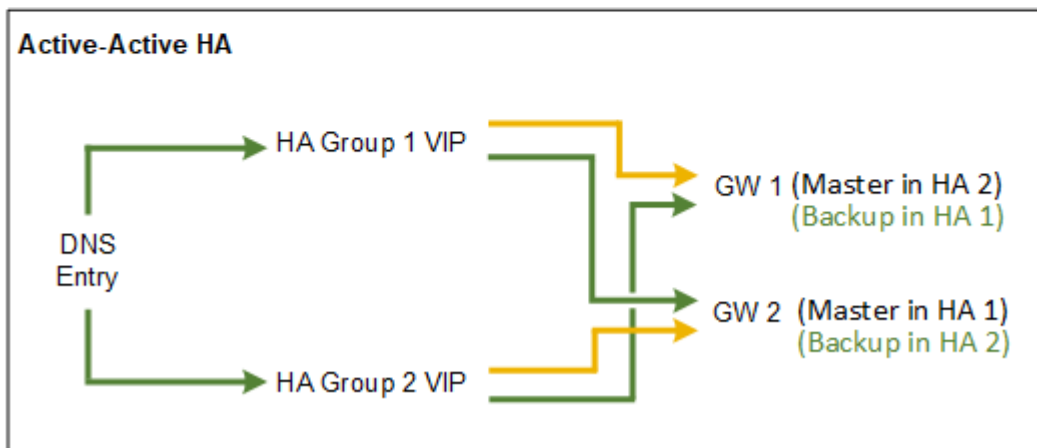
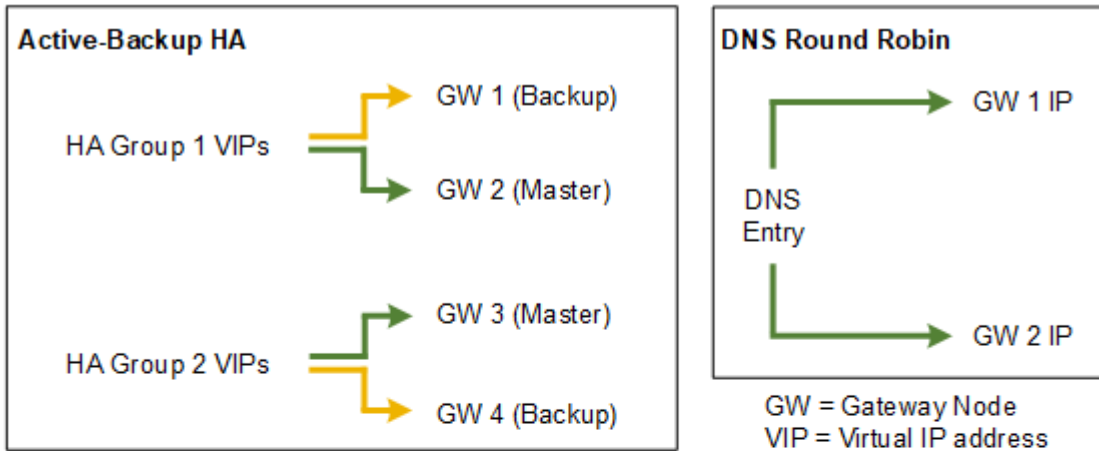
El error del servicio CLB no activa la conmutación por error dentro del grupo ha.



El servicio CLB está obsoleto.

Opciones de configuración para grupos de alta disponibilidad

Los diagramas siguientes proporcionan ejemplos de diferentes formas de configurar grupos de alta disponibilidad. Cada opción tiene ventajas y desventajas.



Al crear varios grupos de alta disponibilidad solapados como se muestra en el ejemplo de alta disponibilidad activo-activo, el rendimiento total se escala con el número de nodos y grupos de alta disponibilidad. Con tres o más nodos y tres o más grupos de alta disponibilidad, también tiene la capacidad de continuar con las operaciones utilizando cualquiera de los VIP incluso durante los procedimientos de mantenimiento, lo que requiere que desconecte un nodo.

La tabla resume las ventajas de cada configuración de alta disponibilidad que se muestra en el diagrama.

