Administre StorageGRID

StorageGRID software

NetApp
January 14, 2026

Tabla de contenidos

Administre StorageGRID

Administre StorageGRID

Siga estas instrucciones para configurar y administrar un sistema StorageGRID.

Acerca de estas instrucciones

Las tareas principales para configurar y administrar StorageGRID le permiten:

- Utilice Grid Manager para configurar grupos y usuarios
- Cree cuentas de arrendatario para permitir que las aplicaciones cliente S3 almacenen y recuperen objetos
- Configurar y gestionar redes StorageGRID
- Configure AutoSupport
- Gestione la configuración del nodo

Antes de empezar

- Tiene una visión general del sistema StorageGRID.
- Tiene un conocimiento muy detallado de los shell de comandos de Linux, las conexiones de red y la instalación y configuración del hardware de servidor.

Comience a usar Grid Manager

Requisitos del navegador web

Debe utilizar un navegador web compatible.

Navegador Web	Versión mínima admitida
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Establezca la ventana del navegador en un ancho recomendado.

Ancho del navegador	Píxeles
Mínimo	1024
Óptimo	1280

Inicie sesión en Grid Manager

Para acceder a la página de inicio de sesión de Grid Manager, introduzca el nombre de dominio completo (FQDN) o la dirección IP de un nodo de administración en la barra de direcciones de un explorador web compatible.

Cada sistema StorageGRID incluye un nodo de administrador primario y cualquier número de nodos de administrador que no son primarios. Puede iniciar sesión en Grid Manager en cualquier nodo de administrador para gestionar el sistema StorageGRID. Sin embargo, algunos procedimientos de mantenimiento sólo se pueden realizar desde el nodo de administración principal.

Conéctese a un grupo de alta disponibilidad

Si se incluyen nodos de administración en un grupo de alta disponibilidad (ha), puede conectarse mediante la dirección IP virtual del grupo de alta disponibilidad o un nombre de dominio completo que asigne la dirección IP virtual. El nodo de administración principal se debe seleccionar como la interfaz principal del grupo, de modo que al acceder a Grid Manager, se tiene acceso en el nodo de administración principal a menos que el nodo de administración principal no esté disponible. Consulte "Gestión de grupos de alta disponibilidad".

Utilice SSO

Los pasos para iniciar sesión son ligeramente diferentes si"Se ha configurado el inicio de sesión único (SSO)" .

Inicie sesión en Grid Manager en el primer nodo de administración

Antes de empezar

- Tiene sus credenciales de inicio de sesión.
- Está utilizando una "navegador web compatible".
- Las cookies están habilitadas en su navegador web.
- Pertenece a un grupo de usuarios que tiene al menos un permiso.
- Tiene la dirección URL de Grid Manager:

  `https://FQDN_or_Admin_Node_IP/`

  Puede usar el nombre de dominio completo, la dirección IP de un nodo de administración o la dirección IP virtual de un grupo de alta disponibilidad de nodos de administración.

  Para acceder a Grid Manager en un puerto que no sea el puerto predeterminado para HTTPS (443), incluya el número de puerto en la dirección URL:

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO no está disponible en el puerto restringido de Grid Manager. Se debe usar el puerto 443.

Pasos

1. Inicie un explorador web compatible.
2. En la barra de direcciones del navegador, introduzca la dirección URL de Grid Manager.

3. Si se le solicita una alerta de seguridad, instale el certificado con el asistente de instalación del explorador. Consulte "Gestionar certificados de seguridad".
4. Inicie sesión en Grid Manager.

   La pantalla de inicio de sesión que aparece depende de si se ha configurado el inicio de sesión único (SSO) para StorageGRID.

   No se utiliza SSO

   a. Introduzca su nombre de usuario y contraseña para el administrador de grid.
   b. Seleccione **Iniciar sesión**.

   Uso de SSO

   - Si StorageGRID utiliza SSO y esta es la primera vez que accede a la URL en este explorador:
     i. Seleccione **Iniciar sesión**. Puede dejar el 0 en el campo Cuenta.
     ii. Ingrese sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

     Por ejemplo, si StorageGRID usa SSO y usted ha accedido previamente al Administrador de Grid o a una cuenta de inquilino:

     A. Introduzca **0** (el ID de cuenta de Grid Manager) o seleccione **Grid Manager** si aparece en la lista de cuentas recientes.
     B. Seleccione **Iniciar sesión**.
     C. Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

Al iniciar sesión, aparece la página inicial de Grid Manager, que incluye el panel de control. Para saber qué información se proporciona, consulte "Permite ver y gestionar el panel de control".

Conéctese a otro nodo de administración

Siga estos pasos para iniciar sesión en otro nodo de administración.

No se utiliza SSO

Pasos

1. En la barra de direcciones del navegador, introduzca el nombre de dominio completo o la dirección IP del otro nodo de administración. Incluya el número de puerto según sea necesario.
2. Introduzca su nombre de usuario y contraseña para el administrador de grid.
3. Seleccione **Iniciar sesión**.

Uso de SSO

Si StorageGRID está utilizando SSO y ha iniciado sesión en un nodo de administración, puede acceder a otros nodos de administración sin tener que volver a iniciar sesión.

Pasos

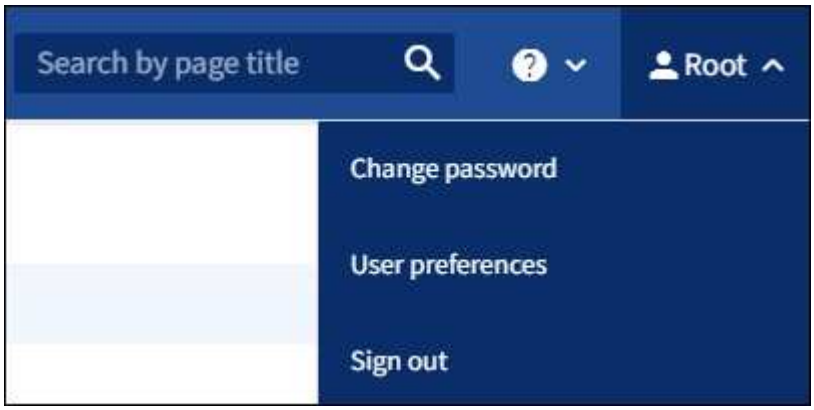
1. Introduzca el nombre de dominio completo o la dirección IP del otro nodo de administración en la barra de direcciones del navegador.
2. Si su sesión de SSO ha caducado, vuelva a introducir sus credenciales.

Cierre la sesión en Grid Manager

Cuando haya terminado de trabajar con Grid Manager, debe cerrar sesión para asegurarse de que los usuarios no autorizados no puedan acceder al sistema StorageGRID. Es posible que cerrar el navegador no le cierre la sesión del sistema según la configuración de cookies del navegador.

Pasos

1. Seleccione su nombre de usuario en la esquina superior derecha.



2. Selecciona **Cerrar sesión**.

Opción	Descripción
SSO no en uso	Ha cerrado sesión en el nodo de administrador. Se muestra la página de inicio de sesión de Grid Manager. **Nota:** Si ha iniciado sesión en más de un nodo de administración, debe cerrar sesión en cada nodo.

Opción	Descripción
SSO activado	Inició sesión en todos los nodos de administrador a los que accedían. Aparece la página de inicio de sesión de StorageGRID. **Grid Manager** aparece como el valor predeterminado en la lista desplegable **Cuentas recientes**, y el campo **ID de cuenta** muestra 0. **Nota:** Si SSO está habilitado y también ha iniciado sesión en el Administrador de inquilinos, también debe"cierre la sesión de la cuenta de inquilino" a"Cierre la sesión de SSO" .

Cambie la contraseña

Si es un usuario local de Grid Manager, puede cambiar su propia contraseña.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".

Acerca de esta tarea

Si inicia sesión en StorageGRID como usuario federado o si está habilitado el inicio de sesión único (SSO), no podrá cambiar la contraseña en Grid Manager. En su lugar, debe cambiar la contraseña en el origen de identidad externo, por ejemplo, Active Directory u OpenLDAP.

Pasos

1. En el encabezado de Grid Manager, seleccione ***su nombre*** > **Cambiar contraseña**.
2. Introduzca su contraseña actual.
3. Escriba una nueva contraseña.

   La contraseña debe contener al menos 8 caracteres y no más de 32. Las contraseñas distinguen mayúsculas de minúsculas.

4. Vuelva a introducir la nueva contraseña.
5. Seleccione **Guardar**.

Consulte la información de licencia de StorageGRID

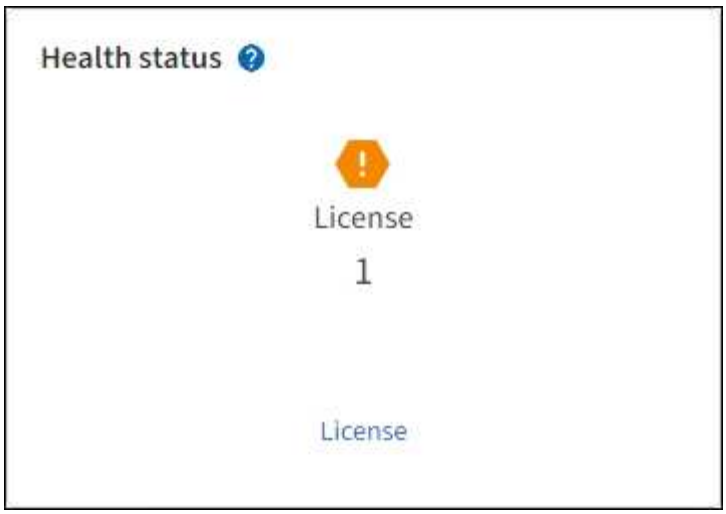
Puede ver la información de licencia del sistema StorageGRID, como la capacidad de almacenamiento máxima de su grid, cuando sea necesario.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".

Acerca de esta tarea

Si hay un problema con la licencia de software para este sistema StorageGRID, la tarjeta de estado del panel incluye un icono de estado de licencia y un enlace de **Licencia**. El número indica el número de problemas relacionados con la licencia.



Pasos

1. Para acceder a la página Licencia, realice una de las siguientes acciones:
   - Seleccione **Mantenimiento** > **Sistema** > **Licencia**.
   - En la tarjeta de estado de salud del panel de control, seleccione el icono de estado de la licencia o el enlace **Licencia**.

     Este vínculo sólo aparece si hay un problema con la licencia.

2. Vea los detalles de sólo lectura de la licencia actual:
   - ID del sistema de StorageGRID, que es el número de identificación exclusivo para esta instalación de StorageGRID
   - Número de serie de la licencia
   - Tipo de licencia, ya sea **Perpetual** o **Suscripción**
   - Capacidad de almacenamiento bajo licencia del grid
   - Capacidad de almacenamiento admitida
   - Fecha de finalización de la licencia. **N/A** aparece para una licencia perpetua.
   - Fecha de finalización del soporte

     Esta fecha se lee del archivo de licencia actual y puede estar obsoleta si se amplió o renovó el contrato de servicio de soporte después de obtener el archivo de licencia. Para actualizar este valor, consulte "Actualice la información de licencia de StorageGRID". También puede consultar la fecha de finalización real del contrato mediante Active IQ.

   - Contenido del archivo de texto de licencia

Actualice la información de licencia de StorageGRID

Debe actualizar la información de licencia del sistema de StorageGRID en cualquier momento que cambien las condiciones de su licencia. Por ejemplo, debe actualizar la información de la licencia si adquiere capacidad de almacenamiento adicional para su grid.

