Gestionar redes y conexiones StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

Gestionar redes y conexiones StorageGRID

Puede utilizar Grid Manager para configurar y administrar redes y conexiones StorageGRID.

Consulte "Configurar las conexiones de clientes S3 y Swift" Para aprender a conectar clientes S3 o Swift.

- "Directrices para redes StorageGRID"
- "Visualización de direcciones IP"
- "Cifrados compatibles para conexiones TLS salientes"
- "Cambiando el cifrado de transferencia de red"
- "Configuración de certificados de servidor"
- "Configurando la configuración del proxy de almacenamiento"
- "Configurando los ajustes del proxy de administrador"
- "Gestión de directivas de clasificación de tráfico"
- "¿Cuáles son los costes de enlace"

Directrices para redes StorageGRID

StorageGRID admite hasta tres interfaces de red por nodo de grid, lo que permite configurar la red para cada nodo de grid individual de modo que se ajuste a sus requisitos de seguridad y acceso.

> Para modificar o añadir una red para un nodo de grid, consulte las instrucciones de recuperación y mantenimiento. Para obtener más información acerca de la topología de red, consulte las instrucciones de redes.

Red Grid

Obligatorio. La red de red se utiliza para todo el tráfico interno de StorageGRID. Proporciona conectividad entre todos los nodos de la cuadrícula, en todos los sitios y subredes.

Red de administración

Opcional. La red de administración suele utilizarse para la administración y el mantenimiento del sistema. También se puede utilizar para el acceso a protocolos de cliente. La red de administración suele ser una red privada y no es necesario que se pueda enrutar entre sitios.

Red cliente

Opcional. La red cliente es una red abierta que se suele utilizar para proporcionar acceso a aplicaciones cliente S3 y Swift, de modo que la red Grid se pueda aislar y proteger. La red de cliente puede comunicarse con cualquier subred accesible a través de la puerta de enlace local.

Directrices

- Cada nodo de grid StorageGRID requiere una interfaz de red dedicada, una dirección IP, una máscara de subred y una puerta de enlace para cada red a la que está asignado.
- Un nodo de grid no puede tener más de una interfaz en una red.
- Se admite una sola puerta de enlace, por red y cada nodo de grid, y debe estar en la misma subred que el nodo. Si es necesario, puede implementar un enrutamiento más complejo en la puerta de enlace.
- En cada nodo, cada red asigna una interfaz de red específica.

Red	Nombre de la interfaz
Cuadrícula	eth0
Admin (opcional)	eth1
Cliente (opcional)	eth2

- Si el nodo está conectado a un dispositivo StorageGRID, se utilizan puertos específicos para cada red. Para obtener más información, consulte las instrucciones de instalación del dispositivo.
- La ruta predeterminada se genera automáticamente, por nodo. Si eth2 está habilitado, 0.0.0.0/0 utiliza la red cliente en eth2. Si eth2 no está habilitado, 0.0.0.0/0 utiliza la red de cuadrícula en eth0.
- La red cliente no se pone en funcionamiento hasta que el nodo de grid se ha Unido a la cuadrícula
- La red de administrador se puede configurar durante la puesta en marcha del nodo de grid para permitir el acceso a la interfaz de usuario de la instalación antes de que la cuadrícula esté totalmente instalada.

Información relacionada

"Mantener recuperar"

"Directrices de red"

Visualización de direcciones IP

Puede ver la dirección IP de cada nodo de grid en el sistema StorageGRID. A continuación, puede usar esta dirección IP para iniciar sesión en el nodo de grid en la línea de comandos y realizar varios procedimientos de mantenimiento.

Lo que necesitará

Debe iniciar sesión en Grid Manager mediante un explorador compatible.

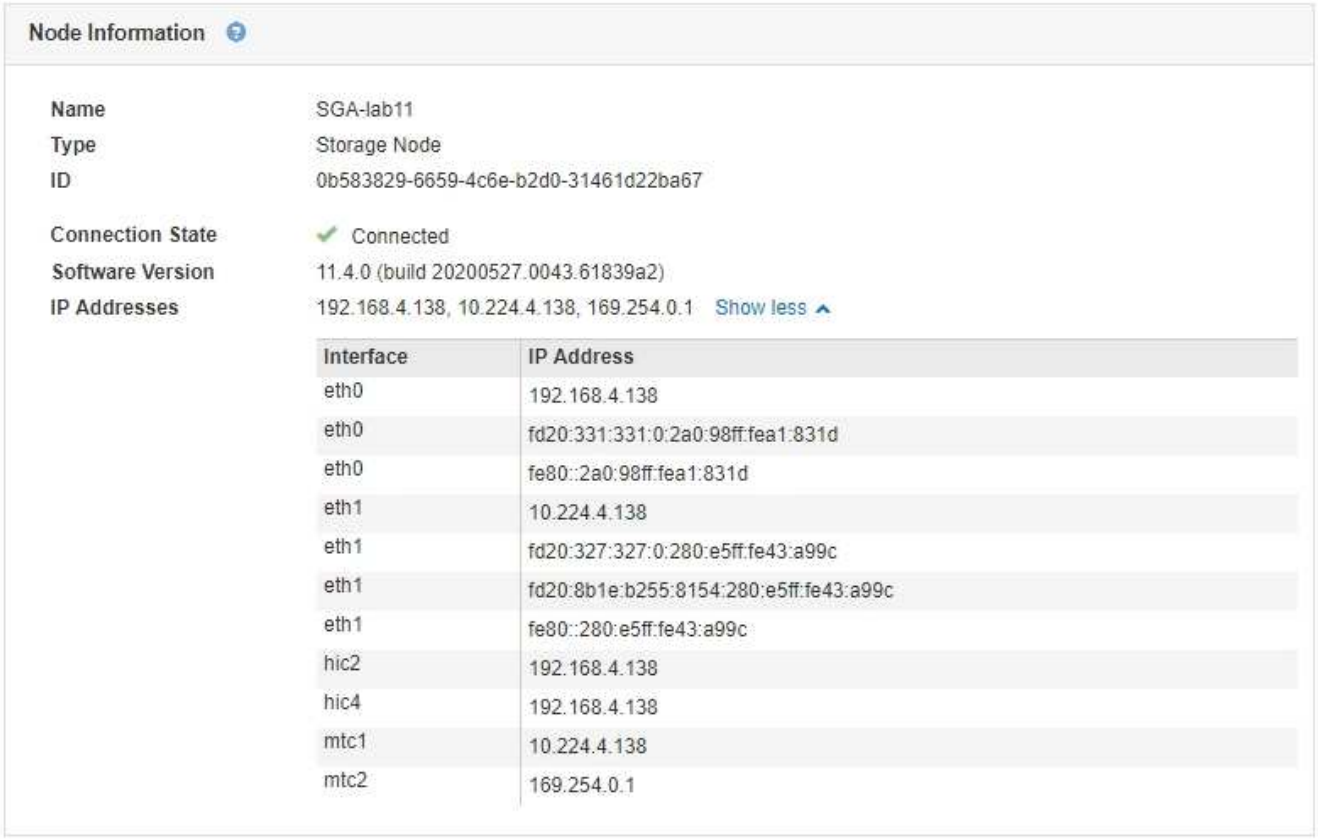
Acerca de esta tarea

Para obtener información acerca de cómo cambiar direcciones IP, consulte las instrucciones de recuperación y mantenimiento.

Pasos

1. Seleccione **Nodes** > ***grid node*** > **Descripción general**.
2. Haga clic en **Mostrar más** a la derecha del título direcciones IP.

   Las direcciones IP de ese nodo de grid se enumeran en una tabla.



Información relacionada

"Mantener recuperar"

Cifrados compatibles para conexiones TLS salientes

El sistema StorageGRID es compatible con un conjunto limitado de conjuntos de cifrado para conexiones TLS (seguridad de la capa de transporte) con los sistemas externos utilizados para la federación de identidades y los pools de almacenamiento en cloud.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3 para conexiones a sistemas externos que se utilizan para la federación de identidades y los pools de almacenamiento en cloud.

Se han seleccionado los cifrados TLS compatibles con sistemas externos para garantizar la compatibilidad con una gama de sistemas externos. La lista supera la lista de cifrados que se admiten con aplicaciones cliente S3 o Swift.

> Las opciones de configuración de TLS, como las versiones del protocolo, los cifrados, los algoritmos de intercambio de claves y los algoritmos MAC no se pueden configurar en StorageGRID. Si tiene solicitudes específicas sobre esta configuración, póngase en contacto con su representante de cuenta de NetApp.

Paquetes de cifrado TLS 1.2 admitidos

Se admiten los siguientes conjuntos de cifrado TLS 1.2:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Paquetes de cifrado TLS 1.3 admitidos

Se admiten los siguientes conjuntos de cifrado TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Cambiando el cifrado de transferencia de red

El sistema StorageGRID utiliza Seguridad de la capa de transporte (TLS) para proteger el tráfico de control interno entre los nodos de la cuadrícula. La opción Network Transfer Encryption (cifrado de transferencia de red) establece el algoritmo utilizado por TLS para cifrar el tráfico de control entre los nodos de la cuadrícula. Esta configuración no afecta al cifrado de datos.

Lo que necesitará

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

Acerca de esta tarea

De forma predeterminada, el cifrado de transferencia de red utiliza el algoritmo AES256-SHA. El tráfico de control también se puede cifrar utilizando el algoritmo AES128-SHA.

Pasos

1. Seleccione **Configuración** > **Configuración del sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de red, cambie el cifrado de transferencia de red a **AES128-SHA** o **AES256-SHA** (predeterminado).

3. Haga clic en **Guardar**.

Configuración de certificados de servidor

Puede personalizar los certificados de servidor que utiliza el sistema StorageGRID.

El sistema StorageGRID utiliza certificados de seguridad para varios fines distintos:

- Certificados del servidor de la interfaz de gestión: Se utiliza para proteger el acceso al administrador de grid, al administrador de inquilinos, a la API de gestión de grid y a la API de gestión de inquilinos.
- Certificados de servidor de API de almacenamiento: Se utiliza para proteger el acceso a los nodos de almacenamiento y puerta de enlace, que las aplicaciones cliente API utilizan para cargar y descargar datos de objetos.

Puede utilizar los certificados predeterminados creados durante la instalación, o puede reemplazar, o ambos, estos tipos predeterminados de certificados por sus propios certificados personalizados.

Tipos admitidos de certificado de servidor personalizado

El sistema StorageGRID admite certificados de servidor personalizados cifrados con RSA o ECDSA (algoritmo de firma digital de curva elíptica).

Para obtener más información sobre cómo protege StorageGRID las conexiones de cliente para la API REST, consulte las guías de implementación de S3 o Swift.

Certificados para extremos de equilibrador de carga

StorageGRID gestiona los certificados utilizados para los extremos del equilibrador de carga por separado. Para configurar certificados de equilibrador de carga, consulte las instrucciones para configurar los extremos de equilibrador de carga.