Configuración	Ventajas	Desventajas
Alta disponibilidad de Active-Backup	<ul style="list-style-type: none"> • Gestionada por StorageGRID sin dependencias externas. • Rápida recuperación tras fallos. 	<ul style="list-style-type: none"> • Solo un nodo de un grupo de alta disponibilidad está activo. Al menos un nodo por grupo de alta disponibilidad estará inactivo.

Configuración	Ventajas	Desventajas
Operación por turnos DNS	<ul style="list-style-type: none"> • Mayor rendimiento total. • Sin hosts inactivos. 	<ul style="list-style-type: none"> • Conmutación al respaldo lenta, que puede depender del comportamiento del cliente. • Requiere la configuración del hardware fuera de StorageGRID. • Necesita una comprobación del estado implementada por el cliente.
Activa-activa	<ul style="list-style-type: none"> • El tráfico se distribuye entre varios grupos de alta disponibilidad. • Alto rendimiento de agregado escalable con el número de grupos de alta disponibilidad. • Rápida recuperación tras fallos. 	<ul style="list-style-type: none"> • Más complejo de configurar. • Requiere la configuración del hardware fuera de StorageGRID. • Necesita una comprobación del estado implementada por el cliente.

Crear un grupo de alta disponibilidad

Puede crear uno o varios grupos de alta disponibilidad para proporcionar acceso de alta disponibilidad a los servicios en nodos de administración o nodos de puerta de enlace.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.

Acerca de esta tarea

Una interfaz debe cumplir las siguientes condiciones para incluirse en un grupo de alta disponibilidad:

- La interfaz debe ser para un nodo de puerta de enlace o un nodo de administrador.
- La interfaz debe pertenecer a la red de cuadrícula (eth0) o a la red de cliente (eth2).
- La interfaz debe configurarse con dirección IP fija o estática, no con DHCP.

Pasos

1. Seleccione **Configuración > Configuración de red > grupos de alta disponibilidad**.

Aparece la página grupos de alta disponibilidad.

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.

+ Create Edit Remove

Name	Description	Virtual IP Addresses	Interfaces
No HA groups found.			

2. Haga clic en **Crear**.

Se muestra el cuadro de diálogo Crear grupo de alta disponibilidad.

3. Escriba un nombre y, si lo desea, una descripción del grupo de alta disponibilidad.

4. Haga clic en **Seleccionar interfaces**.

Se muestra el cuadro de diálogo Add interfaces to High Availability Group. En la tabla se enumeran los nodos elegibles, las interfaces y las subredes IPv4.

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
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

Cancel Apply

Una interfaz no aparece en la lista si DHCP asigna su dirección IP.

5. En la columna **Agregar al grupo ha**, active la casilla de verificación de la interfaz que desee agregar al grupo ha.

Tenga en cuenta las siguientes directrices para seleccionar interfaces:

- Debe seleccionar al menos una interfaz.
- Si selecciona más de una interfaz, todas las interfaces deben estar en la red de cuadrícula (eth0) o en la red de cliente (eth2).
- Todas las interfaces deben estar en la misma subred o en subredes con un prefijo común.

Las direcciones IP se restringirán a la subred más pequeña (la que tenga el prefijo más grande).

- Si selecciona interfaces en diferentes tipos de nodos y se produce una conmutación al nodo de respaldo, solo estarán disponibles en las IP virtuales los servicios comunes a los nodos seleccionados.
 - Seleccione dos o más nodos de administrador para la protección de alta disponibilidad de Grid Manager o del inquilino Manager.
 - Seleccione dos o más nodos de administrador, nodos de puerta de enlace o ambos para la protección de alta disponibilidad del servicio Load Balancer.
 - Seleccione dos o más nodos de puerta de enlace para la protección de alta disponibilidad del servicio CLB.



El servicio CLB está obsoleto.

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
<input checked="" type="checkbox"/>	DC1-ADM1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC1-G1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	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.

Cancel

Apply

6. Haga clic en **aplicar**.

Las interfaces seleccionadas se muestran en la sección interfaces de la página Create High Availability Group. De forma predeterminada, la primera interfaz de la lista se selecciona como patrón preferido.

Create High Availability Group

High Availability Group

Name

Description

Interfaces

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

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
g140-g1	eth2	47.47.0.0/21	<input checked="" type="radio"/>
g140-g2	eth2	47.47.0.0/21	<input type="radio"/>

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



Cancel

Save

- Si desea que una interfaz diferente sea el Master preferido, seleccione esa interfaz en la columna **Master** preferido.