Antes de empezar

- Tiene un nuevo archivo de licencia que se aplicará al sistema StorageGRID.
- Tienes "permisos de acceso específicos".
- Tiene la clave de acceso de aprovisionamiento.

Pasos

1. Seleccione **Mantenimiento** > **Sistema** > **Licencia**.
2. En la sección Actualizar licencia, seleccione **Examinar**.
3. Busque y seleccione el nuevo archivo de licencia (`.txt`).

   El nuevo archivo de licencia se valida y muestra.

4. Introduzca la clave de acceso de aprovisionamiento.
5. Seleccione **Guardar**.

Utilice la API

Utilice la API de gestión de grid

Puede realizar tareas de administración del sistema mediante la API REST de Grid Management en lugar de la interfaz de usuario de Grid Manager. Por ejemplo, se recomienda utilizar la API para automatizar operaciones o crear varias entidades, como los usuarios, más rápidamente.

Recursos de alto nivel

La API de gestión de grid proporciona los siguientes recursos de nivel superior:

- `/grid`: El acceso está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados.
- `/org`: El acceso está restringido a los usuarios que pertenecen a un grupo LDAP local o federado para una cuenta de inquilino. Para obtener más información, consulte "Usar una cuenta de inquilino".
- `/private`: El acceso está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados. Las API privadas están sujetas a cambios sin previo aviso. Los extremos privados de StorageGRID también ignoran la versión de API de la solicitud.

Emita solicitudes API

La API de gestión de grid utiliza la plataforma API de código abierto de Swagger. Swagger proporciona una interfaz de usuario intuitiva que permite a los desarrolladores y no desarrolladores realizar operaciones en tiempo real en StorageGRID con la API.

La interfaz de usuario de Swagger proporciona detalles y documentación completos para cada operación de API.

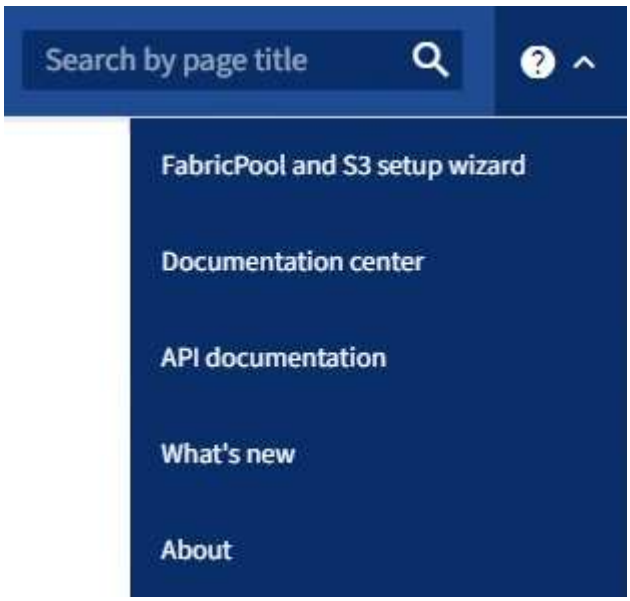
Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "permisos de acceso específicos".

Cualquier operación de API que realice mediante la página web de Documentación de API es operaciones en directo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

Pasos

1. En el encabezado de Grid Manager, selecciona el icono de ayuda y selecciona **Documentación de API**.



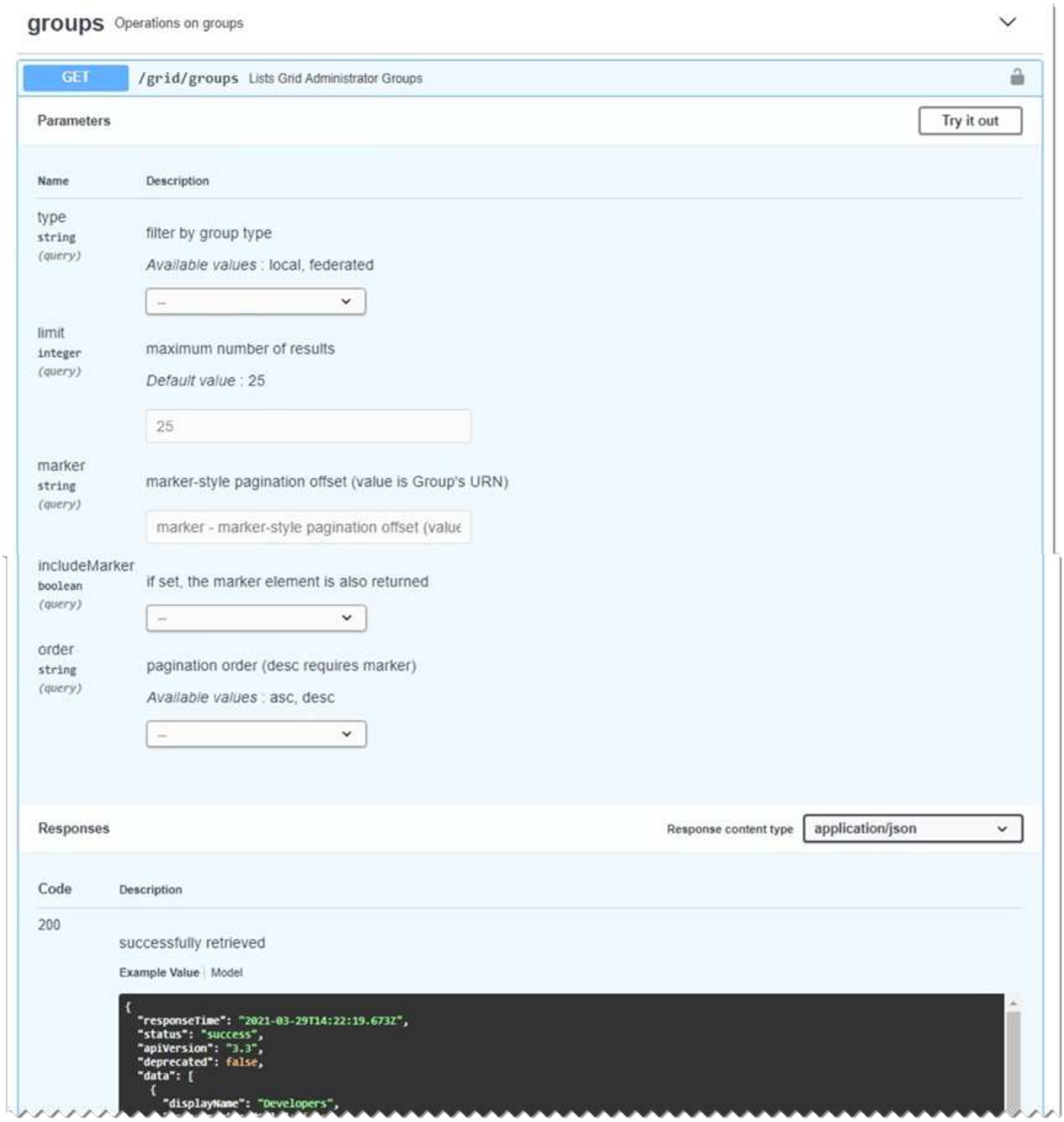
2. Para realizar una operación con la API privada, seleccione **Ir a documentación de API privada** en la página API de administración de StorageGRID.

   Las API privadas están sujetas a cambios sin previo aviso. Los extremos privados de StorageGRID también ignoran la versión de API de la solicitud.

3. Seleccione la operación deseada.

   Al expandir una operación de API, puede ver las acciones HTTP disponibles, como GET, PUT, UPDATE y DELETE.

4. Seleccione una acción HTTP para ver los detalles de la solicitud, incluida la dirección URL del extremo, una lista de los parámetros necesarios o opcionales, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.



5. Determine si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. A continuación, obtenga estos valores. Es posible que primero deba emitir una solicitud de API diferente para obtener la información que necesita.
6. Determine si necesita modificar el cuerpo de solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.
7. Seleccione **probar**.
8. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.
9. Seleccione **Ejecutar**.
10. Revise el código de respuesta para determinar si la solicitud se ha realizado correctamente.

Operaciones de API de gestión de grid

La API de gestión de grid organiza las operaciones disponibles en las siguientes secciones.

> Esta lista solo incluye las operaciones disponibles en la API pública.

- **CUENTAS**: Operaciones para administrar cuentas de inquilinos de almacenamiento, incluyendo la creación de nuevas cuentas y la recuperación del uso de almacenamiento para una cuenta dada.
- **ALERT-HISTORY**: Operaciones en alertas resueltas.
- **RECEPTORES DE ALERTA**: Operaciones en receptores de notificación de alerta (correo electrónico).
- **ALERT-RULES**: Operaciones en reglas de alerta.
- **ALERT-SILENCES**: Operaciones en silencios de alerta.
- **ALERTAS**: Operaciones en alertas.
- **AUDIT**: Operaciones para listar y actualizar la configuración de auditoría.
- **AUTH**: Operaciones para realizar la autenticación de sesión de usuario.

  La API de administración de grid admite el esquema de autenticación de token de Bearer. Para iniciar sesión, proporcione un nombre de usuario y una contraseña en el cuerpo JSON de la solicitud de autenticación (es decir, `POST /api/v3/authorize`). Si el usuario se autentica correctamente, se devuelve un token de seguridad. Este token se debe proporcionar en el encabezado de las siguientes solicitudes de API ("autorización: Portador *token*"). El token caduca después de 16 horas.

  > Si el inicio de sesión único está habilitado para el sistema StorageGRID, debe realizar pasos diferentes para la autenticación. Consulte Autenticación en la API si el inicio de sesión único está activado.

  Consulte Protección contra errores de solicitudes entre sitios para obtener información sobre cómo mejorar la seguridad de la autenticación.

- **CERTIFICADOS DE CLIENTE**: Operaciones para configurar certificados de cliente de modo que se pueda acceder a StorageGRID de forma segura utilizando herramientas de monitoreo externas.
- **Config**: Operaciones relacionadas con el lanzamiento del producto y versiones de la API de administración de grid. Es posible mostrar la versión del producto y las versiones principales de la API de Grid Management compatibles con esta versión, así como deshabilitar las versiones obsoletas de la API.
- **Funciones desactivadas**: Operaciones para ver características que podrían haber sido desactivadas.
- **Servidores dns**: Operaciones para listar y cambiar servidores DNS externos configurados.
- **Drive-details**: Operaciones en unidades para modelos específicos de dispositivos de almacenamiento.
- **Endpoint-domain-names**: Operaciones para listar y cambiar los nombres de dominio de punto final S3.
- **Código de borrado**: Operaciones en perfiles de codificación de borrado.
- **EXPANSIÓN**: Operaciones de expansión (nivel de procedimiento).
- **EXPANSION-NODES**: Operaciones en expansión (nivel de nodo).
- **Sitios de expansión**: Operaciones en expansión (nivel de sitio).
- **Grid-networks**: Operaciones para listar y cambiar la Lista de Red de Grid.
- **Grid-passwords**: Operaciones para la gestión de contraseñas de grid.