Información relacionada

"Use S3"

"Use Swift"

"Configuración de los extremos del equilibrador de carga"

Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos

Puede reemplazar el certificado de servidor StorageGRID predeterminado por un único

certificado de servidor personalizado que permite a los usuarios acceder al Administrador de grid y al Administrador de inquilinos sin tener que encontrar advertencias de seguridad.

Acerca de esta tarea

De manera predeterminada, cada nodo del administrador se envía un certificado firmado por la CA de grid. Estos certificados firmados por CA pueden sustituirse por un solo certificado de servidor personalizado común y una clave privada correspondiente.

Dado que se utiliza un único certificado de servidor personalizado para todos los nodos de administración, debe especificar el certificado como un comodín o certificado de varios dominios si los clientes necesitan verificar el nombre de host al conectarse a Grid Manager y al Gestor de inquilinos. Defina el certificado personalizado de modo que coincida con todos los nodos de administrador de la cuadrícula.

Debe completar la configuración en el servidor y, en función de la entidad emisora de certificados raíz (CA) que esté utilizando, los usuarios también pueden necesitar instalar el certificado de CA raíz en el explorador Web que utilizarán para acceder a Grid Manager y al Gestor de inquilinos.

> Para garantizar que las operaciones no se interrumpen con un certificado de servidor fallido, la alarma **caducidad del certificado de servidor para la interfaz de administración** y la alarma de caducidad del certificado de interfaz de administración heredada (MCEP) se activan cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver el número de días hasta que caduque el certificado de servicio actual seleccionando **Soporte** > **Herramientas** > **Topología de cuadrícula**. A continuación, seleccione ***primary Admin Node*** > **CMN** > **Resources**.

> Si accede a Grid Manager o a Intenant Manager utilizando un nombre de dominio en lugar de una dirección IP, el explorador mostrará un error de certificado sin una opción para omitir si se produce alguna de las siguientes situaciones:
>
> - El certificado del servidor de la interfaz de gestión personalizada caduca.
> - Se revierte de un certificado del servidor de interfaz de gestión personalizado al certificado de servidor predeterminado.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **certificados de servidor**.
2. En la sección Certificado de servidor de la interfaz de administración, haga clic en **instalar certificado personalizado**.
3. Cargue los archivos de certificado de servidor requeridos:
   - **Certificado de servidor**: El archivo de certificado de servidor personalizado (`.crt`).
   - **Clave privada del certificado del servidor**: El archivo de clave privada del certificado del servidor personalizado (`.key`).

     > Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

   - **Paquete CA**: Un único archivo que contiene los certificados de cada entidad emisora de certificados intermedia (CA). El archivo debe contener cada uno de los archivos de certificado de CA codificados con PEM, concatenados en el orden de la cadena de certificados.

4. Haga clic en **Guardar**.

   Los certificados de servidor personalizados se utilizan para todas las conexiones de cliente nuevas posteriores.

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

   > Después de cargar un nuevo certificado, permita que se borren todas las alertas de caducidad de certificados (o alarmas heredadas) relacionadas.

5. Actualice la página para garantizar que se actualice el explorador web.

Restauración de los certificados de servidor predeterminados para el administrador de grid y el administrador de inquilinos

Puede volver a utilizar los certificados de servidor predeterminados para el administrador de grid y el administrador de inquilinos.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **certificados de servidor**.
2. En la sección Administrar certificado de servidor de interfaz, haga clic en **utilizar certificados predeterminados**.
3. Haga clic en **Aceptar** en el cuadro de diálogo de confirmación.

   Al restaurar los certificados de servidor predeterminados, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. Los certificados de servidor predeterminados se utilizan para todas las conexiones de cliente nuevas posteriores.

4. Actualice la página para garantizar que se actualice el explorador web.

Configuración de un certificado de servidor personalizado para las conexiones al nodo de almacenamiento o al servicio CLB

Es posible reemplazar el certificado de servidor que se utiliza para las conexiones de clientes S3 o Swift al nodo de almacenamiento o al servicio CLB (obsoleto) en Gateway Node. El certificado de servidor personalizado de reemplazo es específico de su organización.

Acerca de esta tarea

De forma predeterminada, cada nodo de almacenamiento recibe un certificado de servidor X.509 firmado por la CA de grid. Estos certificados firmados por CA pueden sustituirse por un solo certificado de servidor personalizado común y una clave privada correspondiente.

Un único certificado de servidor personalizado se usa para todos los nodos de almacenamiento, por lo que debe especificar el certificado como comodín o certificado de varios dominios si los clientes necesitan verificar el nombre de host al conectarse al extremo de almacenamiento. Defina el certificado personalizado de forma que coincida con todos los nodos de almacenamiento de la cuadrícula.

Después de completar la configuración en el servidor, es posible que los usuarios también deban instalar el certificado de CA raíz en el cliente API S3 o Swift que utilizarán para acceder al sistema, según la entidad de

certificación (CA) raíz que use.

> Para asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alarma **caducidad del certificado de servidor para los extremos de la API de almacenamiento** y la alarma de caducidad del certificado de los extremos del servicio de la API de almacenamiento (SCEP) se activan cuando el certificado del servidor raíz está a punto de expirar. Según sea necesario, puede ver el número de días hasta que caduque el certificado de servicio actual seleccionando **Soporte** > **Herramientas** > **Topología de cuadrícula**. A continuación, seleccione ***primary Admin Node*** > **CMN** > **Resources**.

Los certificados personalizados solo se utilizan si los clientes se conectan a StorageGRID mediante el servicio CLB obsoleto en los nodos de puerta de enlace o si se conectan directamente a los nodos de almacenamiento. Los clientes S3 o Swift que se conectan a StorageGRID mediante el servicio Load Balancer en los nodos de administración o de puerta de enlace usan el certificado configurado para el extremo de balanceo de carga.

> La alerta **caducidad del certificado de punto final de equilibrador de carga** se activa para los extremos de equilibrador de carga que caducarán pronto.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **certificados de servidor**.
2. En la sección Object Storage API Service Endpoints Server Certificate, haga clic en **instalar certificado personalizado**.
3. Cargue los archivos de certificado de servidor requeridos:
   - **Certificado de servidor**: El archivo de certificado de servidor personalizado (`.crt`).
   - **Clave privada del certificado del servidor**: El archivo de clave privada del certificado del servidor personalizado (`.key`).

     > Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

   - **Paquete CA**: Un único archivo que contiene los certificados de cada entidad emisora de certificados intermedia (CA). El archivo debe contener cada uno de los archivos de certificado de CA codificados con PEM, concatenados en el orden de la cadena de certificados.
4. Haga clic en **Guardar**.

   El certificado de servidor personalizado se utiliza para todas las conexiones de cliente API nuevas posteriores.

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

   > Después de cargar un nuevo certificado, permita que se borren todas las alertas de caducidad de certificados (o alarmas heredadas) relacionadas.

5. Actualice la página para garantizar que se actualice el explorador web.

Información relacionada

"Use S3"

"Use Swift"

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

Restaurar los certificados de servidor predeterminados para los extremos de la API DE REST de S3 y Swift

Puede revertir a usar los certificados de servidor predeterminados para los extremos de la API DE REST de S3 y Swift.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **certificados de servidor**.
2. En la sección Object Storage API Service Endpoints Server Certificate, haga clic en **utilizar certificados predeterminados**.
3. Haga clic en **Aceptar** en el cuadro de diálogo de confirmación.

   Cuando se restauran los certificados de servidor predeterminados para los extremos de API de almacenamiento de objetos, se eliminan los archivos de certificado de servidor personalizados que se configuraron y no se pueden recuperar desde el sistema. Los certificados de servidor predeterminados se utilizan para todas las conexiones de clientes API nuevas posteriores.

4. Actualice la página para garantizar que se actualice el explorador web.

Copia del certificado de CA del sistema StorageGRID

StorageGRID usa una entidad de certificación (CA) interna para proteger el tráfico interno. Este certificado no cambia si carga sus propios certificados.

Lo que necesitará

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

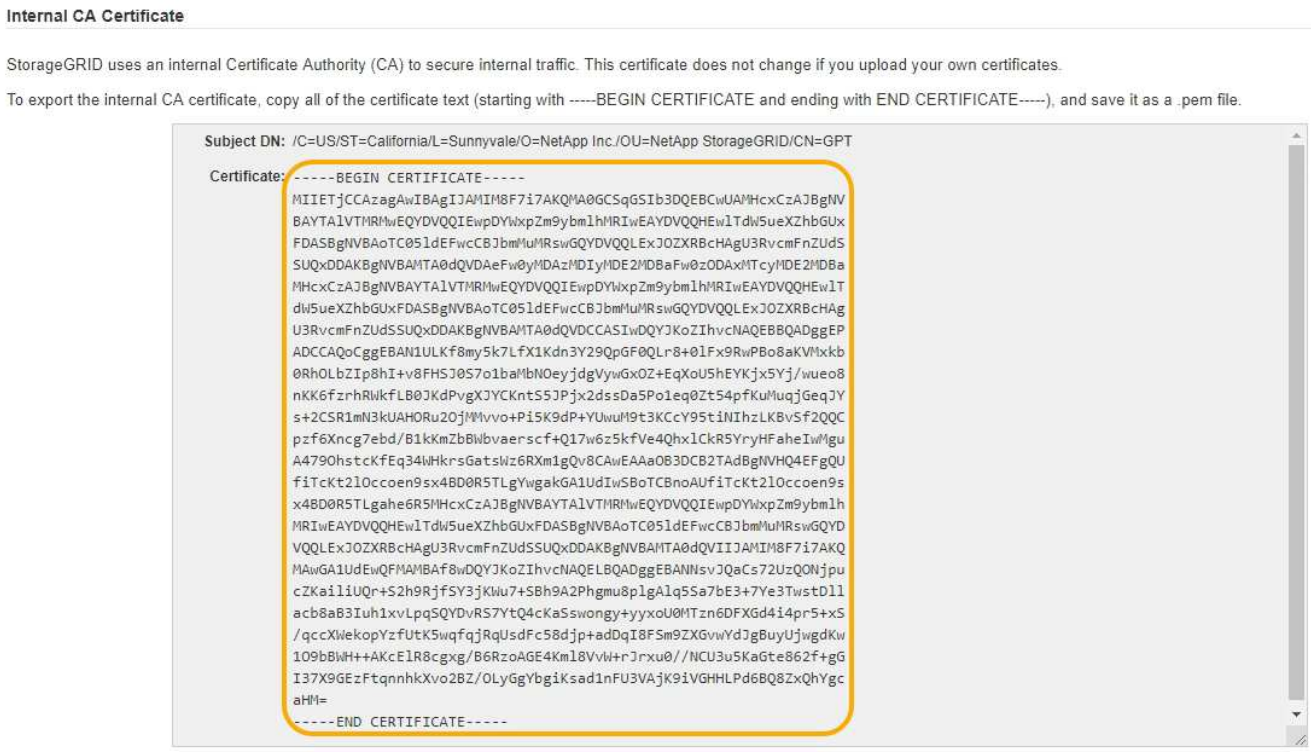
Acerca de esta tarea

Si se ha configurado un certificado de servidor personalizado, las aplicaciones cliente deben verificar el servidor mediante el certificado de servidor personalizado. No deben copiar el certificado de CA desde el sistema StorageGRID.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **certificados de servidor**.
2. En la sección **Certificado CA interno**, seleccione todo el texto del certificado.