El principal preferido es la interfaz activa a menos que se produzca un fallo que haga que las direcciones VIP se reasignan a una interfaz de copia de seguridad.



Si el grupo ha proporciona acceso a Grid Manager, debe seleccionar una interfaz en el nodo de administración principal para que sea el maestro preferido. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

- En la sección direcciones IP virtuales de la página, introduzca de una a 10 direcciones IP virtuales para el grupo de alta disponibilidad. Haga clic en el signo más (+) Para agregar varias direcciones IP.

Debe proporcionar al menos una dirección IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

Las direcciones IPv4 deben estar en la subred IPv4 compartida por todas las interfaces miembros.

9. Haga clic en **Guardar**.

El grupo ha se ha creado y ahora puede utilizar las direcciones IP virtuales configuradas.

Información relacionada

["Instale Red Hat Enterprise Linux o CentOS"](#)

["Instale VMware"](#)

["Instalar Ubuntu o Debian"](#)

["Gestión del equilibrio de carga"](#)

Edición de un grupo de alta disponibilidad

Puede editar un grupo de alta disponibilidad para cambiar su nombre y descripción, agregar o quitar interfaces, o agregar o actualizar una dirección IP virtual.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.

Acerca de esta tarea

Entre algunos de los motivos para editar un grupo de alta disponibilidad se encuentran los siguientes:

- Agregar una interfaz a un grupo existente. La dirección IP de la interfaz debe estar dentro de la misma subred que otras interfaces ya asignadas al grupo.
- Quitar una interfaz de un grupo de alta disponibilidad. Por ejemplo, no puede iniciar un procedimiento de retirada de sitio o nodo si se utiliza la interfaz de un nodo para la red de cuadrícula o la red de cliente en un grupo ha.

Pasos

1. Seleccione **Configuración > Configuración de red > grupos de alta disponibilidad**.

Aparece la página grupos de alta disponibilidad.

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
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. Seleccione el grupo ha que desea editar y haga clic en **Editar**.

Se muestra el cuadro de diálogo Editar grupo de alta disponibilidad.

3. Si lo desea, actualice el nombre o la descripción del grupo.
4. Opcionalmente, haga clic en **Seleccionar interfaces** para cambiar las interfaces del grupo ha.

Se muestra el cuadro de diálogo Add interfaces to High Availability Group.

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
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

Una interfaz no aparece en la lista si DHCP asigna su dirección IP.

5. Active o anule la selección de las casillas de verificación para agregar o quitar interfaces.

Tenga en cuenta las siguientes directrices para seleccionar interfaces:

- Debe seleccionar al menos una interfaz.
- Si selecciona más de una interfaz, todas las interfaces deben estar en la red de cuadrícula (eth0) o en la red de cliente (eth2).
- Todas las interfaces deben estar en la misma subred o en subredes con un prefijo común.

Las direcciones IP se restringirán a la subred más pequeña (la que tenga el prefijo más grande).

- Si selecciona interfaces en diferentes tipos de nodos y se produce una conmutación al nodo de respaldo, solo estarán disponibles en las IP virtuales los servicios comunes a los nodos seleccionados.
 - Seleccione dos o más nodos de administrador para la protección de alta disponibilidad de Grid Manager o del inquilino Manager.
 - Seleccione dos o más nodos de administrador, nodos de puerta de enlace o ambos para la protección de alta disponibilidad del servicio Load Balancer.
 - Seleccione dos o más nodos de puerta de enlace para la protección de alta disponibilidad del servicio CLB.



El servicio CLB está obsoleto.

6. Haga clic en **aplicar**.

Las interfaces seleccionadas se muestran en la sección interfaces de la página. De forma predeterminada, la primera interfaz de la lista se selecciona como patrón preferido.

Edit High Availability Group 'HA Group - Admin Nodes'

High Availability Group

Name

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	<input checked="" type="radio"/>
DC2-ADM1	eth0	10.96.100.0/23	<input type="radio"/>

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

7. Si desea que una interfaz diferente sea el Master preferido, seleccione esa interfaz en la columna **Master** preferido.

El principal preferido es la interfaz activa a menos que se produzca un fallo que haga que las direcciones VIP se reasignan a una interfaz de copia de seguridad.