- **GRUPOS**: Operaciones para administrar grupos de administradores de grid locales y para recuperar grupos de administradores de grid federados desde un servidor LDAP externo.
- **Identity-source**: Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información federada del grupo y del usuario.
- **ilm**: Operaciones de gestión del ciclo de vida de la información (ILM).
- **Procedimientos en curso**: Recupera los procedimientos de mantenimiento que están actualmente en curso.
- **LICENCIA**: Operaciones para recuperar y actualizar la licencia de StorageGRID.
- **Logs**: Operaciones para recopilar y descargar archivos de registro.v
- **Métricas**: Operaciones en métricas StorageGRID, incluidas consultas métricas instantáneas en un único punto en el tiempo y consultas métricas de rango durante un intervalo de tiempo. La API de gestión de grid utiliza la herramienta de supervisión de sistemas Prometheus como origen de datos de back-end. Para obtener información sobre la construcción de consultas Prometheus, consulte el sitio web Prometheus.

> Las métricas que se incluyen `private` en sus nombres están destinadas solo para uso interno. Estas métricas están sujetas a cambios entre las versiones de StorageGRID sin previo aviso.

- **Node-details**: Operaciones en los detalles del nodo.
- **Node-health**: Operaciones en el estado de salud del nodo.
- **Node-storage-state**: Operaciones en el estado de almacenamiento del nodo.
- **Servidores ntp**: Operaciones para listar o actualizar servidores externos de Protocolo de Tiempo de Red (NTP).
- **OBJETOS**: Operaciones en objetos y metadatos de objetos.
- **RECUPERACIÓN**: Operaciones para el procedimiento de recuperación.
- **recovery-package**: Operaciones para descargar el paquete de recuperación.
- **REGIONES**: Operaciones para ver y crear regiones.
- **S3-object-lock**: Operaciones en la configuración global de S3 Object Lock.
- **Server-certificate**: Operaciones para ver y actualizar los certificados de servidor de Grid Manager.
- **snmp**: Operaciones en la configuración SNMP actual.
- **Storage-watermarks**: Marcas de agua del nodo de almacenamiento.
- **Clases de tráfico**: Operaciones para las políticas de clasificación de tráfico.
- **Red-cliente-no confiable**: Operaciones en la configuración de la red cliente no confiable.
- **Usuarios**: Operaciones para ver y administrar usuarios de Grid Manager.

Creación de versiones de la API de gestión de grid

La API de gestión de grid utiliza versiones para permitir actualizaciones sin interrupciones.

Por ejemplo, esta URL de solicitud especifica la versión 4 de la API.

`https://hostname_or_ip_address/api/v4/authorize`

La versión principal de la API se salta cuando se realizan cambios que son *no compatibles* con versiones anteriores. La versión secundaria de la API se salta cuando se realizan cambios que son compatibles con versiones anteriores. Los cambios compatibles incluyen la adición de nuevos extremos o nuevas propiedades.

En el ejemplo siguiente se muestra cómo la versión de API se bONTAP en función del tipo de cambios realizados.

Tipo de cambio en la API	Versión anterior	Nueva versión
Compatible con versiones anteriores	2,1	2,2
No es compatible con versiones anteriores	2,1	3,0

Al instalar el software StorageGRID por primera vez, solo se habilita la versión más reciente de la API. Sin embargo, cuando actualice a una versión de función nueva de StorageGRID, seguirá teniendo acceso a la versión de API anterior para al menos una versión de función de StorageGRID.

> Puede configurar las versiones admitidas. Consulte la sección **config** de la documentación de API de Swagger para "API de gestión de grid"obtener más información. Debe desactivar la compatibilidad con la versión anterior después de actualizar todos los clientes API para que usen la versión más reciente.

Las solicitudes obsoletas se marcan como obsoletas de las siguientes formas:

- El encabezado de la respuesta es "Dedeprecated: True"
- El cuerpo de respuesta JSON incluye "obsoleto": TRUE
- Se agrega una advertencia obsoleta a nms.log. Por ejemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determine qué versiones de API son compatibles con la versión actual

Utilice `GET /versions` la solicitud de API para devolver una lista de las versiones principales de la API admitidas. Esta solicitud se encuentra en la sección **config** de la documentación de la API de Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Especifique una versión API para una solicitud

Puede especificar la versión de la API mediante un parámetro de ruta (`/api/v4`) o una cabecera)(`Api-Version: 4`. Si proporciona ambos valores, el valor de encabezado anula el valor de ruta de acceso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protección contra falsificación de solicitudes entre sitios (CSRF)

Puede ayudar a protegerse contra ataques de falsificación de solicitudes entre sitios (CSRF) contra StorageGRID mediante tokens CSRF para mejorar la autenticación que usa cookies. El administrador de grid y el administrador de inquilinos habilitan automáticamente esta característica de seguridad; otros clientes de API pueden elegir si habilitar la función cuando se conectan.

Un atacante que pueda activar una solicitud a un sitio diferente (por ejemplo, con UNA POST de formulario HTTP) puede provocar ciertas solicitudes mediante las cookies del usuario que ha iniciado sesión.

StorageGRID ayuda a proteger contra ataques de CSRF mediante tokens CSRF. Cuando se activa, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro DE cuerpo DE POST específico.

Para habilitar la función, se debe establecer `csrfToken` el parámetro en `true` durante la autenticación. El valor predeterminado es `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Cuando es verdadero, una `GridCsrfToken` cookie se establece con un valor aleatorio para los inicios de sesión en Grid Manager, y la `AccountCsrfToken` cookie se establece con un valor aleatorio para los inicios de sesión en el gestor de inquilinos.

Si la cookie está presente, todas las solicitudes que puedan modificar el estado del sistema (POST, PUT, PATCH, DELETE) deben incluir una de las siguientes:

- `X-Csrf-Token`El encabezado, con el valor del encabezado definido en el valor de la cookie de token CSRF.
- Para puntos finales que aceptan un cuerpo codificado en forma: Un `csrfToken` parámetro de cuerpo de solicitud codificado en forma.

Consulte la documentación de API en línea para obtener detalles y ejemplos adicionales.

> Las solicitudes que tienen un conjunto de cookies de token CSRF también aplicarán el encabezado de tipo de contenido: Aplicación/json para cualquier solicitud que espere un cuerpo de solicitud JSON como una protección adicional contra los ataques CSRF.

Use la API si está activado el inicio de sesión único

Utilizar la API si está activado el inicio de sesión único (Active Directory)

Si tienes"Inicio de sesión único configurado y habilitado (SSO)" y utiliza Active Directory como proveedor de SSO, debe emitir una serie de solicitudes de API para obtener un token de autenticación que sea válido para la API de administración de Grid o la API de administración de inquilinos.

Inicie sesión en la API si está habilitado el inicio de sesión único

Estas instrucciones se aplican si utiliza Active Directory como proveedor de identidades SSO.

Antes de empezar

- Conoce el nombre de usuario y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- El `storagegrid-ssoauth.py` Script de Python, que se encuentra en el directorio de archivos de instalación de StorageGRID(`./rpms` para RHEL, `./debs` para Ubuntu o Debian, y `./vsphere` para

VMware).

- Ejemplo de flujo de trabajo de solicitudes curl.

  El flujo de trabajo curl podría llegar a ocurrir si lo hace demasiado lentamente. Es posible que vea el error: `A valid SubjectConfirmation was not found on this Response`.

  > El flujo de trabajo curl de ejemplo no protege la contraseña de ser vista por otros usuarios.

Si tiene un problema de codificación de URL, puede que aparezca el error: `Unsupported SAML version`.

Pasos

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
   - Utilice `storagegrid-ssoauth.py` el script de Python. Vaya al paso 2.
   - Usar solicitudes curl. Vaya al paso 3.
2. Si desea utilizar `storagegrid-ssoauth.py` el script, pase el script al intérprete de Python y ejecute el script.

   Cuando se le solicite, escriba valores para los siguientes argumentos:

   - El método SSO. Introduzca ADFS o adfs.
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID
   - La dirección de StorageGRID
   - El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

3. Si desea usar solicitudes curl, use el siguiente procedimiento.

   a. Declare las variables necesarias para iniciar sesión.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

Para acceder a la API de gestión de grid, utilice 0 como `TENANTACCOUNTID`.

b. Para recibir una URL de autenticación firmada, emita una solicitud POST a `/api/v3/authorize-saml` y elimine la codificación JSON adicional de la respuesta.

Este ejemplo muestra una solicitud POST para una URL de autenticación firmada para `TENANTACCOUNTID`. Los resultados se pasarán a `python -m json.tool` para eliminar la codificación JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La respuesta de este ejemplo incluye una dirección URL firmada codificada por URL, pero no incluye la capa de codificación JSON adicional.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Guarde el `SAMLRequest` de la respuesta para utilizarlo en comandos posteriores.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Obtenga una URL completa que incluya el ID de solicitud de cliente de AD FS.

Una opción es solicitar el formulario de inicio de sesión mediante la URL de la respuesta anterior.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

La respuesta incluye el ID de solicitud del cliente:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Guarde el ID de solicitud de cliente de la respuesta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envíe sus credenciales a la acción de formulario de la respuesta anterior.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS devuelve un redireccionamiento 302, con información adicional en los encabezados.

> Si la autenticación multifactor (MFA) está habilitada para el sistema SSO, la entrada del formulario también contendrá la segunda contraseña u otras credenciales.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Guarde la `MSISAuth` cookie de la respuesta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envíe una solicitud GET a la ubicación especificada con las cookies de LA PUBLICACIÓN de autenticación.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Los encabezados de respuesta contendrán información de sesión de AD FS para el uso posterior del cierre de sesión y el cuerpo de respuesta contiene el SAMLResponse en un campo de formulario oculto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Guarde el `SAMLResponse` desde el campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Uso de Guardado `SAMLResponse`, Realice una solicitud StorageGRID`/api/saml-response` para generar un token de autenticación StorageGRID.

Para `RelayState`, utilice el ID de cuenta de inquilino o utilice 0 si desea iniciar sesión en la API de gestión de grid.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La respuesta incluye el token de autenticación.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Guarde el token de autenticación en la respuesta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ahora puede usar `MYTOKEN` para otras solicitudes, de forma similar a cómo usaría la API si no se estaba utilizando SSO.

Cierre sesión en la API si el inicio de sesión único está habilitado

Si se ha activado el inicio de sesión único (SSO), debe emitir una serie de solicitudes API para cerrar sesión en la API de gestión de grid o en la API de gestión de inquilinos. Estas instrucciones se aplican si utiliza Active Directory como proveedor de identidades SSO

Acerca de esta tarea

Si es necesario, puede cerrar sesión en la API de StorageGRID cerrando sesión en la página de cierre de sesión único de su organización. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, que requiere un token de portador de StorageGRID válido.

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase la cookie «sso=true» a la API de SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Se devuelve una URL de cierre de sesión:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Guarde la URL de cierre de sesión.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. Envíe una solicitud a la URL de cierre de sesión para activar SLO y redirigir de nuevo a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta de 302. La ubicación de redirección no se aplica a la salida de sólo API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Elimine el token del portador de StorageGRID.

La eliminación del token del portador de StorageGRID funciona de la misma forma que sin SSO. Si no se proporciona 'cookie 'sso=true', el usuario se cierra la sesión de StorageGRID sin afectar al estado de SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

Una `204 No Content` respuesta indica que el usuario ha cerrado sesión.

```
HTTP/1.1 204 No Content
```

Utilice la API si el inicio de sesión único está habilitado (ID de entrada)

Si tienes"Inicio de sesión único configurado y habilitado (SSO)" y utiliza Entra ID como proveedor de SSO, puede usar dos scripts de ejemplo para obtener un token de autenticación que sea válido para la API de administración de red o la API de administración de inquilinos.