   Debe incluir `-----BEGIN CERTIFICATE-----` y.. `-----END CERTIFICATE-----` en su selección.



3. Haga clic con el botón derecho del ratón en el texto seleccionado y seleccione **Copiar**.
4. Pegue el certificado copiado en un editor de texto.
5. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Configurar certificados StorageGRID para FabricPool

En el caso de clientes S3 que realizan una validación de nombre de host estricta y no admiten la deshabilitación de la validación estricta de nombre de host, como clientes ONTAP que utilizan FabricPool, puede generar o cargar un certificado de servidor al configurar el extremo del equilibrador de carga.

Lo que necesitará

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

Acerca de esta tarea

Al crear un extremo de equilibrador de carga, puede generar un certificado de servidor autofirmado o cargar un certificado firmado por una entidad de certificación (CA) conocida. En los entornos de producción, se debe utilizar un certificado firmado por una CA conocida. Los certificados firmados por una CA se pueden rotar de forma no disruptiva. También son más seguros porque ofrecen una mejor protección contra los ataques de tipo "hombre en el medio".

En los siguientes pasos, se ofrecen directrices generales para clientes S3 que usan FabricPool. Para obtener información y procedimientos más detallados, consulte las instrucciones de configuración de StorageGRID para FabricPool.

El servicio de equilibrador de carga de conexión (CLB) independiente en los nodos de puerta de enlace queda obsoleto y ya no se recomienda su uso con FabricPool.

Pasos

1. Opcionalmente, configure un grupo de alta disponibilidad (ha) para que lo utilice FabricPool.
2. Cree un extremo de equilibrador de carga de S3 para que se utilice FabricPool.

   Cuando crea un extremo de equilibrador de carga HTTPS, se le solicita que cargue el certificado de servidor, la clave privada de certificado y el paquete de CA.

3. Adjuntar StorageGRID como nivel de cloud en ONTAP.

   Especifique el puerto de extremo de equilibrio de carga y el nombre de dominio completo utilizado en el certificado de CA que ha cargado. A continuación, proporcione el certificado de CA.

   Si una CA intermedia emitió el certificado StorageGRID, debe proporcionar el certificado de CA intermedio. Si la CA raíz emitió directamente el certificado StorageGRID, debe proporcionar el certificado de CA raíz.

Información relacionada

"Configure StorageGRID para FabricPool"

Generar un certificado de servidor autofirmado para la interfaz de gestión

Puede usar un script para generar un certificado de servidor autofirmado para los clientes API de gestión que requieren una validación de nombre de host estricta.

Lo que necesitará

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.

Acerca de esta tarea

En los entornos de producción, debe utilizar un certificado firmado por una entidad de certificación (CA) conocida. Los certificados firmados por una CA se pueden rotar de forma no disruptiva. También son más seguros porque ofrecen una mejor protección contra los ataques de tipo "hombre en el medio".

Pasos

1. Obtenga el nombre de dominio completo (FQDN) de cada nodo de administrador.
2. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

3. Configure StorageGRID con un certificado autofirmado nuevo.

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

- Para `--domains`, Utilice comodines para representar los nombres de dominio completos de todos los nodos Admin. Por ejemplo: `*.ui.storagegrid.example.com` utiliza el comodín * que se va a representar `admin1.ui.storagegrid.example.com` y.. `admin2.ui.storagegrid.example.com`.
- Configurado `--type` para `management` Para configurar el certificado utilizado por el Administrador de grid y el Administrador de inquilinos.
- De forma predeterminada, los certificados generados son válidos durante un año (365 días) y deben volver a crearse antes de que expiren. Puede utilizar el `--days` argumento para anular el período de validez predeterminado.

> El período de validez de un certificado comienza cuando `make-certificate` se ejecuta. Debe asegurarse de que el cliente de API de gestión esté sincronizado con el mismo origen de hora que StorageGRID; de lo contrario, el cliente podría rechazar el certificado.

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

El resultado contiene el certificado público que necesita el cliente API de gestión.

4. Seleccione y copie el certificado.

   Incluya las etiquetas INICIAL Y FINAL en su selección.

5. Cierre la sesión del shell de comandos. `$ exit`
6. Confirme que se configuró el certificado:
   a. Acceda a Grid Manager.
   b. Seleccione **Configuración** > **certificados de servidor** > **Certificado de servidor de interfaz de administración**.
7. Configure el cliente de API de gestión para que utilice el certificado público que ha copiado. Incluya las etiquetas INICIAL Y FINAL.

Configurando la configuración del proxy de almacenamiento

Si utiliza servicios de plataforma o pools de almacenamiento en cloud, puede configurar un proxy no transparente entre los nodos de almacenamiento y los extremos de S3 externos. Por ejemplo, es posible que necesite un proxy no transparente para permitir que los mensajes de servicios de plataforma se envíen a extremos externos, como un punto final en Internet.

Lo que necesitará

- Debe tener permisos de acceso específicos.

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

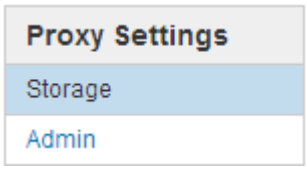
Acerca de esta tarea

Puede configurar los ajustes de un único proxy de almacenamiento.

Pasos

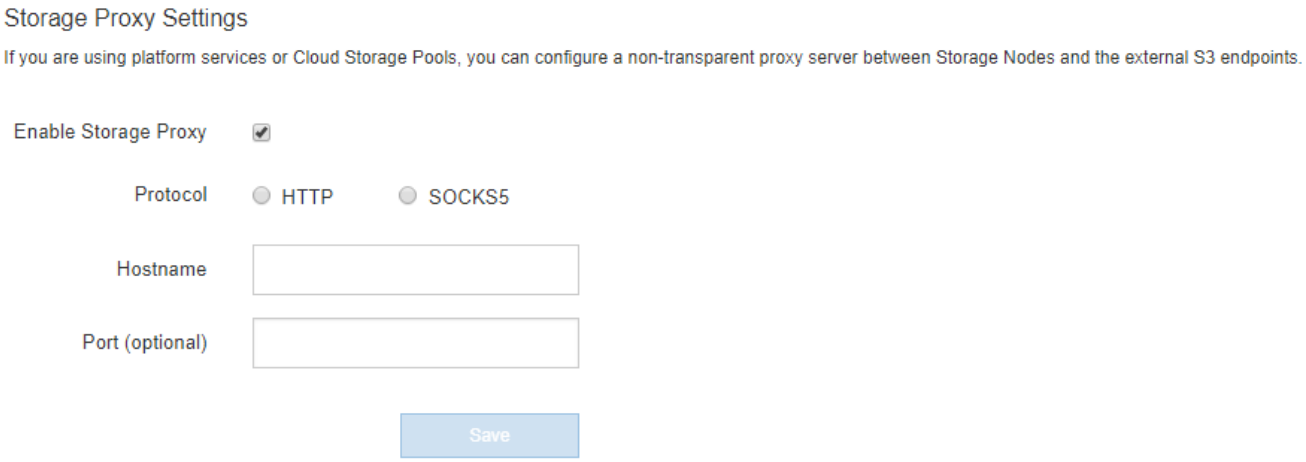
1. Seleccione **Configuración** > **Configuración de red** > **Configuración de proxy**.

   Se muestra la página Storage Proxy Settings. De forma predeterminada, **almacenamiento** está seleccionado en el menú de la barra lateral.

2. Active la casilla de verificación **Activar proxy de almacenamiento**.

   Aparecen los campos para configurar un proxy de almacenamiento.

3. Seleccione el protocolo del proxy de almacenamiento no transparente.
4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. De manera opcional, introduzca el puerto utilizado para conectarse al servidor proxy.

   Puede dejar este campo en blanco si utiliza el puerto predeterminado para el protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Haga clic en **Guardar**.

   Una vez guardado el proxy de almacenamiento, se pueden configurar y probar nuevos extremos para los servicios de plataforma o Cloud Storage Pools.

   > Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

7. Compruebe la configuración del servidor proxy para asegurarse de que los mensajes de StorageGRID relacionados con el servicio de la plataforma no se bloqueen.

Después de terminar

Si necesita desactivar un proxy de almacenamiento, anule la selección de la casilla de verificación **Activar proxy de almacenamiento** y haga clic en **Guardar**.

Información relacionada

"Redes y puertos para servicios de plataforma"

"Gestión de objetos con ILM"

Configurando los ajustes del proxy de administrador

Si envía mensajes de AutoSupport mediante HTTP o HTTPS, puede configurar un servidor proxy no transparente entre los nodos de administrador y el soporte técnico (AutoSupport).

Lo que necesitará

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

Acerca de esta tarea

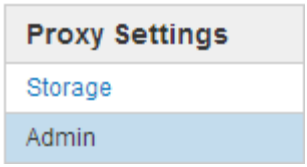
Puede configurar los ajustes de un único proxy de administración.

Pasos

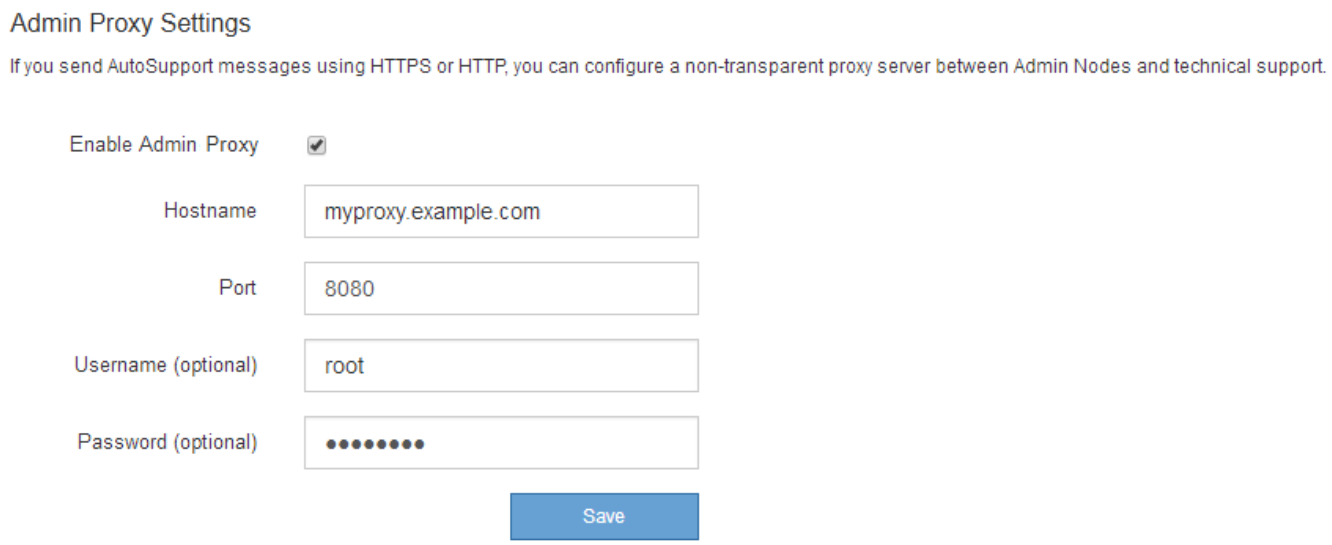
1. Seleccione **Configuración** > **Configuración de red** > **Configuración de proxy**.