Si el grupo proporciona acceso a Grid Manager, debe seleccionar una interfaz en el nodo de administración principal para que sea el maestro preferido. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

8. De manera opcional, actualice las direcciones IP virtuales del grupo de alta disponibilidad.

Debe proporcionar al menos una dirección IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

Las direcciones IPv4 deben estar en la subred IPv4 compartida por todas las interfaces miembros.

9. Haga clic en **Guardar**.

El grupo de alta disponibilidad se ha actualizado.

Eliminar un grupo de alta disponibilidad

Puede eliminar un grupo de alta disponibilidad que ya no utilice.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.

Aboque por esta tarea

Si quita un grupo de alta disponibilidad, todos los clientes S3 o Swift que se hayan configurado para usar una de las direcciones IP virtuales del grupo ya no podrán conectarse a StorageGRID. Para evitar que se produzcan interrupciones en el cliente, debe actualizar todas las aplicaciones cliente S3 o Swift afectadas antes de quitar un grupo de alta disponibilidad. Actualice cada cliente para que se conecte mediante otra dirección IP, por ejemplo, la dirección IP virtual de un grupo ha diferente o la dirección IP configurada para una interfaz durante la instalación o mediante DHCP.

Pasos

1. Seleccione **Configuración > Configuración de red > grupos de alta disponibilidad**.

Aparece la página grupos de alta disponibilidad.

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.

<input type="button" value="+ Create"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>				
	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. Seleccione el grupo ha que desea quitar y haga clic en **Quitar**.

Aparece la advertencia Eliminar grupo de alta disponibilidad.

Warning

Delete High Availability Group

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

Cancel

OK

3. Haga clic en **Aceptar**.

El grupo de alta disponibilidad se ha eliminado.

Configurar nombres de dominio de extremo de API de S3

Para admitir solicitudes de estilo alojado virtuales S3, debe usar Grid Manager para configurar la lista de nombres de dominio de extremo a los que se conectan los clientes S3.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Debe haber confirmado que no hay una actualización de grid en curso.



No realice ningún cambio en la configuración del nombre de dominio cuando se esté realizando una actualización de la cuadrícula.

Acerca de esta tarea

Para habilitar que los clientes usen nombres de dominio extremo de S3, debe realizar todas las tareas siguientes:

- Use Grid Manager para añadir los nombres de dominio de extremo S3 al sistema StorageGRID.
- Asegúrese de que el certificado que utiliza el cliente para las conexiones HTTPS a StorageGRID esté firmado para todos los nombres de dominio que el cliente necesita.

Por ejemplo, si el extremo es `s3.company.com`, Debe asegurarse de que el certificado utilizado para las conexiones HTTPS incluye `s3.company.com` Nombre alternativo (SAN) del asunto comodín del extremo y del extremo: `*.s3.company.com`.

- Configure el servidor DNS que utiliza el cliente. Incluya registros DNS para las direcciones IP que utilizan los clientes para realizar conexiones y asegúrese de que los registros hagan referencia a todos los nombres de dominio de extremo requeridos, incluidos los nombres de comodín.



Los clientes se pueden conectar a StorageGRID mediante la dirección IP de un nodo de puerta de enlace, un nodo de administrador o un nodo de almacenamiento, o bien mediante la conexión a la dirección IP virtual de un grupo de alta disponibilidad. Debe comprender cómo se conectan las aplicaciones cliente a la cuadrícula para que incluya las direcciones IP correctas en los registros DNS.

El certificado que un cliente utiliza para las conexiones HTTPS depende de cómo se conecta el cliente al grid:

- Si un cliente se conecta mediante el servicio Load Balancer, utiliza el certificado para un extremo de equilibrio de carga específico.



Cada extremo de equilibrador de carga tiene su propio certificado y cada extremo se puede configurar para reconocer diferentes nombres de dominio de extremo.

- Si el cliente se conecta a un nodo de almacenamiento o al servicio CLB en un nodo de puerta de enlace, el cliente utiliza un certificado de servidor personalizado de cuadrícula que se ha actualizado para incluir todos los nombres de dominio de extremo requeridos.



El servicio CLB está obsoleto.

Pasos

1. Seleccione **Configuración > Configuración de red > nombres de dominio**.

Aparece la página Endpoint Domain Names.