Sign in en la API si el inicio de sesión único de Entra ID está habilitado

Estas instrucciones se aplican si está utilizando Entra ID como proveedor de identidad SSO

Antes de empezar

- Conoce la dirección de correo electrónico y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar las siguientes secuencias de comandos de ejemplo:

- El `storagegrid-ssoauth-azure.py` script de Python
- `storagegrid-ssoauth-azure.js`El script Node.js

Ambos scripts se encuentran en el directorio de archivos de instalación de StorageGRID(`./rpms` para RHEL, `./debs` para Ubuntu o Debian, y `./vsphere` para VMware).

Para escribir su propia integración de API con Entra ID, consulte la `storagegrid-ssoauth-azure.py` guion. El script de Python realiza dos solicitudes a StorageGRID directamente (primero para obtener SAMLRequest y luego para obtener el token de autorización) y también llama al script Node.js para interactuar con Entra ID para realizar las operaciones de SSO.

Las operaciones de SSO se pueden ejecutar mediante una serie de solicitudes de API, pero hacerlo no es sencillo. El módulo Node.js Puppeteer se utiliza para extraer la interfaz SSO de Entra ID.

Si tiene un problema de codificación de URL, puede que aparezca el error: `Unsupported SAML version`.

Pasos

1. Instale las dependencias necesarias de la siguiente manera:

a. Instale Node.js (consulte "https://nodejs.org/en/download/").

b. Instale los módulos Node.js necesarios (tippeteer y jsdom):

```
npm install -g <module>
```

2. Pase la secuencia de comandos de Python al intérprete de Python para ejecutar la secuencia de comandos.

   Luego, el script de Python llamará al script Node.js correspondiente para realizar las interacciones SSO de Entra ID.

3. Cuando se le solicite, introduzca valores para los siguientes argumentos (o bien, pasarlos mediante parámetros):
   - La dirección de correo electrónico SSO utilizada para iniciar sesión en Entra ID
   - La dirección de StorageGRID
   - El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos
4. Cuando se le solicite, ingrese la contraseña y prepárese para proporcionar una autorización MFA a Entra ID si se le solicita.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> La secuencia de comandos asume que la MFA se realiza utilizando Microsoft Authenticator. Es posible que necesite modificar el script para admitir otras formas de MFA (como introducir un código recibido en un mensaje de texto).

El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

Utilizar la API si está activado el inicio de sesión único (PingFederate)

Si tienes"Inicio de sesión único configurado y habilitado (SSO)" y utiliza PingFederate como proveedor de SSO, debe emitir una serie de solicitudes de API para obtener un token de autenticación que sea válido para la API de administración de red o la API de administración de inquilinos.

Inicie sesión en la API si está habilitado el inicio de sesión único

Estas instrucciones se aplican si está utilizando PingFederate como proveedor de identidades SSO

Antes de empezar

- Conoce el nombre de usuario y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- El `storagegrid-ssoauth.py` Script de Python, que se encuentra en el directorio de archivos de instalación de StorageGRID(`./rpms` para RHEL, `./debs` para Ubuntu o Debian, y `./vsphere` para VMware).
- Ejemplo de flujo de trabajo de solicitudes curl.

  El flujo de trabajo curl podría llegar a ocurrir si lo hace demasiado lentamente. Es posible que vea el error: `A valid SubjectConfirmation was not found on this Response`.

  > El flujo de trabajo curl de ejemplo no protege la contraseña de ser vista por otros usuarios.

  Si tiene un problema de codificación de URL, puede que aparezca el error: `Unsupported SAML version`.

Pasos

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
   - Utilice `storagegrid-ssoauth.py` el script de Python. Vaya al paso 2.
   - Usar solicitudes curl. Vaya al paso 3.
2. Si desea utilizar `storagegrid-ssoauth.py` el script, pase el script al intérprete de Python y ejecute el script.

   Cuando se le solicite, escriba valores para los siguientes argumentos:

   - El método SSO. Puede introducir cualquier variación de “pingfederate” (PINGFEDERATE, pingfederate, etc.).
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID. Este campo no se utiliza para PingFederate. Puede dejarlo en blanco o introducir cualquier valor.
   - La dirección de StorageGRID
   - El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

3. Si desea usar solicitudes curl, use el siguiente procedimiento.

   a. Declare las variables necesarias para iniciar sesión.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

   Para acceder a la API de gestión de grid, utilice 0 como `TENANTACCOUNTID`.

   b. Para recibir una URL de autenticación firmada, emita una solicitud POST a `/api/v3/authorize-saml` y elimine la codificación JSON adicional de la respuesta.

   En este ejemplo se muestra una solicitud POST para una dirección URL de autenticación firmada para TENANTACCOUNTID. Los resultados se pasan a python -m json.tool para quitar la codificación JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

   La respuesta de este ejemplo incluye una dirección URL firmada codificada por URL, pero no incluye la capa de codificación JSON adicional.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

   c. Guarde el `SAMLRequest` de la respuesta para utilizarlo en comandos posteriores.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

   d. Exporte la respuesta y el cookie y añada la respuesta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exporte el valor 'pf.adapterId' y añada la respuesta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exporte el valor 'href' (retire la barra diagonal inversa /) y añada la respuesta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exporte el valor de 'acción':

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Enviar cookies junto con credenciales:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Guarde el `SAMLResponse` desde el campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Uso de Guardado `SAMLResponse`, Realice una solicitud StorageGRID`/api/saml-response` para generar un token de autenticación StorageGRID.

   Para `RelayState`, utilice el ID de cuenta de inquilino o utilice 0 si desea iniciar sesión en la API de gestión de grid.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La respuesta incluye el token de autenticación.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Guarde el token de autenticación en la respuesta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ahora puede usar `MYTOKEN` para otras solicitudes, de forma similar a cómo usaría la API si no se estaba utilizando SSO.

Cierre sesión en la API si el inicio de sesión único está habilitado

Si se ha activado el inicio de sesión único (SSO), debe emitir una serie de solicitudes API para cerrar sesión en la API de gestión de grid o en la API de gestión de inquilinos. Estas instrucciones se aplican si está utilizando PingFederate como proveedor de identidades SSO

Acerca de esta tarea

Si es necesario, puede cerrar sesión en la API de StorageGRID cerrando sesión en la página de cierre de sesión único de su organización. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, que requiere un token de portador de StorageGRID válido.

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase la cookie «sso=true» a la API de SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Se devuelve una URL de cierre de sesión:

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Guarde la URL de cierre de sesión.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envíe una solicitud a la URL de cierre de sesión para activar SLO y redirigir de nuevo a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta de 302. La ubicación de redirección no se aplica a la salida de sólo API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Elimine el token del portador de StorageGRID.

La eliminación del token del portador de StorageGRID funciona de la misma forma que sin SSO. Si no se proporciona 'cookie 'sso=true', el usuario se cierra la sesión de StorageGRID sin afectar al estado de SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

Una `204 No Content` respuesta indica que el usuario ha cerrado sesión.

```
HTTP/1.1 204 No Content
```

Desactivar las funcionalidades con la API

Puede utilizar la API de gestión de grid para desactivar por completo determinadas funciones del sistema StorageGRID. Cuando se desactiva una función, no se pueden asignar permisos a nadie para realizar las tareas relacionadas con esa función.

Acerca de esta tarea

El sistema de funciones desactivadas le permite impedir el acceso a determinadas funciones del sistema StorageGRID. La desactivación de una característica es la única forma de impedir que el usuario raíz o los usuarios que pertenecen a grupos de administración con permiso **acceso raíz** puedan utilizar esa función.

Para comprender cómo puede ser útil esta funcionalidad, considere el siguiente escenario:

Company A es un proveedor de servicios que arrienda la capacidad de almacenamiento de su sistema StorageGRID mediante la creación de cuentas de inquilino. Para proteger la seguridad de los objetos de sus arrendatarios, la Compañía A desea asegurarse de que sus propios empleados nunca tengan acceso a ninguna cuenta de arrendatario después de que se haya implementado la cuenta.

*La empresa A puede lograr este objetivo mediante el sistema Desactivar características en la API de gestión de grid. Al desactivar completamente la función **Cambiar contraseña raíz del inquilino** en Grid Manager (tanto la interfaz de usuario como la API), la Compañía A garantiza que los usuarios administradores, incluidos el usuario raíz y los usuarios que pertenecen a grupos con el permiso **root access**, no puedan cambiar la contraseña para el usuario raíz de cualquier cuenta de inquilino.*

Pasos

1. Acceda a la documentación de Swagger para la API de Grid Management. Consulte "Utilice la API de gestión de grid".
2. Busque el extremo Desactivar funciones.
3. Para desactivar una función, como Cambiar contraseña raíz de inquilino, envíe un cuerpo a la API de este modo:

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   Cuando se completa la solicitud, la función Cambiar contraseña raíz de inquilino está desactivada. El permiso de administración de **Change tenant root password** ya no aparece en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña root para un inquilino fallará con “403 Forbidden”.

Reactivar las funciones desactivadas

De forma predeterminada, puede utilizar la API de administración de grid para reactivar una función que se haya desactivado. Sin embargo, si desea evitar que alguna vez se reactiven las funciones desactivadas, puede desactivar la propia función **activateFeatures**.

> La función **activateFeatures** no se puede reactivar. Si decide desactivar esta función, tenga en cuenta que perderá permanentemente la capacidad de reactivar otras funciones desactivadas. Para restaurar cualquier funcionalidad perdida, debe ponerse en contacto con el soporte técnico.

Pasos

1. Acceda a la documentación de Swagger para la API de Grid Management.

2. Busque el extremo Desactivar funciones.
3. Para reactivar todas las funciones, envíe un cuerpo a la API de este modo:

```
{ "grid": null }
```

Cuando se completa esta solicitud, se reactivan todas las funciones, incluida la función Cambiar contraseña raíz del inquilino. El permiso de administración **Cambiar contraseña raíz de arrendatario** aparece ahora en la interfaz de usuario y cualquier solicitud de API que intente cambiar la contraseña raíz de un inquilino se realizará correctamente, suponiendo que el usuario tenga el permiso de administración **acceso raíz** o **Cambiar contraseña raíz de inquilino**.

El ejemplo anterior hace que se reactiven las funciones *all* desactivadas. Si se han desactivado otras funciones que deben permanecer desactivadas, debe especificarlas explícitamente en la solicitud PUT. Por ejemplo, para reactivar la función Change tenant root password y continuar desactivando el permiso de gestión storageAdmin, envíe esta solicitud PUT:

```
{ "grid": {"storageAdmin": true} }
```

Control del acceso a StorageGRID

Control del acceso a StorageGRID

Puede controlar quién puede acceder a StorageGRID y qué tareas pueden realizar los usuarios creando o importando grupos y usuarios, y asignando permisos a cada grupo. De manera opcional, puede habilitar el inicio de sesión único (SSO), crear certificados de cliente y cambiar contraseñas de grid.

Controle el acceso a Grid Manager

Para determinar quién puede acceder a Grid Manager y a la API de gestión de grid, importe grupos y usuarios desde un servicio de federación de identidades o configure grupos locales y usuarios locales.

El uso "federación de identidades" hace que la configuración "grupos" "usuarios"sea más rápida, y permite a los usuarios iniciar sesión en StorageGRID usando credenciales conocidas. Puede configurar la federación de identidades si utiliza Active Directory, OpenLDAP u Oracle Directory Server.

Póngase en contacto con el soporte técnico si desea utilizar otro servicio LDAP v3.