   Aparece la página Admin Proxy Settings (Configuración del proxy de administración). De forma predeterminada, **almacenamiento** está seleccionado en el menú de la barra lateral.

2. En el menú de la barra lateral, seleccione **Admin**.



3. Active la casilla de verificación **Activar proxy de administración**.



4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Introduzca el puerto utilizado para conectarse al servidor proxy.
6. Si lo desea, introduzca el nombre de usuario del proxy.

   Deje este campo en blanco si el servidor proxy no requiere un nombre de usuario.

7. De forma opcional, introduzca la contraseña del proxy.

   Deje este campo en blanco si el servidor proxy no requiere una contraseña.

8. Haga clic en **Guardar**.

   Una vez guardado el proxy de administrador, se configura el servidor proxy entre los nodos de administrador y el soporte técnico.

   > Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

9. Si necesita desactivar el proxy, anule la selección de la casilla de verificación **Activar proxy de administración** y haga clic en **Guardar**.

Información relacionada

"Especificar el protocolo para los mensajes de AutoSupport"

Gestión de directivas de clasificación de tráfico

Para mejorar sus ofertas de calidad de servicio (QoS), puede crear normativas de clasificación del tráfico para identificar y supervisar distintos tipos de tráfico de red. Estas políticas pueden ayudar a limitar y supervisar el tráfico.

Las políticas de clasificación del tráfico se aplican a los extremos en el servicio StorageGRID Load Balancer para los nodos de puerta de enlace y los nodos de administración. Para crear directivas de clasificación de tráfico, debe haber creado ya puntos finales de equilibrador de carga.

Reglas de coincidencia y límites opcionales

Cada directiva de clasificación de tráfico contiene una o más reglas coincidentes para identificar el tráfico de red relacionado con una o varias de las siguientes entidades:

- Cucharones
- Clientes
- Subredes (subredes IPv4 que contienen al cliente)
- Puntos finales (puntos finales del equilibrador de carga)

StorageGRID supervisa el tráfico que coincide con cualquier regla dentro de la política de acuerdo con los objetivos de la regla. Cualquier tráfico que coincida con cualquier regla de una directiva se gestiona mediante dicha directiva. A la inversa, puede establecer reglas que coincidan con todo el tráfico excepto una entidad especificada.

Opcionalmente, puede establecer límites para una directiva en función de los siguientes parámetros:

- Ancho de banda del agregado en
- Ancho de banda del agregado agotado
- Solicitudes de lectura simultáneas
- Solicitudes de escritura simultáneas
- Ancho de banda por solicitud en
- Ancho de banda por solicitud agotado
- Tasa de solicitud de lectura
- Tasa de solicitudes de escritura

> Puede crear políticas para limitar el ancho de banda agregado o para limitar el ancho de banda por solicitud. Sin embargo, StorageGRID no puede limitar ambos tipos de ancho de banda a la vez. Los límites de ancho de banda agregados pueden imponer un impacto adicional mínimo en el rendimiento en el tráfico no limitado.

Limitación del tráfico

Cuando ha creado directivas de clasificación de tráfico, el tráfico se limita según el tipo de reglas y límites establecidos. Para límites de ancho de banda agregados o por solicitud, las solicitudes se transmiten de entrada o salida a la velocidad establecida. StorageGRID sólo puede aplicar una velocidad, por lo que la política más específica, por tipo de matrcher, es la aplicada. Para todos los demás tipos de límites, las solicitudes de clientes se retrasan 250 milisegundos y reciben una respuesta de reducción lenta de 503 para las solicitudes que exceden cualquier límite de directiva coincidente.

En Grid Manager, puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera.

Uso de políticas de clasificación del tráfico con SLA

Puede utilizar políticas de clasificación del tráfico junto con los límites de capacidad y protección de datos para aplicar acuerdos de nivel de servicio (SLA) que ofrezcan detalles sobre la capacidad, la protección de datos y el rendimiento.

Los límites de clasificación del tráfico se implementan por equilibrador de carga. Si el tráfico se distribuye de forma simultánea entre varios equilibradores de carga, las tasas máximas totales son un múltiplo de los límites de velocidad que especifique.

El siguiente ejemplo muestra tres niveles de un acuerdo de nivel de servicio. Puede crear políticas de clasificación del tráfico para alcanzar los objetivos de rendimiento de cada nivel de SLA.

Nivel de servicio	Capacidad	Protección de datos	Rendimiento	Coste
Oro	1 PB de almacenamiento permitido	Regla de 3 copia de ILM	25 000 solicitudes/s Ancho de banda de 5 GB/s (40 Gbps)	por mes
Plata	Capacidad de almacenamiento de 250 TB	2 regla de copia de ILM	10 000 solicitudes/s Ancho de banda de 1.25 GB/s (10 Gbps)	$$ al mes
Bronce	Capacidad de almacenamiento de 100 TB	2 regla de copia de ILM	5 000 solicitudes/s Ancho de banda de 1 GB/s (8 Gbps)	$ al mes

Creación de directivas de clasificación de tráfico

Cree políticas de clasificación de tráfico si desea supervisar y, opcionalmente, limitar el tráfico de red por bloque, inquilino, subred IP o extremo de equilibrador de carga. De manera opcional, puede establecer límites para una política en función del ancho de banda, el número de solicitudes simultáneas o la tasa de solicitudes.

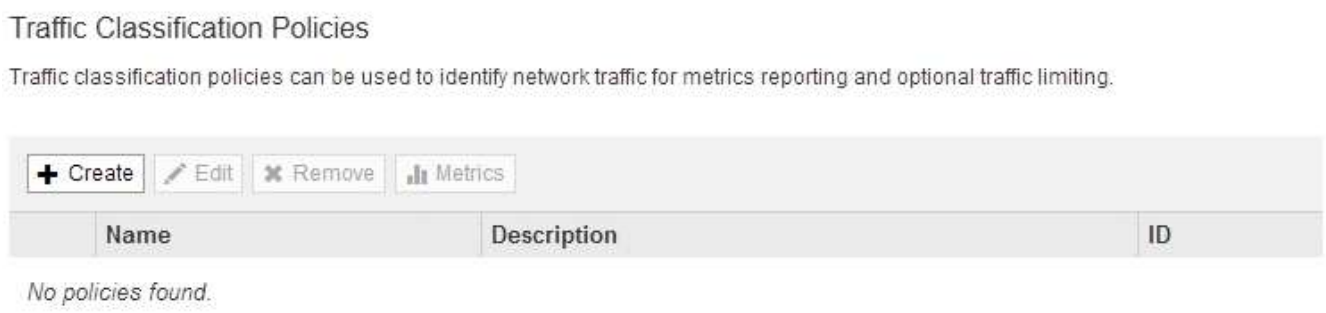
Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.
- Debe haber creado cualquier punto final de equilibrador de carga que desee que coincida.
- Debe haber creado los inquilinos que desee que coincidan.

Pasos

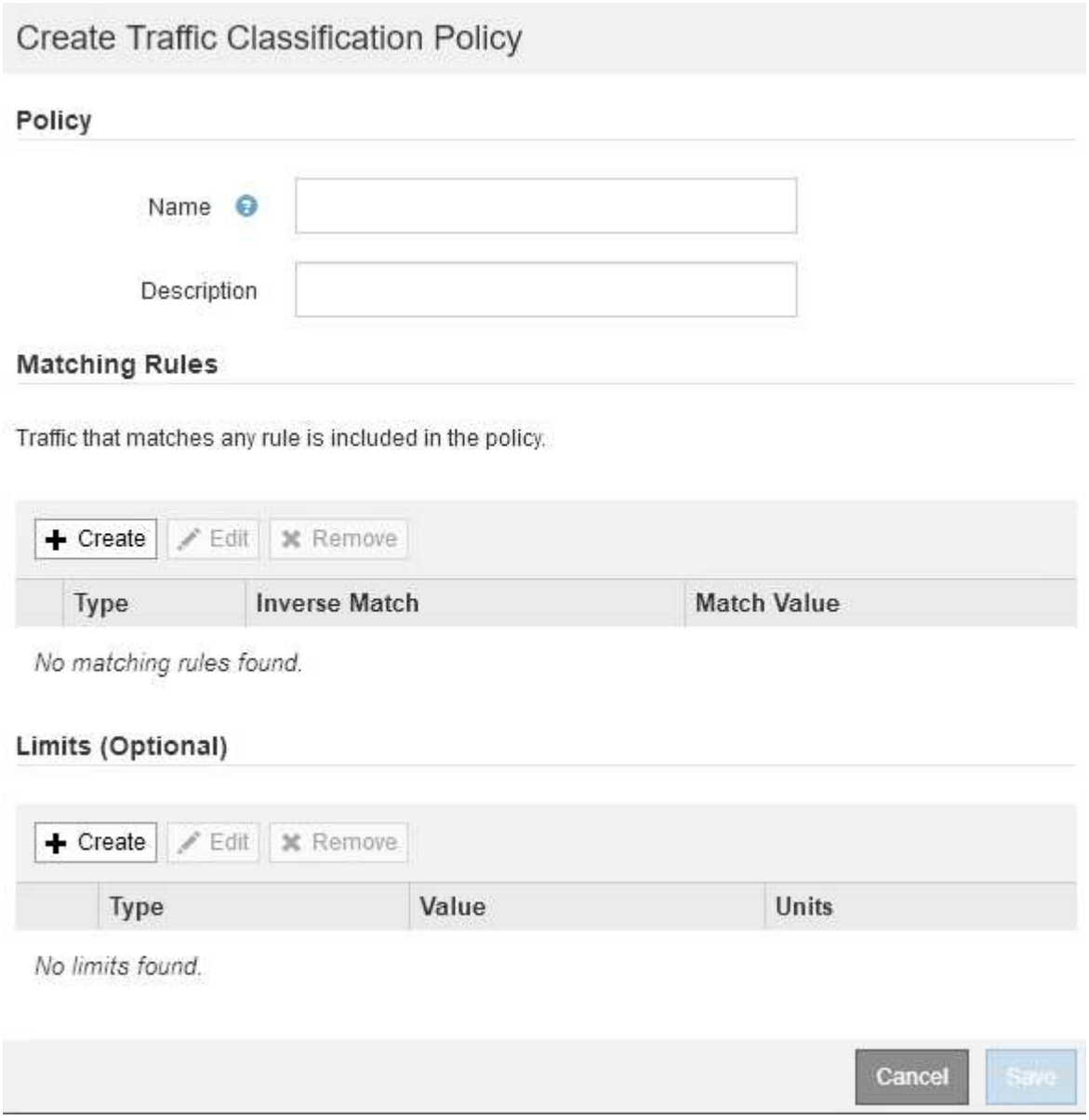
1. Seleccione **Configuración** > **Configuración de red** > **Clasificación de tráfico**.