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	<input type="text" value="s3.example.com"/>	✕
Endpoint 2	<input type="text"/>	+ ✕

2. Con el icono (+) para añadir campos adicionales, introduzca la lista de nombres de dominio de extremo API de S3 en los campos **Endpoint**.

Si esta lista está vacía, se deshabilita la compatibilidad con las solicitudes de estilo alojado virtuales de S3.

3. Haga clic en **Guardar**.
4. Asegúrese de que los certificados de servidor que utilizan los clientes coinciden con los nombres de dominio de extremo requeridos.
 - Para los clientes que utilizan el servicio Load Balancer, actualice el certificado asociado con el extremo de equilibrio de carga al que se conecta el cliente.
 - Para los clientes que se conectan directamente a nodos de almacenamiento o que usan el servicio CLB en nodos de puerta de enlace, actualice el certificado de servidor personalizado para la cuadrícula.

5. Agregue los registros DNS necesarios para garantizar que se puedan resolver las solicitudes de nombres de dominio de extremo.

Resultado

Ahora, cuando los clientes utilizan el extremo `bucket.s3.company.com`, El servidor DNS resuelve el punto final correcto y el certificado autentica el punto final como se esperaba.

Información relacionada

["Use S3"](#)

["Visualización de direcciones IP"](#)

["Crear un grupo de alta disponibilidad"](#)

["Configuración de un certificado de servidor personalizado para las conexiones al nodo de almacenamiento o al servicio CLB"](#)

["Configuración de los extremos del equilibrador de carga"](#)

Habilitar HTTP para las comunicaciones del cliente

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para todas las conexiones a nodos de almacenamiento o al servicio CLB obsoleto en nodos de puerta de enlace. Puede habilitar HTTP opcionalmente para estas conexiones, por ejemplo, al probar una cuadrícula que no sea de producción.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

Complete esta tarea solo si los clientes S3 y Swift necesitan realizar conexiones HTTP directamente a los nodos de almacenamiento o al servicio CLB obsoleto en los nodos de puerta de enlace.

No es necesario completar esta tarea para clientes que solo utilizan conexiones HTTPS o para clientes que se conectan al servicio Load Balancer (ya que puede configurar cada extremo de Load Balancer para usar HTTP o HTTPS). Consulte la información sobre la configuración de puntos finales del equilibrador de carga para obtener más información.

Consulte ["Resumen: Direcciones IP y puertos para conexiones cliente"](#) Para conocer los puertos que utilizan los clientes S3 y Swift al conectarse a los nodos de almacenamiento o al servicio CLB obsoleto a través de HTTP o HTTPS



Tenga cuidado al habilitar HTTP para una cuadrícula de producción porque las solicitudes se enviarán sin cifrar.

Pasos

1. Seleccione **Configuración > Configuración del sistema > Opciones de cuadrícula**.
2. En la sección Opciones de red , active la casilla de verificación **Activar conexión HTTP** .

Network Options



3. Haga clic en **Guardar**.

Información relacionada

["Configuración de los extremos del equilibrador de carga"](#)

["Use S3"](#)

["Use Swift"](#)

Controlar qué operaciones de cliente están permitidas

Puede seleccionar la opción de cuadrícula evitar modificación de cliente para denegar operaciones específicas de cliente HTTP.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

Evitar modificación de cliente es un valor para todo el sistema. Cuando se selecciona la opción impedir modificación de cliente, se deniegan las siguientes solicitudes:

• API REST S3

- Eliminar solicitudes de bloques
- Cualquier solicitud para modificar los datos de un objeto existente, los metadatos definidos por el usuario o el etiquetado de objetos S3



Este ajuste no se aplica a bloques con versiones habilitadas. El control de versiones ya evita modificaciones en los datos de objetos, los metadatos definidos por el usuario y el etiquetado de objetos.

• API REST de Swift

- Eliminar solicitudes de contenedor
- Solicitudes para modificar cualquier objeto existente. Por ejemplo, se deniegan las siguientes operaciones: Put Overwrite, Delete, Metadata Update, etc.

Pasos

1. Seleccione **Configuración > Configuración del sistema > Opciones de cuadrícula**.

2. En la sección Opciones de red, active la casilla de verificación **evitar modificación de cliente**.

Network Options

Prevent Client Modification



Enable HTTP Connection



Network Transfer Encryption



AES128-SHA

AES256-SHA

3. Haga clic en **Guardar**.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.