Para determinar qué tareas puede realizar cada usuario, asigne diferentes "permisos" a cada grupo. Por ejemplo, es posible que desee que los usuarios de un grupo puedan gestionar las reglas de ILM y los usuarios de otro grupo para realizar tareas de mantenimiento. Un usuario debe pertenecer al menos a un grupo para acceder al sistema.

De manera opcional, puede configurar un grupo para que sea de sólo lectura. Los usuarios de un grupo de sólo lectura sólo pueden ver la configuración y las funciones. No pueden realizar cambios ni realizar ninguna operación en Grid Manager o la API de administración de grid.

Active el inicio de sesión único

El sistema StorageGRID admite el inicio de sesión único (SSO) mediante el estándar Security Assertion Markup Language 2.0 (SAML 2.0). Después de usted"Configure y habilite SSO" Todos los usuarios deben

estar autenticados por un proveedor de identidad externo antes de poder acceder al Administrador de Grid, al Administrador de Inquilinos, a la API de Administración de Grid o a la API de Administración de Inquilinos. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cambie la clave de acceso de aprovisionamiento

La frase de contraseña de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para descargar el paquete de recuperación de StorageGRID . La frase de contraseña también es necesaria para descargar copias de seguridad de la información de topología de la red y de las claves de cifrado para el sistema StorageGRID . Puede"cambie la contraseña" según sea necesario.

Cambie las contraseñas de la consola de los nodos

Cada nodo de su red tiene una contraseña de consola de nodo, que necesita para iniciar sesión en el nodo como "admin" mediante SSH, o como usuario root en una conexión de consola física/VM. Según sea necesario, puede"cambie la contraseña de la consola del nodo" para cada nodo.

Cambie la clave de acceso del aprovisionamiento

Utilice este procedimiento para cambiar la frase de contraseña de aprovisionamiento de StorageGRID . La frase de contraseña es necesaria para los procedimientos de recuperación, expansión y mantenimiento. La frase de contraseña también es necesaria para descargar copias de seguridad del paquete de recuperación que incluyen la información de topología de la red, las contraseñas de la consola del nodo de la red y las claves de cifrado para el sistema StorageGRID .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tiene permisos de acceso raíz o de mantenimiento.
- Tiene la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

La frase de contraseña de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para"descargando el paquete de recuperación" . La frase de contraseña de aprovisionamiento no aparece en la `Passwords.txt` archivo. Asegúrese de documentar la contraseña de aprovisionamiento y guardarla en un lugar seguro.

Pasos

1. Seleccione **Configuración** > **Control de acceso**> **Contraseñas de red**.
2. En **Cambiar contraseña de aprovisionamiento**, selecciona **Hacer un cambio**
3. Introduzca la clave de acceso de aprovisionamiento actual.
4. Introduzca la nueva frase de contraseña. La frase de contraseña debe contener al menos 8 caracteres y no más de 32. Las passphrasas distinguen entre mayúsculas y minúsculas.

   > Guarde la contraseña de aprovisionamiento en una ubicación segura. Es necesario para los procedimientos de instalación, expansión y mantenimiento.

5. Vuelva a introducir la nueva contraseña y seleccione **Guardar**.

   El sistema muestra un banner verde de éxito cuando se completa el cambio de la clave de acceso de

aprovisionamiento.

6. Seleccione **paquete de recuperación**.
7. Ingrese la nueva contraseña de aprovisionamiento para descargar el nuevo paquete de recuperación.

> Después de cambiar la contraseña de aprovisionamiento, debe descargar inmediatamente un nuevo paquete de recuperación. El archivo del paquete de recuperación le permite restaurar el sistema si ocurre una falla.

Cambie las contraseñas de la consola de los nodos

Cada nodo de su red tiene una contraseña de consola de nodo, que usted utiliza para iniciar sesión en el nodo. De forma predeterminada, cada nodo tiene una contraseña única. Puede cambiar cada contraseña por una nueva contraseña única o puede cambiar la contraseña de cada nodo para utilizar una contraseña global. Las contraseñas se almacenan en el paquete de recuperación.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

Utilice una contraseña de consola de nodo para iniciar sesión en un nodo como "admin" mediante SSH, o como usuario root en una conexión de consola física/VM. Puede cambiar las contraseñas de la consola del nodo utilizando una de estas opciones:

- Aplicar automáticamente contraseñas aleatorias a cada nodo
- Especifique y aplique una contraseña global a todos los nodos
- Especificar y aplicar una contraseña única a uno o más nodos

Las contraseñas se almacenan de forma actualizada. `Passwords.txt` archivo en el paquete de recuperación. Las contraseñas se enumeran en la columna Contraseña del archivo.

> El"Contraseñas de acceso SSH" Las claves SSH utilizadas para la comunicación entre nodos son independientes de las contraseñas de la consola del nodo. Este procedimiento no cambia las contraseñas de acceso SSH.

Acceda al asistente

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Contraseñas de red**.
2. En **Cambiar contraseñas de consola de nodo**, selecciona **Hacer un cambio**.

Descargue el paquete de recuperación actual

Antes de cambiar las contraseñas de la consola del nodo, descargue el paquete de recuperación actual. Puede utilizar las contraseñas de este archivo si el proceso de cambio de contraseña falla para algún nodo.

Pasos

1. Introduzca la clave de acceso de aprovisionamiento para el grid.
2. Seleccione **Descargar paquete de recuperación**.
3. Copiar el archivo del paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.

   El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

4. Seleccione **continuar**.

Proporcionar nuevas contraseñas

1. Seleccione el método de cambio de contraseña que desea utilizar.
   - **Automático**: StorageGRID asigna automáticamente una nueva contraseña de consola aleatoria a todos los nodos.
   - **Personalizado**: proporcionas contraseñas de consola.

Automático

1. Seleccione **continuar**.

Personalizado

1. Seleccione una de las siguientes opciones:
   - **Contraseña de consola global**: aplica la misma contraseña de consola a todos los nodos.
   - **Contraseñas de consola únicas**: aplique una contraseña diferente en uno o más nodos.
2. Si seleccionó **Contraseña de consola global**, ingrese la contraseña que desea usar para todos los nodos.
3. Si seleccionó **Contraseñas de consola únicas**, ingrese una contraseña única para uno o más nodos.
4. Seleccione **continuar**.

Completar el cambio de contraseña

1. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para que StorageGRID comience a cambiar las contraseñas de la consola del nodo.

   No puede cancelar este proceso una vez que se inicia.

   StorageGRID genera un nuevo paquete de recuperación que contiene la nueva contraseña.

2. Cuando el nuevo paquete de recuperación esté listo, seleccione **Descargar nuevo paquete de recuperación** y guarde el paquete de recuperación.

3. Abra el `.zip` archivo.
4. Confirme que puede acceder al contenido, incluido `Passwords.txt` el archivo, que contiene las nuevas contraseñas de la consola del nodo.
5. Copiar el nuevo archivo del paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.

   > No sobrescriba el paquete de recuperación antiguo.

   Debe proteger el archivo de recuperación, ya que contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .
6. Seleccione la casilla de verificación para indicar que ha descargado el nuevo paquete de recuperación y verificado el contenido.
7. Seleccione **continuar**.

   StorageGRID actualiza la contraseña de cada nodo.

   Si hay un error durante el proceso de actualización, la barra de progreso enumera la cantidad de nodos cuyas contraseñas no se pudieron cambiar. El sistema volverá a intentar automáticamente el proceso en cualquier nodo cuya contraseña no se haya podido cambiar. Si el proceso finaliza con algunos nodos que aún no tienen la contraseña cambiada, aparece el botón **Reintentar**.
8. Si la actualización de la contraseña falló para uno o más nodos:
   a. Revise los mensajes de error que aparecen en la tabla.
   b. Resuelva los problemas.
   c. Seleccione **Reintentar**.

   > Al volver a intentar solo se cambian las contraseñas de la consola de nodos en los nodos que fallaron durante los intentos anteriores de cambio de contraseña.
9. Cuando la barra de progreso indique que no quedan actualizaciones, seleccione **Finalizar**.
10. Después de cambiar las contraseñas de la consola de nodo para todos los nodos, elimine el archivoprimer paquete de recuperación que descargaste .

Cambiar las contraseñas de acceso SSH para los nodos de administración

Al cambiar las contraseñas de acceso SSH para los nodos de administración, también se actualizan los conjuntos únicos de claves SSH internas de cada nodo del grid. El nodo de administración principal utiliza estas claves SSH para acceder a los nodos utilizando una autenticación segura y sin contraseña.

Utilice una clave SSH para iniciar sesión en un nodo `admin` como o para el usuario raíz en una máquina virtual o una conexión de consola física.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

Las nuevas contraseñas de acceso para los nodos de administración y las nuevas claves internas para cada nodo se almacenan en el `Passwords.txt` archivo en el paquete de recuperación. Las claves se enumeran en la columna Contraseña de ese archivo.

Hay contraseñas de acceso SSH separadas para las claves SSH que se usan para la comunicación entre nodos. Estos no se modifican con este procedimiento.

Acceda al asistente

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Contraseñas de red**.
2. En **Cambiar claves SSH**, selecciona **Hacer un cambio**.

Descargue el paquete de recuperación actual

Antes de cambiar las claves de acceso SSH, descargue el paquete de recuperación actual. Puede utilizar las claves de este archivo si el proceso de cambio de clave falla para algún nodo.

Pasos

1. Introduzca la clave de acceso de aprovisionamiento para el grid.
2. Seleccione **Descargar paquete de recuperación**.
3. Copiar el archivo del paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.

   El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

4. Seleccione **continuar**.
5. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para comenzar a cambiar las claves de acceso SSH.

   No puede cancelar este proceso una vez que se inicia.

Cambiar las claves de acceso SSH

Cuando se inicia el proceso de cambio de claves de acceso SSH, se genera un nuevo paquete de recuperación que incluye las nuevas claves. Luego, las claves se actualizan en cada nodo.

Pasos

1. Espere a que se genere el nuevo paquete de recuperación, lo que puede tardar unos minutos.
2. Cuando el botón Descargar nuevo paquete de recuperación esté habilitado, seleccione **Descargar nuevo paquete de recuperación** y guarde el archivo del nuevo paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.
3. Cuando finalice la descarga:

   a. Abra el `.zip` archivo.

   b. Confirme que puede acceder al contenido, incluido `Passwords.txt` el archivo, que contiene las nuevas claves de acceso SSH.

c. Copiar el nuevo archivo del paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.

> No sobrescriba el paquete de recuperación antiguo.

El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

4. Espere a que las claves se actualicen en cada nodo, lo que puede tardar unos minutos.

   Si se cambian las claves para todos los nodos, aparece un banner verde correcto.

   Si se produce un error durante el proceso de actualización, un mensaje de banner muestra el número de nodos que no pudieron cambiar sus claves. El sistema volverá a intentar automáticamente el proceso en cualquier nodo que no haya cambiado su clave. Si el proceso termina con algunos nodos que aún no tienen una clave cambiada, aparece el botón **Reintentar**.

   Si la actualización de clave falló para uno o más nodos:

   a. Revise los mensajes de error que aparecen en la tabla.
   b. Resuelva los problemas.
   c. Seleccione **Reintentar**.

      El reintento sólo cambia las claves de acceso SSH en los nodos que han fallado durante los intentos de cambio de clave anteriores.