   Aparece la página Directivas de clasificación del tráfico.



2. Haga clic en **Crear**.

   Aparece el cuadro de diálogo Crear directiva de clasificación de tráfico.



3. En el campo **Nombre**, escriba un nombre para la directiva.

   Introduzca un nombre descriptivo para poder reconocer la política.

4. Opcionalmente, agregue una descripción para la directiva en el campo **Descripción**.

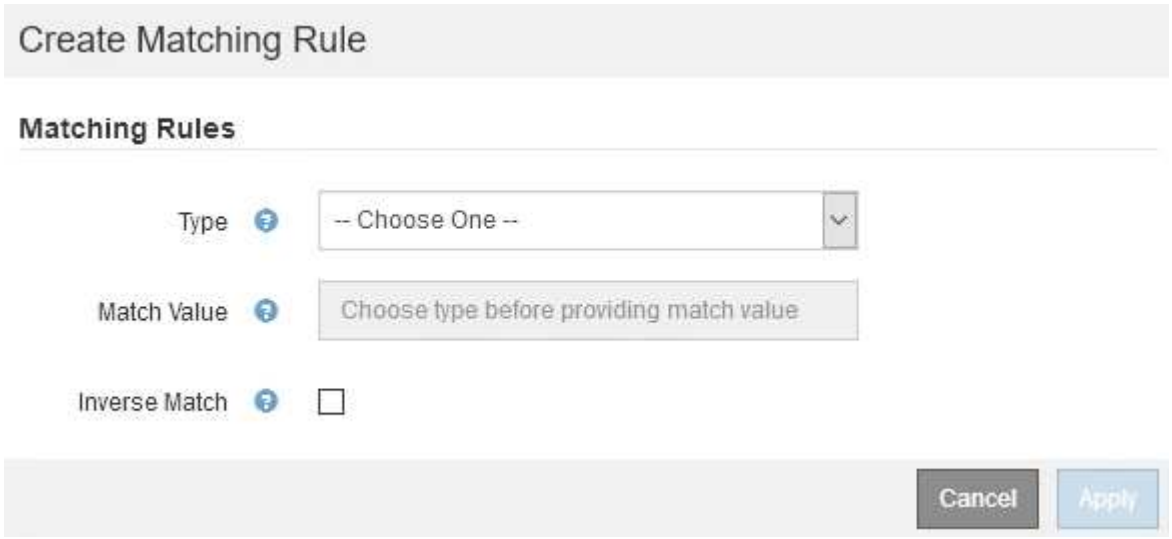
   Por ejemplo, describa a qué se aplica esta política de clasificación del tráfico y a qué se limitará.

5. Cree una o varias reglas coincidentes para la política.

   Las reglas coincidentes controlan qué entidades se verán afectadas por esta directiva de clasificación de tráfico. Por ejemplo, seleccione arrendatario si desea que esta directiva se aplique al tráfico de red de un arrendatario específico. O seleccione Endpoint si desea que esta directiva se aplique al tráfico de red en un extremo de equilibrio de carga específico.

   a. Haga clic en **Crear** en la sección **Reglas coincidentes**.

      Aparece el cuadro de diálogo Crear regla de coincidencia.



   b. En la lista desplegable **Tipo**, seleccione el tipo de entidad que se incluirá en la regla de coincidencia.
   c. En el campo **valor de coincidencia**, escriba un valor de coincidencia basado en el tipo de entidad elegido.
      - Bucket: Introduzca un nombre de bloque.
      - Bucket Regex: Introduzca una expresión regular que se utilizará para coincidir con un conjunto de nombres de bloques.

        La expresión regular no está anclada. Utilice el delimitador ^ para que coincida al principio del nombre del bloque y utilice el delimitador $ para que coincida al final del nombre.

      - CIDR: Introduzca una subred IPv4, en notación CIDR, que coincida con la subred deseada.
      - Extremo: Seleccione un extremo de la lista de extremos existentes. Estos son los puntos finales de equilibrador de carga definidos en la página de extremos de equilibrador de carga.
      - Inquilino: Seleccione un inquilino de la lista de arrendatarios existentes. La coincidencia de inquilinos se basa en la propiedad del bloque al que se va a acceder. El acceso anónimo a un bloque coincide con el inquilino al que pertenece el bloque.
   d. Si desea hacer coincidir todo el tráfico de red *excepto* que sea coherente con el valor Type and Match que acaba de definir, active la casilla de verificación **Inverse** . De lo contrario, deje la casilla de verificación sin seleccionar.

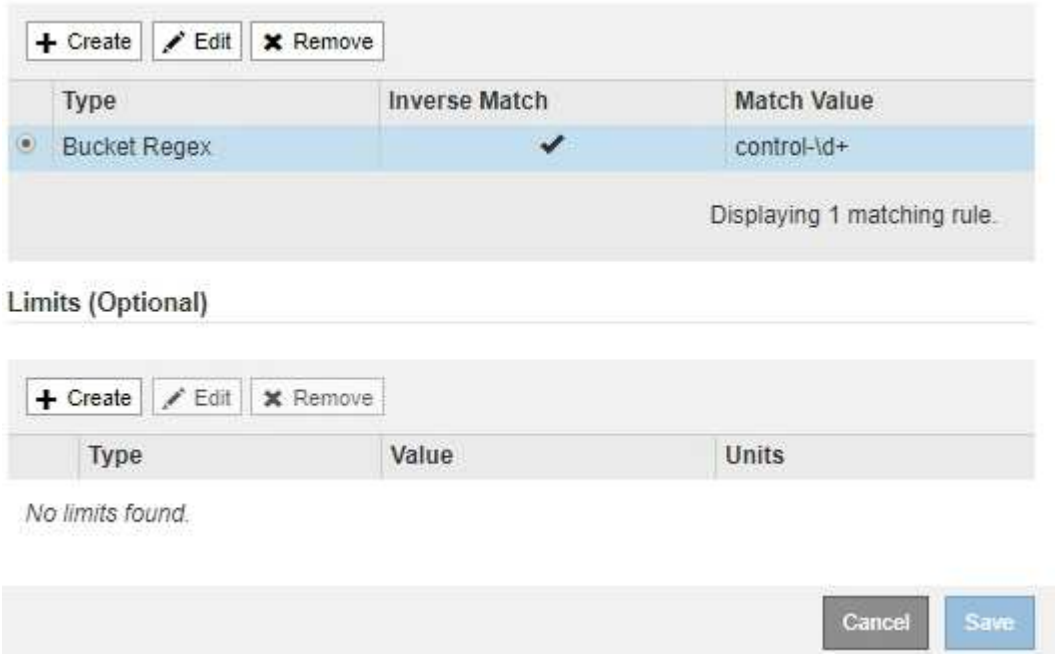
      Por ejemplo, si desea que esta directiva se aplique a todos los puntos finales del equilibrador de carga

excepto uno, especifique el punto final del equilibrador de carga que se excluirá y seleccione **Inverse**.

> Para una directiva que contiene varios matchers donde al menos uno es un matcher inverso, tenga cuidado de no crear una política que coincida con todas las solicitudes.

e. Haga clic en **aplicar**.

La regla se crea y se muestra en la tabla Reglas coincidentes.



a. Repita estos pasos para cada regla que desee crear para la política.

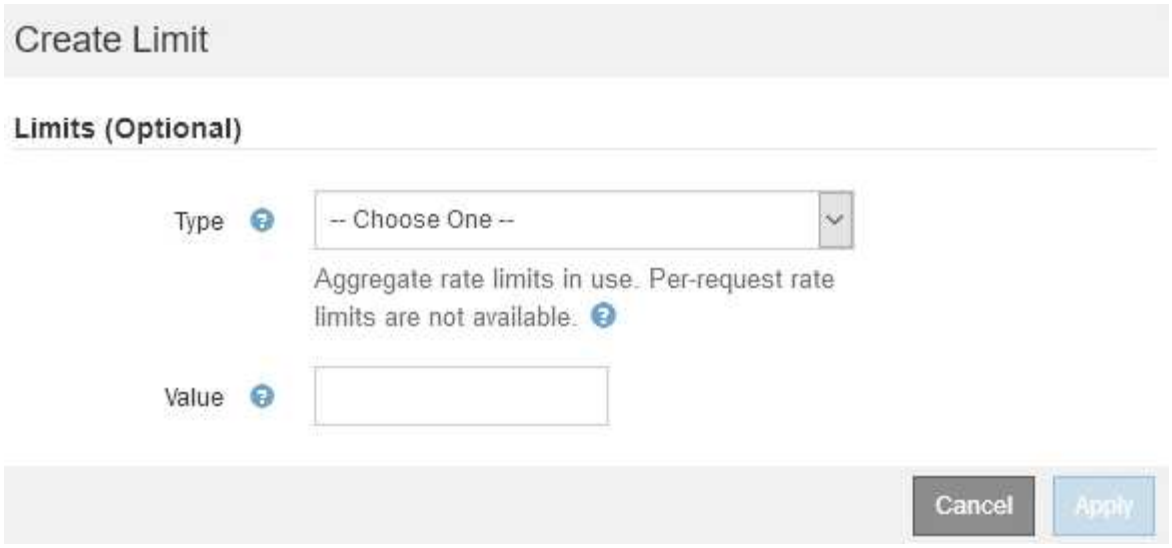
> El tráfico que coincide con cualquier regla se gestiona mediante la directiva.

6. De manera opcional, crear límites para la política.

> Aunque no cree límites, StorageGRID recopila métricas para poder supervisar el tráfico de red que se ajuste a la directiva.

a. Haga clic en **Crear** en la sección **límites**.

Se muestra el cuadro de diálogo Crear límite.



b. En el menú desplegable **Tipo**, seleccione el tipo de límite que desea aplicar a la directiva.

   En la siguiente lista, **in** hace referencia al tráfico de clientes S3 o Swift en el equilibrador de carga StorageGRID, y **OUT** hace referencia al tráfico desde el equilibrador de carga a clientes S3 o Swift.

   - Ancho de banda del agregado en
   - Ancho de banda del agregado agotado
   - Solicitudes de lectura simultáneas
   - Solicitudes de escritura simultáneas
   - Ancho de banda por solicitud en
   - Ancho de banda por solicitud agotado
   - Tasa de solicitud de lectura
   - Tasa de solicitudes de escritura

   > Puede crear políticas para limitar el ancho de banda agregado o para limitar el ancho de banda por solicitud. Sin embargo, StorageGRID no puede limitar ambos tipos de ancho de banda a la vez. Los límites de ancho de banda agregados pueden imponer un impacto adicional mínimo en el rendimiento en el tráfico no limitado.

   Para los límites de ancho de banda, StorageGRID aplica la política que mejor se adapte al tipo de conjunto de límites. Por ejemplo, si tiene una directiva que limita el tráfico en una sola dirección, entonces el tráfico en la dirección opuesta será ilimitado, aunque haya tráfico que coincida con las directivas adicionales que tengan límites de ancho de banda. StorageGRID implementa coincidencias «mejores» para límites de ancho de banda en el siguiente orden:

   - Dirección IP exacta (/máscara 32)
   - Nombre exacto del cucharón
   - Regex. Cucharón
   - Inquilino
   - Extremo
   - Coincidencias CIDR no exactas (no /32)

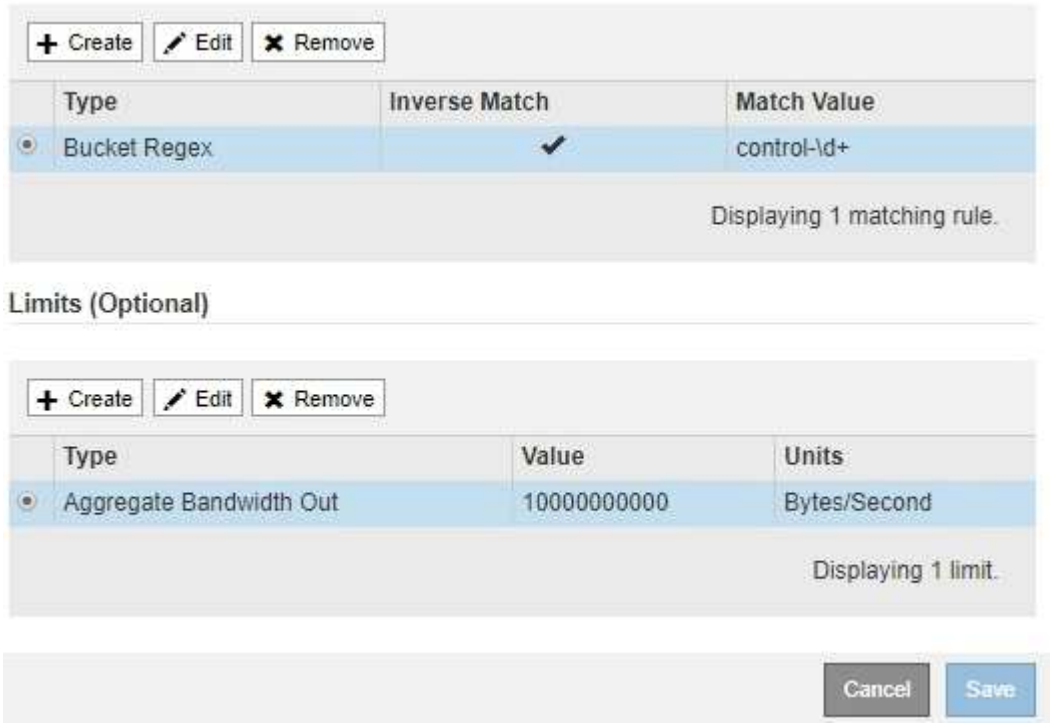
- Coincidencias inversas

c. En el campo **valor**, introduzca un valor numérico para el tipo de límite elegido.

   Las unidades esperadas se muestran cuando se selecciona un límite.

d. Haga clic en **aplicar**.

   El límite se crea y se muestra en la tabla límites.



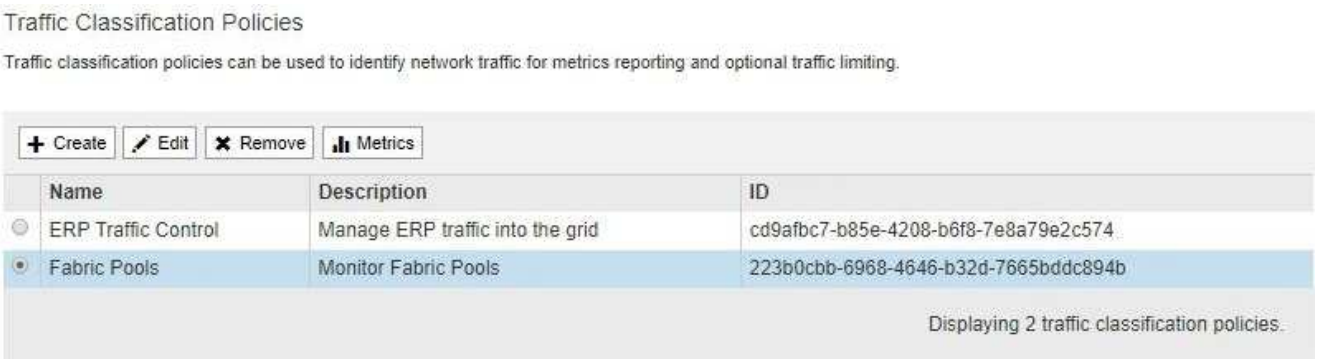
e. Repita estos pasos para cada límite que desee agregar a la directiva.

   Por ejemplo, si desea crear un límite de ancho de banda de 40 Gbps para un nivel de acuerdo de nivel de servicio, cree un límite de ancho de banda del agregado en el límite y un límite de ancho de banda de agregado en y establezca cada uno de entre 1 y 40 Gbps.

> Para convertir megabytes por segundo a gigabits por segundo, multiplique por ocho. Por ejemplo, 125 MB/s equivale a 1,000 Mbps o 1 Gbps.

7. Cuando termine de crear reglas y límites, haga clic en **Guardar**.

La directiva se guarda y se muestra en la tabla Directivas de clasificación del tráfico.



El tráfico del cliente S3 y Swift ahora se gestiona de acuerdo con las políticas de clasificación del tráfico. Puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera.

Información relacionada

"Gestión del equilibrio de carga"

"Ver las métricas de tráfico de red"

Edición de una directiva de clasificación de tráfico

Puede editar una directiva de clasificación de tráfico para cambiar su nombre o descripción, o para crear, editar o eliminar cualquier regla o límite para la directiva.

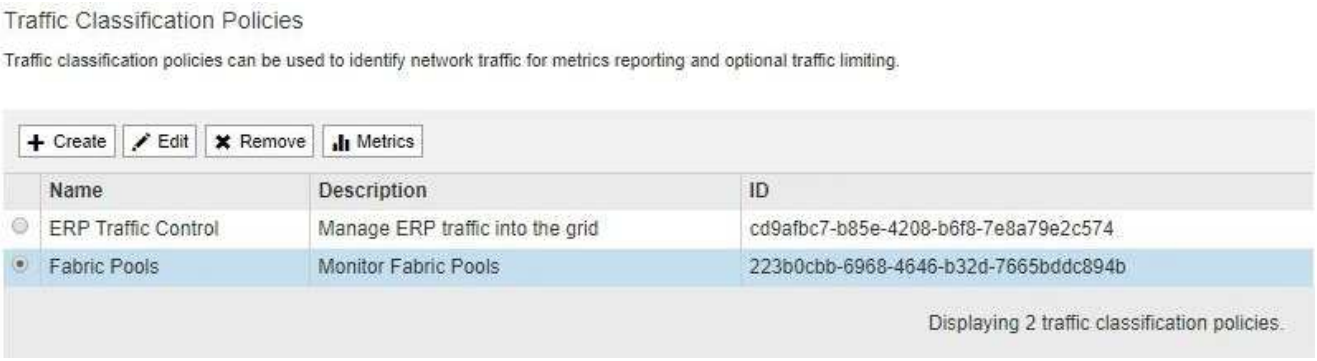
Lo que necesitará

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

Pasos

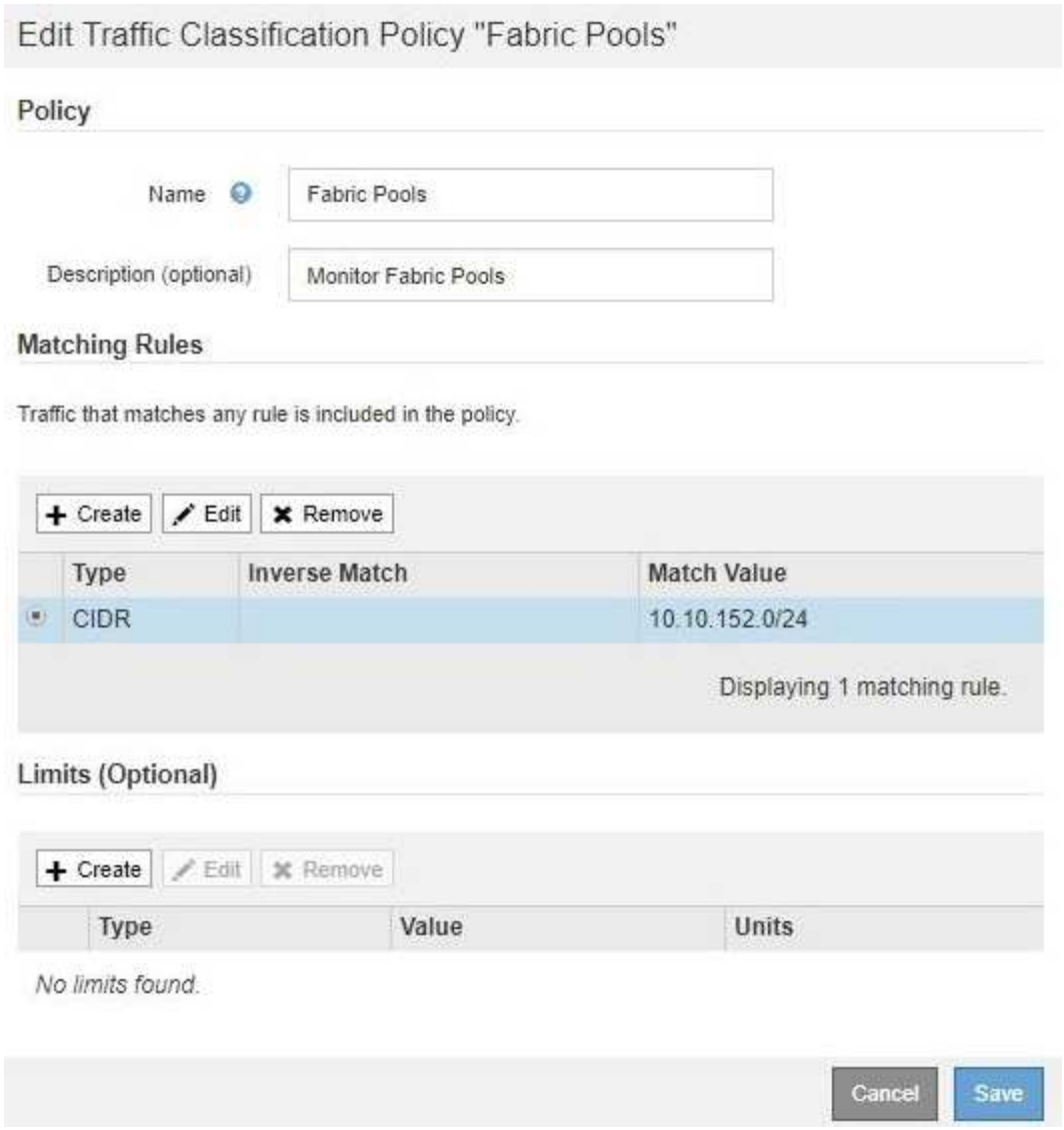
1. Seleccione **Configuración** > **Configuración de red** > **Clasificación de tráfico**.