5. Después de cambiar las claves de acceso SSH para todos los nodos, elimine el archivoprimer paquete de recuperación que descargaste .
6. Opcionalmente, seleccione **Mantenimiento** > **Sistema** > **Paquete de recuperación** para descargar una copia adicional del nuevo paquete de recuperación.

Usar la federación de identidades

El uso de la federación de identidades agiliza la configuración de grupos y usuarios y permite a los usuarios iniciar sesión en StorageGRID utilizando credenciales conocidas.

Configurar la federación de identidades para Grid Manager

Puede configurar la federación de identidad en Grid Manager si desea que los grupos de administradores y los usuarios se administren en otro sistema, como Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server.

Antes de empezar

- Has iniciado sesión en Grid Manager usando un"navegador web compatible" .
- Tú tienes"permisos de acceso específicos" .
- Está utilizando Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server como proveedor de identidad.

> Si desea utilizar un servicio LDAP v3 que no figura en la lista, comuníquese con el soporte técnico.

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Consulte Instrucciones para configurar un servidor OpenLDAP.
- Si planea habilitar el inicio de sesión único (SSO), ha revisado la"requisitos y consideraciones para el inicio de sesión único" .
- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades usa TLS 1.2 o 1.3. Consulte "Cifrados compatibles para conexiones TLS salientes".

Acerca de esta tarea

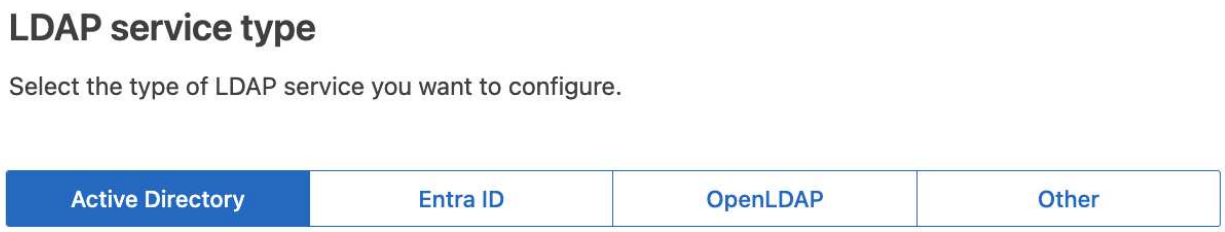
Puede configurar una fuente de identidad para Grid Manager si desea importar grupos de otro sistema, como Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server. Puede importar los siguientes tipos de grupos:

- Grupos de administración. Los usuarios de los grupos de administración pueden iniciar sesión en Grid Manager y realizar tareas basándose en los permisos de administración asignados al grupo.
- Grupos de usuarios de inquilinos para inquilinos que no utilizan su propio origen de identidad. Los usuarios de grupos de inquilinos pueden iniciar sesión en el Administrador de inquilinos y realizar tareas, en función de los permisos asignados al grupo en el Administrador de inquilinos. Consulte "Cree una cuenta de inquilino" y "Usar una cuenta de inquilino" para obtener más información.

Introduzca la configuración

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Federación de identidades**.
2. Seleccione **Activar federación de identidades**.
3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.



   Seleccione **otros** para configurar valores para un servidor LDAP que utilice Oracle Directory Server.

4. Si ha seleccionado **otros**, complete los campos de la sección atributos LDAP . De lo contrario, vaya al paso siguiente.
   - **Nombre único de usuario**: el nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a `sAMAccountName` para Active Directory y `uid` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `uid` .
   - **UUID de usuario**: el nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a `objectGUID` para Active Directory y `entryUUID` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `nsuniqueid` . El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.

- **Nombre único del grupo**: el nombre del atributo que contiene el identificador único de un grupo LDAP. Este atributo es equivalente a `sAMAccountName` para Active Directory y `cn` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `cn` .
- **UUID de grupo**: el nombre del atributo que contiene el identificador único permanente de un grupo LDAP. Este atributo es equivalente a `objectGUID` para Active Directory y `entryUUID` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `nsuniqueid` . El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.

5. Para todos los tipos de servicio LDAP, introduzca la información de servidor LDAP y conexión de red necesaria en la sección Configure LDAP Server.
   - **Hostname**: El nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
   - **Puerto**: El puerto utilizado para conectarse al servidor LDAP.

     > El puerto predeterminado para STARTTLS es 389 y el puerto predeterminado para LDAPS es 636. Sin embargo, puede utilizar cualquier puerto siempre que su firewall esté configurado correctamente.

   - **Nombre de usuario**: La ruta completa del nombre completo (DN) para el usuario que se conectará al servidor LDAP.

     Para Active Directory, también puede especificar el nombre de inicio de sesión de nivel inferior o el nombre principal del usuario.

     El usuario especificado debe tener permiso para enumerar grupos y usuarios y para tener acceso a los siguientes atributos:

     - `sAMAccountName` o. `uid`
     - `objectGUID`, , `entryUUID` o. `nsuniqueid`
     - `cn`
     - `memberOf` o. `isMemberOf`
     - **Active Directory** `objectSid`: , , `primaryGroupID`, `userAccountControl` Y. `userPrincipalName`
     - **ID de entrada**: `accountEnabled` y `userPrincipalName`
   - **Contraseña**: La contraseña asociada al nombre de usuario.

     > Si cambia la contraseña en el futuro, debe actualizarla en esta página.

   - **DN base de grupo**: La ruta completa del nombre distinguido (DN) para un subárbol LDAP que desea buscar grupos. En el ejemplo de Active Directory (a continuación), se pueden usar como grupos federados todos los grupos cuyo nombre distintivo sea relativo al DN base (DC=storagegrid,DC=example,DC=com).

     > Los valores de **Nombre único de grupo** deben ser únicos dentro del **DN base de grupo** al que pertenecen.

   - **DN base de usuario**: La ruta completa del nombre completo (DN) de un subárbol LDAP que desea buscar usuarios.

> Los valores de **Nombre único de usuario** deben ser únicos dentro del **DN base de usuario** al que pertenecen.

- **Formato de nombre de usuario de enlace** (opcional): El patrón de nombre de usuario predeterminado StorageGRID debe usarse si el patrón no se puede determinar automáticamente.

  Se recomienda proporcionar **Formato de nombre de usuario Bind** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede enlazar con la cuenta de servicio.

  Introduzca uno de estos patrones:

  - **Patrón UserPrincipalName (ID de AD y Entra)**: `[USERNAME]@example.com`
  - **Patrón de nombre de inicio de sesión de nivel inferior (ID de AD y Entra)**: `example\[USERNAME]`
  - * Patrón de nombre distinguido *: `CN=[USERNAME],CN=Users,DC=example,DC=com`

    Incluya **[USERNAME]** exactamente como está escrito.

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.
   - **Usar STARTTLS**: utilice STARTTLS para proteger las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u otros, pero esta opción no es compatible con Microsoft Entra ID.
   - **Usar LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Microsoft Entra ID.
   - **No utilizar TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Microsoft Entra ID.

   > No se admite el uso de la opción **No usar TLS** si su servidor de Active Directory aplica la firma LDAP. Debe utilizar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.
   - **Utilizar certificado CA del sistema operativo**: Utilice el certificado predeterminado de CA de red instalado en el sistema operativo para asegurar las conexiones.
   - **Utilizar certificado de CA personalizado**: Utilice un certificado de seguridad personalizado.

     Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

Pruebe la conexión y guarde la configuración

Después de introducir todos los valores, es necesario probar la conexión para poder guardar la configuración. StorageGRID verifica la configuración de conexión del servidor LDAP y el formato de nombre de usuario de enlace, si proporcionó uno.

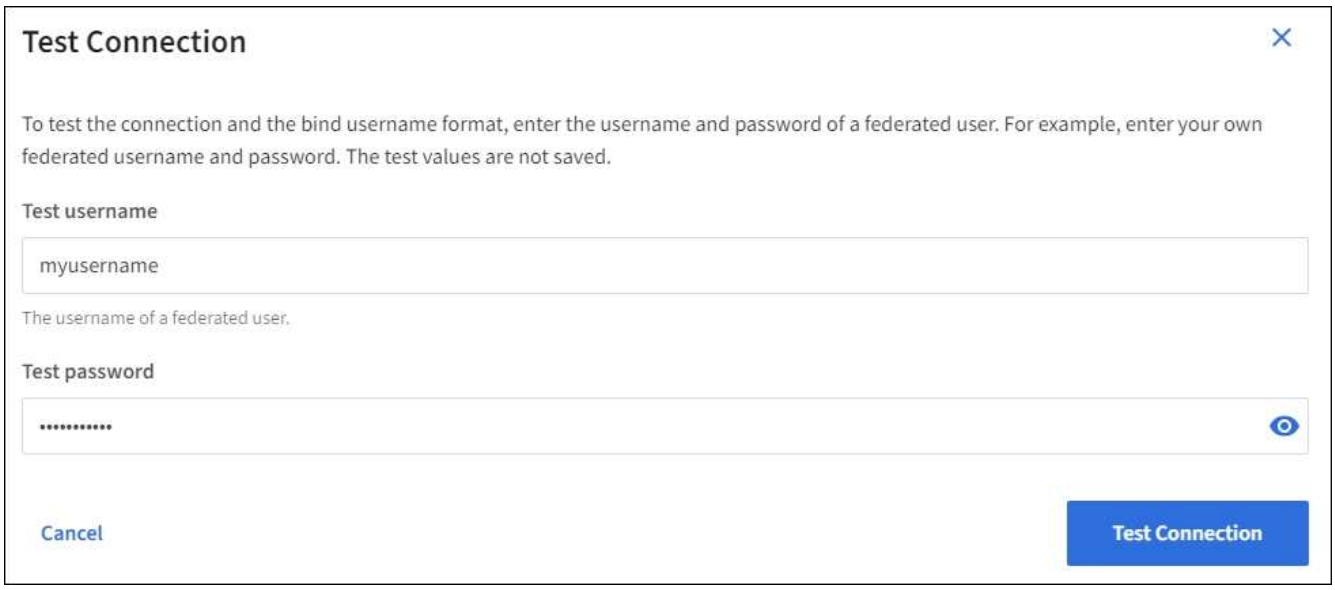
Pasos

1. Seleccione **probar conexión**.
2. Si no proporcionó un formato de nombre de usuario vinculado:
   - Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.

- Si la configuración de conexión no es válida, aparecerá un mensaje que indica que no se ha podido establecer la conexión de prueba. Seleccione **Cerrar**. Luego, resuelva cualquier problema y vuelva a probar la conexión.

3. Si proporcionó un formato de nombre de usuario de enlace, introduzca el nombre de usuario y la contraseña de un usuario federado válido.

   Por ejemplo, introduzca su propio nombre de usuario y contraseña. No incluya ningún carácter especial en el nombre de usuario, como @ o /.



   - Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.
   - Aparecerá un mensaje de error si las opciones de conexión, el formato de nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva los problemas y vuelva a probar la conexión.

Forzar la sincronización con el origen de identidades

El sistema StorageGRID sincroniza periódicamente grupos federados y usuarios del origen de identidades. Puede forzar el inicio de la sincronización si desea habilitar o restringir los permisos de usuario lo antes posible.

Pasos

1. Vaya a la página federación de identidades.
2. Seleccione **servidor de sincronización** en la parte superior de la página.

   El proceso de sincronización puede tardar bastante tiempo en función del entorno.

> La alerta **fallo de sincronización de la federación de identidades** se activa si hay un problema al sincronizar grupos federados y usuarios del origen de identidades.