   Aparece la página Directivas de clasificación del tráfico y las directivas existentes se muestran en la tabla.



2. Seleccione el botón de opción situado a la izquierda de la directiva que desea editar.
3. Haga clic en **Editar**.

   Aparece el cuadro de diálogo Editar directiva de clasificación del tráfico.



4. Cree, edite o elimine reglas y límites coincidentes según sea necesario.
   a. Para crear una regla o un límite coincidente, haga clic en **Crear** y siga las instrucciones para crear una regla o crear un límite.
   b. Para editar una regla o un límite coincidente, seleccione el botón de opción de la regla o límite, haga clic en **Editar** en la sección **Reglas coincidentes** o en la sección **límites** y siga las instrucciones para crear una regla o crear un límite.
   c. Para eliminar una regla o un límite coincidente, seleccione el botón de opción de la regla o límite y haga clic en **Quitar**. A continuación, haga clic en **Aceptar** para confirmar que desea eliminar la regla o el límite.
5. Cuando haya terminado de crear o editar una regla o un límite, haga clic en **aplicar**.
6. Cuando termine de editar la directiva, haga clic en **Guardar**.

   Los cambios realizados en la directiva se guardan y el tráfico de red se gestiona de acuerdo con las directivas de clasificación del tráfico. Puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera.

Eliminación de una directiva de clasificación de tráfico

Si ya no necesita una directiva de clasificación del tráfico, puede eliminarla.

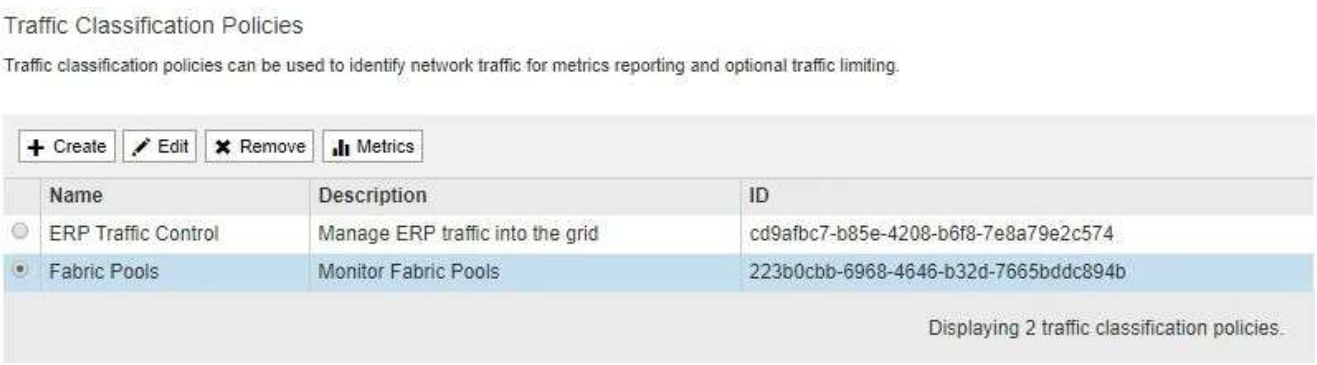
Lo que necesitará

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

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **Clasificación de tráfico**.

   Aparece la página Directivas de clasificación del tráfico y las directivas existentes se muestran en la tabla.



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

   Aparecerá un cuadro de diálogo Advertencia.

4. Haga clic en **Aceptar** para confirmar que desea eliminar la directiva.

   La directiva se elimina.

Ver las métricas de tráfico de red

Puede supervisar el tráfico de red mediante la visualización de los gráficos disponibles en la página Directivas de clasificación del tráfico.

Lo que necesitará

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

Acerca de esta tarea

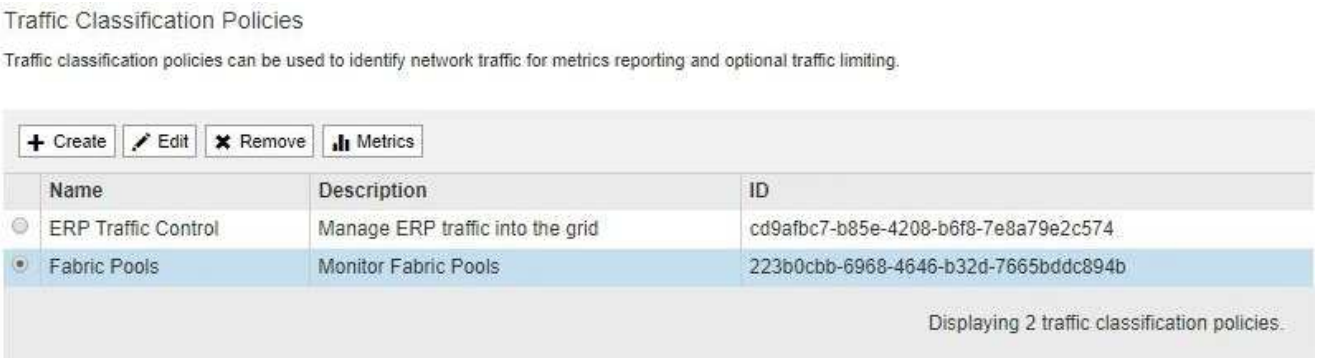
Para cualquier directiva de clasificación de tráfico existente, puede ver las métricas del servicio Load Balancer para determinar si la directiva limita correctamente el tráfico en toda la red. Los datos de los gráficos pueden ayudarle a determinar si es necesario ajustar la política.

Incluso si no se establecen límites para una política de clasificación del tráfico, se recopilan las métricas y los gráficos proporcionan información útil para comprender las tendencias del tráfico.

Pasos

1. Seleccione **Configuración** > **Configuración de red** > **Clasificación de tráfico**.

   Aparece la página Directivas de clasificación del tráfico y las directivas existentes se muestran en la tabla.



2. Seleccione el botón de opción situado a la izquierda de la política para la que desea ver las métricas.
3. Haga clic en **métricas**.

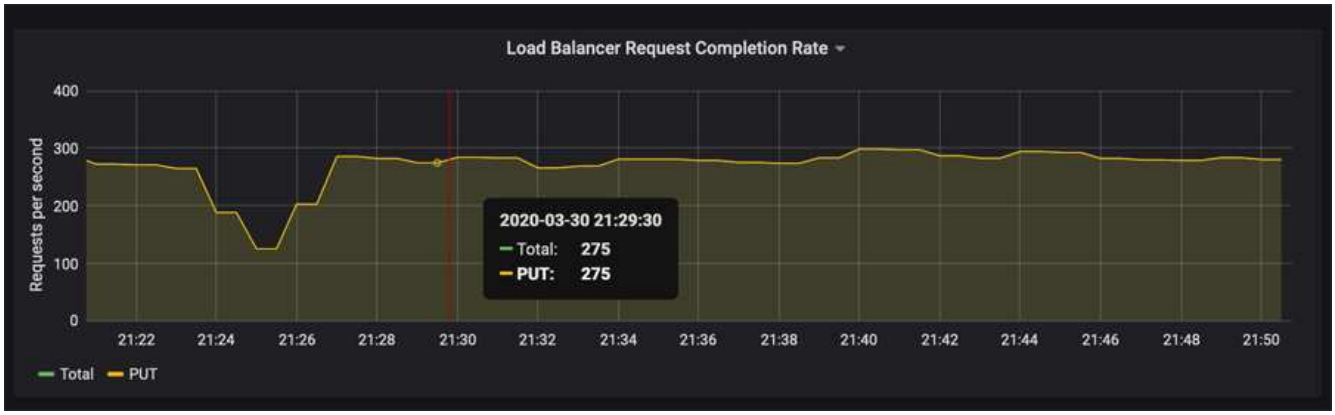
   Se abrirá una nueva ventana del explorador y aparecerán los gráficos de la directiva de clasificación del tráfico. Los gráficos muestran métricas solo para el tráfico que coincide con la directiva seleccionada.

   Puede seleccionar otras directivas para visualizarlas mediante el menú desplegable **Policy**.

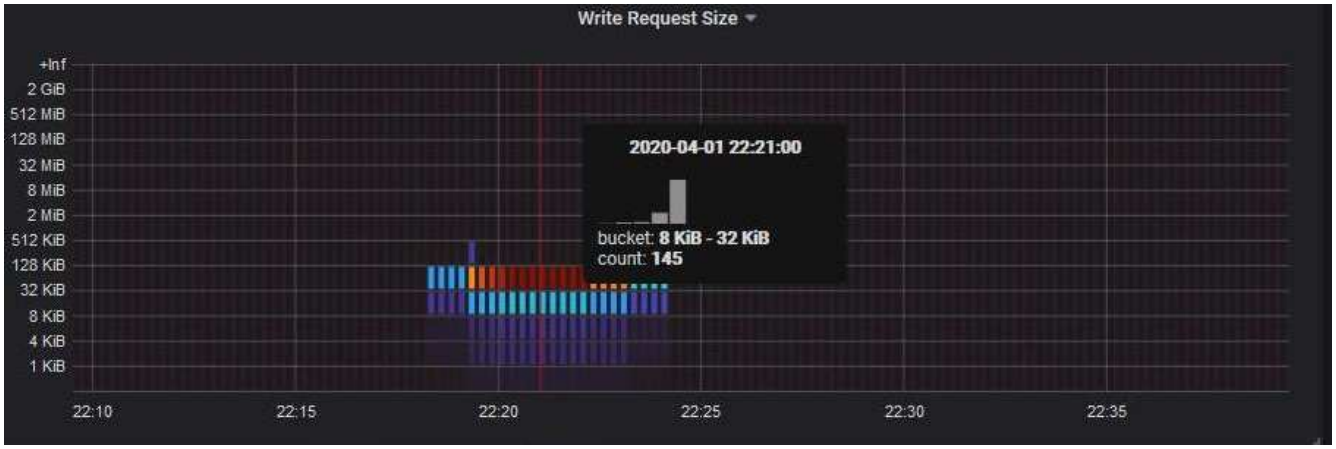
Los siguientes gráficos están incluidos en la página web.