Deshabilitar la federación de identidades

Puede deshabilitar temporal o permanentemente la federación de identidad para grupos y usuarios. Cuando la federación de identidad está deshabilitada, no hay comunicación entre StorageGRID y la fuente de identidad.

Sin embargo, cualquier configuración que haya realizado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidad en el futuro.

Acerca de esta tarea

Antes de deshabilitar la federación de identidades, debe tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que hayan iniciado sesión en ese momento, retendrán el acceso al sistema StorageGRID hasta que caduque la sesión, pero no podrán iniciar sesión después de que caduque la sesión.
- No se producirá sincronización entre el sistema StorageGRID y la fuente de identidad, y no se generarán alertas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Habilitar federación de identidad** está deshabilitada si el estado de inicio de sesión único (SSO) es **Habilitado** o **Modo Sandbox**. El estado de SSO en la página de inicio de sesión único debe ser **Deshabilitado** antes de poder deshabilitar la federación de identidad. Ver "Desactive el inicio de sesión único" .

Pasos

1. Vaya a la página federación de identidades.
2. Desmarque la casilla de verificación **Habilitar federación de identidad**.

Instrucciones para configurar un servidor OpenLDAP

Si desea utilizar un servidor OpenLDAP para la federación de identidades, debe configurar ajustes específicos en el servidor OpenLDAP.

> Para las fuentes de identidad que no sean Active Directory o Microsoft Entra ID, StorageGRID no bloqueará automáticamente el acceso a S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine todas las claves S3 del usuario o elimine el usuario de todos los grupos.

Revestimientos memberOf y reft

Se deben habilitar las superposiciones memberof y reft. Para obtener más información, consulte las instrucciones para invertir el mantenimiento de los miembros del grupo en la "Documentación de OpenLDAP: Guía del administrador de la versión 2.4"sección .

Indización

Debe configurar los siguientes atributos OpenLDAP con las palabras clave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Además, asegúrese de que los campos mencionados en la ayuda para Nombre de usuario estén indexados para un rendimiento óptimo.

Consulte la información sobre el mantenimiento inverso de miembros de grupo en la "Documentación de

OpenLDAP: Guía del administrador de la versión 2.4".

Gestione los grupos de administradores

Es posible crear grupos de administración para gestionar los permisos de seguridad de uno o más usuarios de administrador. Los usuarios deben pertenecer a un grupo para tener acceso al sistema StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Cree un grupo de administración

Los grupos de administración permiten determinar a qué usuarios se puede acceder a qué características y operaciones en Grid Manager y en la API de gestión de grid.

Acceda al asistente

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Grupos de administradores**.
2. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

- Cree un grupo local si desea asignar permisos a los usuarios locales.
- Cree un grupo federado para importar usuarios desde el origen de identidades.

Grupo local

Pasos

1. Seleccione **Grupo local**.
2. Introduzca un nombre para mostrar para el grupo, que puede actualizar más adelante si es necesario. Por ejemplo, «Usuarios de mantenimiento» o «Administradores de ILM».
3. Introduzca un nombre único para el grupo, que no podrá actualizar más tarde.
4. Seleccione **continuar**.

Grupo federado

Pasos

1. Seleccione **Grupo federado**.
2. Introduzca el nombre del grupo que desea importar, exactamente como aparece en el origen de identidad configurado.
   - Para Active Directory y Microsoft Entra ID, utilice sAMAccountName.
   - Para OpenLDAP, utilice CN (Nombre común).
   - Para otro LDAP, utilice el nombre exclusivo adecuado para el servidor LDAP.
3. Seleccione **continuar**.

Administrar permisos de grupo

Pasos

1. En **modo de acceso**, seleccione si los usuarios del grupo pueden cambiar la configuración y realizar operaciones en Grid Manager y la API de gestión de grid o si sólo pueden ver la configuración y las características.
   - **Read-write** (predeterminado): Los usuarios pueden cambiar la configuración y realizar las operaciones permitidas por sus permisos de administración.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en Grid Manager o la API de administración de grid. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

     Si un usuario pertenece a varios grupos y cualquier grupo está establecido en **sólo lectura**, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

2. Seleccione una o más "permisos de grupo de administración".

   Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenezcan al grupo no podrán iniciar sesión en StorageGRID.

3. Si está creando un grupo local, seleccione **continuar**. Si está creando un grupo federado, seleccione **Crear grupo** y **Finalizar**.

Añadir usuarios (sólo grupos locales)

Pasos

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.

Si todavía no ha creado usuarios locales, puede guardar el grupo sin agregar usuarios. Puede agregar este grupo al usuario en la página usuarios. Consulte "Gestionar usuarios" para obtener más información.

2. Seleccione **Crear grupo** y **Finalizar**.

Consulte y edite los grupos de administración

Puede ver los detalles de los grupos existentes, modificar un grupo o duplicar un grupo.

- Para ver información básica de todos los grupos, revise la tabla de la página grupos.
- Para ver todos los detalles de un grupo específico o editar un grupo, utilice el menú **acciones** o la página de detalles.

Tarea	Menú Actions	Detalles
Ver detalles del grupo	a. Seleccione la casilla de verificación para el grupo. b. Seleccione **acciones** > **Ver detalles del grupo**.	Seleccione el nombre del grupo en la tabla.
Editar nombre para mostrar (sólo grupos locales)	a. Seleccione la casilla de verificación para el grupo. b. Seleccione **acciones** > **Editar nombre de grupo**. c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del grupo para mostrar los detalles. b. Seleccione el icono de edición . c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.
Edite el modo de acceso o los permisos	a. Seleccione la casilla de verificación para el grupo. b. Seleccione **acciones** > **Ver detalles del grupo**. c. Si lo desea, cambie el modo de acceso del grupo. d. Si lo desea, seleccione o desactive "permisos de grupo de administración". e. Seleccione **Guardar cambios**.	a. Seleccione el nombre del grupo para mostrar los detalles. b. Si lo desea, cambie el modo de acceso del grupo. c. Si lo desea, seleccione o desactive "permisos de grupo de administración". d. Seleccione **Guardar cambios**.

Duplicar un grupo

Pasos

1. Seleccione la casilla de verificación para el grupo.
2. Seleccione **acciones** > **Duplicar grupo**.
3. Complete el asistente para grupos duplicados.

Eliminar un grupo

Es posible eliminar un grupo de administración cuando se desea quitar el grupo del sistema y quitar todos los permisos asociados con el grupo. Al eliminar un grupo de administración, se quitan todos los usuarios del grupo, pero no se eliminan los usuarios.

Pasos

1. En la página Groups, seleccione la casilla de comprobación de cada grupo que desea quitar.
2. Seleccione **acciones** > **Eliminar grupo**.
3. Seleccione **Eliminar grupos**.

Permisos de grupo de administradores

Al crear grupos de usuarios de administrador, debe seleccionar uno o más permisos para controlar el acceso a funciones específicas de Grid Manager. A continuación, puede asignar cada usuario a uno o varios de estos grupos de administración para determinar qué tareas puede realizar el usuario.

Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios pertenecientes a ese grupo no podrán iniciar sesión en Grid Manager o en la API de gestión de grid.

De forma predeterminada, cualquier usuario que pertenezca a un grupo que tenga al menos un permiso puede realizar las siguientes tareas:

- Inicie sesión en Grid Manager
- Vea la consola
- Puede ver las páginas Nodes
- Ver las alertas actuales y resueltas
- Cambiar su propia contraseña (sólo usuarios locales)
- Ver cierta información proporcionada en las páginas de configuración y mantenimiento

Interacción entre permisos y modo de acceso

Para todos los permisos, la configuración del **modo de acceso** del grupo determina si los usuarios pueden cambiar la configuración y realizar operaciones o si sólo pueden ver la configuración y las características relacionadas. Si un usuario pertenece a varios grupos y cualquier grupo está establecido en **sólo lectura**, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

En las siguientes secciones se describen los permisos que se pueden asignar al crear o editar un grupo de administradores. Cualquier funcionalidad que no se haya mencionado explícitamente requiere el permiso **acceso raíz**.

Acceso raíz

Este permiso proporciona acceso a todas las funciones de administración de grid.

Cambiar la contraseña raíz del inquilino

Este permiso proporciona acceso a la opción **Cambiar contraseña raíz** de la página arrendatarios, lo que le permite controlar quién puede cambiar la contraseña del usuario raíz local del arrendatario. Este permiso

también se usa para migrar claves S3 cuando se habilita la función de importación de claves S3. Los usuarios que no tienen este permiso no pueden ver la opción **Cambiar contraseña raíz**.

> Para conceder acceso a la página arrendatarios, que contiene la opción **Cambiar contraseña root**, también asigne el permiso **Cuentas de arrendatario**.

ILM

Este permiso permite acceder a las siguientes opciones del menú **ILM**:

- Bases de datos
- Normativas
- Etiquetas de políticas
- Pools de almacenamiento
- Grados de almacenamiento
- Regiones
- Búsqueda de metadatos de objetos

> Los usuarios deben tener el permiso **Otra configuración de red** para administrar los niveles de almacenamiento.

Mantenimiento

Los usuarios deben tener permiso de mantenimiento para utilizar estas opciones:

- **Configuración** > **Control de acceso**:
  - Contraseñas de grid
- **Configuración** > **Red**:
  - Nombres de dominio de punto final S3
- **Mantenimiento** > **Tareas**:
  - Retirada
  - Expansión
  - Comprobación de existencia de objeto
  - Recuperación
- **Mantenimiento** > **Sistema**:
  - Paquete de recuperación
  - Actualización de software
- **Soporte** > **Herramientas**:
  - Registros

Los usuarios que no tienen el permiso de mantenimiento pueden ver, pero no editar, estas páginas:

- **Mantenimiento** > **Red**:
  - Servidores DNS

    - Red Grid
    - Servidores NTP
- **Mantenimiento** > **Sistema**:
    - Licencia
- **Configuración** > **Red**:
    - Nombres de dominio de punto final S3
- **Configuración** > **Seguridad**:
    - Certificados
- **Configuración** > **Monitoreo**:
    - Servidor de auditoría y syslog

Gestionar alertas

Este permiso proporciona acceso a opciones para gestionar alertas. Los usuarios deben tener este permiso para gestionar las silencios, las notificaciones de alerta y las reglas de alerta.

Consulta de métricas

Este permiso proporciona acceso a:

- Página **Soporte** > **Herramientas** > **Métricas**
- Consultas personalizadas de métricas de Prometheus utilizando la sección **Metrics** de la API de administración de grid
- Tarjetas del panel de control de Grid Manager que contienen métricas

Búsqueda de metadatos de objetos

Este permiso proporciona acceso a la página **ILM** > **Búsqueda de metadatos de objetos**.

Otra configuración de cuadrícula

Este permiso proporciona acceso a estas opciones de configuración de cuadrícula adicionales:

- **ILM**:
    - Grados de almacenamiento
- **Configuración** > **Sistema**:
- **Soporte** > **Otros**:
    - Coste del enlace

Administrador de dispositivos de almacenamiento

Este permiso proporciona:

- Acceso al SANtricity System Manager de E-Series en dispositivos de almacenamiento a través de Grid Manager.
- La capacidad de realizar tareas de solución de problemas y mantenimiento en la pestaña Gestionar unidades para los dispositivos que admiten estas operaciones.