- Tráfico de solicitud del equilibrador de carga: Este gráfico proporciona una media móvil de 3 minutos del rendimiento de los datos transmitidos entre los extremos del equilibrador de carga y los clientes que realizan las solicitudes, en bits por segundo.
- Tasa de finalización de solicitudes de equilibrador de carga: Este gráfico proporciona una media de movimiento de 3 minutos del número de solicitudes completadas por segundo, desglosadas por tipo de solicitud (GET, PUT, HEAD y DELETE). Este valor se actualiza cuando se han validado los encabezados de una nueva solicitud.
- Tasa de respuesta de error: Este gráfico proporciona un promedio móvil de 3 minutos del número de respuestas de error devueltas a clientes por segundo, desglosado por el código de respuesta de error.
- Duración media de la solicitud (sin error): Este gráfico proporciona una media móvil de 3 minutos de duración de la solicitud, desglosada por tipo de solicitud (GET, PUT, HEAD y DELETE). Cada duración de la solicitud comienza cuando el servicio Load Balancer analiza una cabecera de solicitud y finaliza cuando se devuelve el cuerpo de respuesta completo al cliente.
- Tasa de solicitud de escritura por tamaño de objeto: Este mapa térmico proporciona una media móvil de 3 minutos de la velocidad a la que se completan las solicitudes de escritura en función del tamaño del objeto. En este contexto, las solicitudes de escritura se refieren sólo a SOLICITUDES PUT.
- Tasa de solicitud de lectura por tamaño de objeto: Este mapa térmico proporciona una media móvil de 3 minutos de la velocidad a la que se completan las solicitudes de lectura en función del tamaño del objeto. En este contexto, las solicitudes de lectura se refieren sólo a OBTENER solicitudes. Los colores del mapa térmico indican la frecuencia relativa de un tamaño de objeto dentro de un gráfico individual. Los colores más frescos (por ejemplo, púrpura y azul) indican tasas relativas más bajas, y los colores más cálidos (por ejemplo, naranja y rojo) indican tasas relativas más altas.

4. Pase el cursor por un gráfico de líneas para ver una ventana emergente de valores en una parte específica del gráfico.



5. Pase el cursor por encima de un mapa térmico para ver una ventana emergente que muestra la fecha y hora de la muestra, los tamaños de objeto agregados al recuento y el número de solicitudes por segundo durante ese período de tiempo.



6. Utilice el menú desplegable **Política** de la parte superior izquierda para seleccionar una directiva diferente.

   Se muestran los gráficos de la política seleccionada.

7. También puede acceder a los gráficos desde el menú **Soporte**.
   a. Seleccione **Soporte** > **Herramientas** > **parámetros**.
   b. En la sección **Grafana** de la página, seleccione **Directiva de clasificación de tráfico**.
   c. Seleccione la política del menú desplegable que hay en la esquina superior izquierda de la página.

      Las directivas de clasificación del tráfico se identifican por su ID. Los ID de directiva se muestran en la página Directivas de clasificación de tráfico.

8. Analice los gráficos para determinar con qué frecuencia la política limita el tráfico y si necesita ajustar la política.

Información relacionada

"Solución de problemas de monitor"

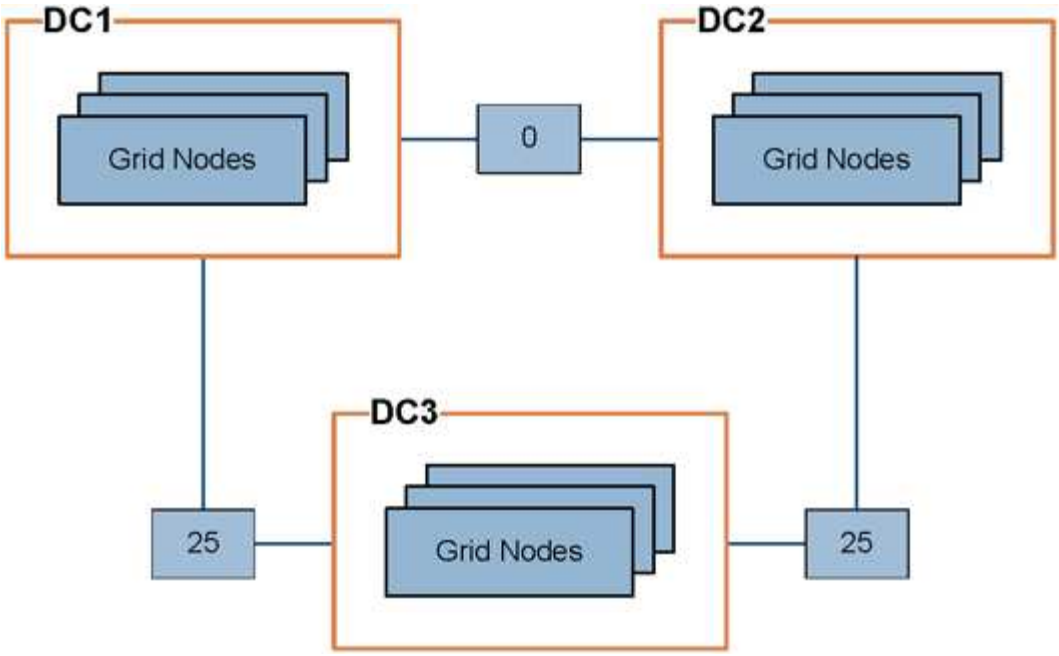
¿Cuáles son los costes de enlace

Los costes de enlace le permiten priorizar qué sitio de centro de datos proporciona un servicio solicitado cuando existen dos o más centros de datos. Puede ajustar los costes de vínculo para reflejar la latencia entre los sitios.

- Los costes de enlace se utilizan para priorizar qué copia de objetos se utiliza para llevar a cabo las recuperaciones de objetos.
- Los costes de enlace los utiliza la API de gestión de grid y la API de gestión de inquilinos para determinar qué servicios StorageGRID internos utilizar.
- Los costes de enlace los utiliza el servicio CLB en los nodos de puerta de enlace para dirigir las conexiones del cliente.

  El servicio CLB está obsoleto.

El diagrama muestra una cuadrícula de tres sitios con costes de enlace configurados entre sitios:



- El servicio CLB de los nodos Gateway distribuye igualmente las conexiones de cliente a todos los nodos de almacenamiento del mismo sitio del centro de datos y a cualquier sitio del centro de datos con un coste de enlace de 0.

  En el ejemplo, un nodo de puerta de enlace en el sitio del centro de datos 1 (DC1) distribuye igualmente conexiones de cliente a nodos de almacenamiento en DC1 y a nodos de almacenamiento en DC2. Un nodo de puerta de enlace en DC3 envía conexiones de cliente sólo a los nodos de almacenamiento en DC3.

- Al recuperar un objeto que existe como varias copias replicadas, StorageGRID recupera la copia en el centro de datos que tiene el coste de enlace más bajo.

  En el ejemplo, si una aplicación cliente en DC2 recupera un objeto almacenado en DC1 y DC3, el objeto se recupera de DC1, ya que el coste del vínculo de DC1 a D2 es 0, que es inferior al coste del vínculo de DC3 a DC2 (25).

Los costes de enlace son números relativos arbitrarios sin unidad de medida específica. Por ejemplo, un costo de enlace de 50 se utiliza de forma menos preferente que un costo de enlace de 25. En la tabla se muestran los costes de los enlaces más utilizados.

Enlace	Coste del enlace	Notas
Entre sitios físicos del centro de datos	25 (predeterminado)	Centros de datos conectados por un enlace WAN.
Entre las ubicaciones lógicas del centro de datos en la misma ubicación física	0	Centros de datos lógicos en el mismo edificio físico o campus conectados por una LAN.

Información relacionada

"Cómo funciona el equilibrio de carga: Servicio CLB"

Actualizando costes de enlace

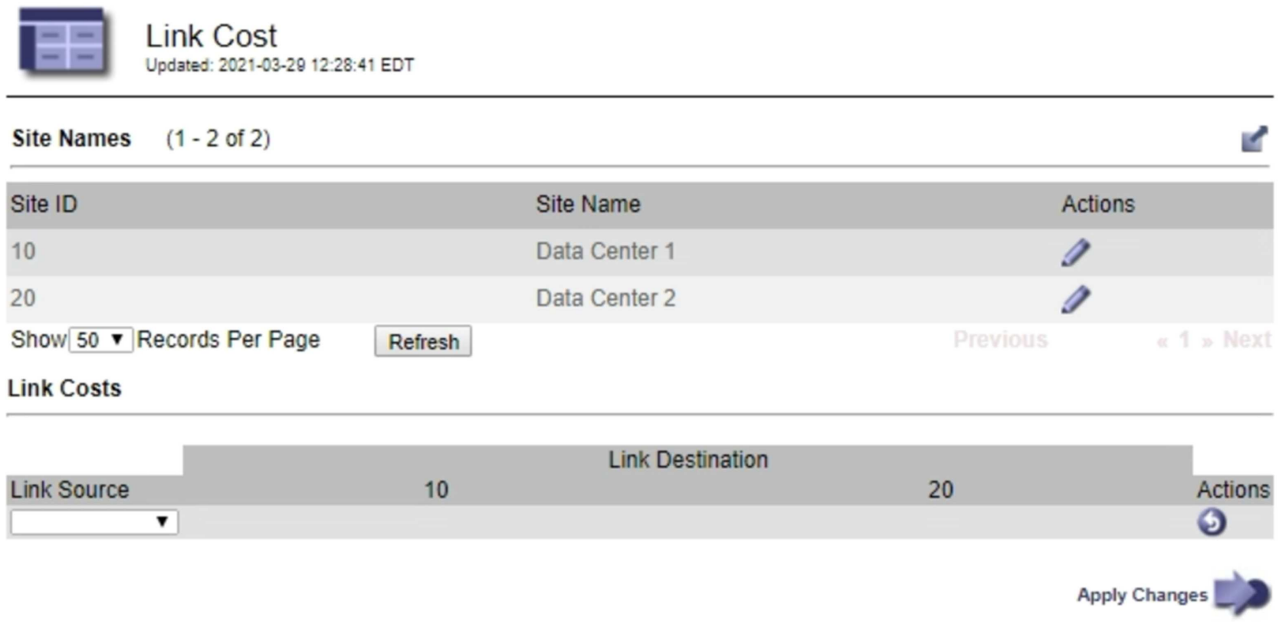
Puede actualizar los costes de enlace entre los sitios de centros de datos para reflejar la latencia entre los sitios.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso Grid Topology Page Configuration.

Pasos

1. Seleccione **Configuración** > **Ajustes de red** > **coste de enlace**.



2. Seleccione un sitio en **origen de enlace** e introduzca un valor de coste entre 0 y 100 en **destino de enlace**.

   No se puede cambiar el coste del vínculo si el origen es el mismo que el destino.

   Para cancelar los cambios, haga clic en **Revert**.

3. Haga clic en **aplicar cambios**.