Cuentas de inquilino

Este permiso permite:

- Acceda a la página Tenedores, donde puede crear, editar y eliminar cuentas de arrendatario
- Ver las políticas de clasificación de tráfico existentes
- Ver tarjetas de consola de Grid Manager que contienen detalles de arrendatario

Gestionar usuarios

Es posible ver usuarios locales y federados. También puede crear usuarios locales y asignarles grupos de administración locales para determinar a qué funciones de Grid Manager pueden acceder estos usuarios.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "permisos de acceso específicos".

Cree un usuario local

Es posible crear uno o varios usuarios locales y asignar cada usuario a uno o varios grupos locales. Los permisos del grupo controlan a qué funciones de Grid Manager y la API de gestión de grid puede acceder el usuario.

Solo es posible crear usuarios locales. Utilice el origen de identidades externo para administrar grupos y usuarios federados.

Grid Manager incluye un usuario local predefinido, denominado «root». No puede eliminar el usuario root.

> Si el inicio de sesión único (SSO) está activado, los usuarios locales no pueden iniciar sesión en StorageGRID.

Acceda al asistente

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Usuarios administradores**.
2. Seleccione **Crear usuario**.

Introduzca las credenciales de usuario

Pasos

1. Introduzca el nombre completo del usuario, un nombre de usuario único y una contraseña.
2. Opcionalmente, seleccione **Sí** si este usuario no debe tener acceso a Grid Manager o a la API de gestión de grid.
3. Seleccione **continuar**.

Asignar a grupos

Pasos

1. Opcionalmente, asigne el usuario a uno o más grupos para determinar los permisos del usuario.

Si aún no ha creado grupos, puede guardar el usuario sin seleccionar grupos. Puede agregar este usuario a un grupo en la página grupos.

Si un usuario pertenece a varios grupos, los permisos son acumulativos. Consulte "Gestione los grupos de administradores" para obtener más información.

2. Seleccione **Crear usuario** y seleccione **Finalizar**.

Ver y editar usuarios locales

Es posible ver detalles de los usuarios locales y federados existentes. Es posible modificar un usuario local para cambiar el nombre completo, la contraseña o la pertenencia a grupos del usuario. También puede impedir temporalmente que un usuario acceda a Grid Manager y a la API de gestión de grid.

Solo puede editar usuarios locales. Utilice el origen de identidad externo para administrar usuarios federados.

- Para ver la información básica de todos los usuarios locales y federados, revise la tabla en la página Users.
- Para ver todos los detalles de un usuario específico, editar un usuario local o cambiar la contraseña de un usuario local, utilice el menú **acciones** o la página de detalles.

  Las modificaciones se aplican la próxima vez que el usuario cierre sesión y vuelva a acceder al Gestor de cuadrícula.

> Los usuarios locales pueden cambiar sus propias contraseñas usando la opción **Cambiar contraseña** en el banner de Grid Manager.

Tarea	Menú Actions	Detalles
Ver los detalles del usuario	a. Seleccione la casilla de control para el usuario. b. Seleccione **acciones** > **Ver detalles del usuario**.	Seleccione el nombre del usuario en la tabla.
Editar nombre completo (sólo usuarios locales)	a. Seleccione la casilla de control para el usuario. b. Seleccione **acciones** > **Editar nombre completo**. c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione el icono de edición . c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.

Tarea	Menú Actions	Detalles
Denegar o permitir el acceso a StorageGRID	a. Seleccione la casilla de control para el usuario. b. Seleccione **acciones** > **Ver detalles del usuario**. c. Seleccione la pestaña Access. d. Seleccione **Sí** para evitar que el usuario inicie sesión en Grid Manager o en la API de gestión de grid, o seleccione **no** para permitir que el usuario inicie sesión. e. Seleccione **Guardar cambios**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la pestaña Access. c. Seleccione **Sí** para evitar que el usuario inicie sesión en Grid Manager o en la API de gestión de grid, o seleccione **no** para permitir que el usuario inicie sesión. d. Seleccione **Guardar cambios**.
Cambiar contraseña (solo usuarios locales)	a. Seleccione la casilla de control para el usuario. b. Seleccione **acciones** > **Ver detalles del usuario**. c. Seleccione la ficha Contraseña. d. Introduzca una contraseña nueva. e. Seleccione **Cambiar contraseña**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la ficha Contraseña. c. Introduzca una contraseña nueva. d. Seleccione **Cambiar contraseña**.
Cambiar grupos (sólo usuarios locales)	a. Seleccione la casilla de control para el usuario. b. Seleccione **acciones** > **Ver detalles del usuario**. c. Seleccione la ficha grupos. d. Opcionalmente, seleccione el vínculo después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del explorador. e. Seleccione **Editar grupos** para seleccionar diferentes grupos. f. Seleccione **Guardar cambios**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la ficha grupos. c. Opcionalmente, seleccione el vínculo después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del explorador. d. Seleccione **Editar grupos** para seleccionar diferentes grupos. e. Seleccione **Guardar cambios**.

Importar usuarios federados

Puede importar uno o más usuarios federados, hasta un máximo de 100 usuarios, directamente a la página Usuarios.

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Usuarios administradores**.
2. Seleccione **Importar usuarios federados**.
3. Introduzca el UUID o nombre de usuario de uno o más usuarios federados.

Para entradas múltiples, agregue cada UUID o nombre de usuario en una nueva línea.

4. Seleccione **Importar**.

   Si la importación al campo Usuarios falla para uno o más usuarios, realice los siguientes pasos:

   a. Expande **Usuarios no importados** y selecciona **Copiar usuarios**.
   b. Vuelva a intentar la importación seleccionando **Anterior** y pegando los usuarios copiados en el cuadro de diálogo **Importar usuarios federados**.

   Después de cerrar el cuadro de diálogo **Importar usuarios federados**, la información del usuario federado se muestra en la página Usuarios para los usuarios importados correctamente.

Duplique un usuario

Puede duplicar un usuario existente para crear un nuevo usuario con los mismos permisos.

Pasos

1. Seleccione la casilla de control para el usuario.
2. Seleccione **acciones** > **Duplicar usuario**.
3. Complete el asistente Duplicar usuario.

Eliminar un usuario

Puede eliminar un usuario local para eliminar de forma permanente ese usuario del sistema.

> No puede eliminar el usuario root.

Pasos

1. En la página Usuarios, seleccione la casilla de verificación de cada usuario que desee eliminar.
2. Seleccione **acciones** > **Eliminar usuario**.
3. Seleccione **Eliminar usuario**.

Utilizar inicio de sesión único (SSO)

Cómo funciona el SSO

Cuando el inicio de sesión único (SSO) está habilitado, los usuarios pueden acceder a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API solo si sus credenciales están autorizadas mediante el proceso de inicio de sesión SSO implementado por su organización. Los usuarios locales no pueden iniciar sesión en StorageGRID.

El sistema StorageGRID admite el inicio de sesión único (SSO) con el estándar de lenguaje de marcado de aserción de seguridad 2.0 (SAML 2.0).

Antes de habilitar el inicio de sesión único (SSO), revise cómo se ven afectados los procesos de inicio de sesión y cierre de sesión de StorageGRID cuando se habilita SSO.

Inicie sesión cuando SSO esté habilitado

Cuando se habilita SSO y usted inicia sesión en StorageGRID, se le redirigirá a la página SSO de su organización para validar sus credenciales.

Pasos

1. Introduzca el nombre de dominio o la dirección IP completos de cualquier nodo de administración de StorageGRID en un navegador web.

   Aparece la página Inicio de sesión de StorageGRID.

   - Si es la primera vez que accede a la URL en este navegador, se le solicitará un ID de cuenta.
   - Si ya ha accedido al Administrador de red o al Administrador de inquilinos, se le solicitará que seleccione una cuenta reciente o que ingrese un ID de cuenta.

   > La página de inicio de sesión de StorageGRID no se muestra cuando se introduce la dirección URL completa para una cuenta de inquilino (es decir, un nombre de dominio completo o una dirección IP seguida de `/?accountId=20-digit-account-id`). En su lugar, se le redirigirá inmediatamente a la página de inicio de sesión de SSO de su organización, donde puede Inicie sesión con sus credenciales de SSO.

2. Indique si desea acceder al administrador de grid o al responsable de inquilinos:
   - Para acceder a Grid Manager, deje el campo **ID de cuenta** en blanco, introduzca **0** como ID de cuenta o seleccione **Gestor de cuadrícula** si aparece en la lista de cuentas recientes.
   - Para acceder al Administrador de arrendatarios, introduzca el ID de cuenta de arrendatario de 20 dígitos o seleccione un arrendatario por nombre si aparece en la lista de cuentas recientes.
3. Seleccione **Iniciar sesión**

   StorageGRID le redirige a la página de inicio de sesión con SSO de su organización. Por ejemplo:

4. inicia sesión con sus credenciales de SSO.

   Si sus credenciales de SSO son correctas:

   a. El proveedor de identidades (IDP) ofrece una respuesta de autenticación a StorageGRID.
   b. StorageGRID valida la respuesta de autenticación.
   c. Si la respuesta es válida y pertenece a un grupo federado con permisos de acceso a StorageGRID, se ha iniciado sesión en el Gestor de grid o el Gestor de inquilinos, según la cuenta seleccionada.

   > Si no se puede acceder a la cuenta de servicio, puede iniciar sesión siempre que sea un usuario existente que pertenezca a un grupo federado con permisos de acceso StorageGRID.

5. Opcionalmente, acceda a otros nodos de administración o acceda al administrador de grid o al administrador de inquilinos, si dispone de los permisos adecuados.

   No es necesario volver a introducir las credenciales de SSO.

Cierre sesión cuando SSO esté habilitado

Cuando se habilita SSO en StorageGRID, lo que sucede cuando se inicia sesión depende de lo que se haya iniciado sesión y del lugar en el que se está cerrando sesión.

Pasos

1. Localice el enlace **Sign Out** en la esquina superior derecha de la interfaz de usuario.
2. Selecciona **Cerrar sesión**.

   Aparece la página Inicio de sesión de StorageGRID. La lista desplegable **Cuentas recientes** se actualiza para incluir **Grid Manager** o el nombre del inquilino, por lo que puede acceder a estas interfaces de usuario más rápidamente en el futuro.

La tabla resume lo que sucede cuando se inicia sesión si está utilizando una sola sesión del navegador. Si ha iniciado sesión en StorageGRID en varias sesiones de explorador, debe cerrar la sesión en todas las sesiones de explorador por separado.

Si ha iniciado sesión en…	Y salir de…	Se ha cerrado sesión en…
Grid Manager en uno o varios nodos de administrador	Grid Manager en cualquier nodo de administrador	Grid Manager en todos los nodos de administración **Nota:** Si usa Entra ID para SSO, puede que tome algunos minutos cerrar sesión en todos los nodos de administración.
Administrador de inquilinos en uno o varios nodos de administrador	Inquilino Manager en cualquier nodo de administrador	Administrador de inquilinos en todos los nodos de administrador
Tanto Grid Manager como Inquilino Manager	Administrador de grid	Sólo Grid Manager. También debe cerrar sesión en el Administrador de inquilinos para cerrar la sesión de SSO.

Requisitos y consideraciones para SSO

Antes de activar el inicio de sesión único (SSO) para un sistema StorageGRID, revise los requisitos y consideraciones.

Requisitos del proveedor de identidades

StorageGRID admite los siguientes proveedores de identidad de SSO (IDP):

- Servicio de Federación de Active Directory (AD FS)
- Identificador de Microsoft Entra
- PingFederate

Debe configurar la federación de identidades para el sistema StorageGRID antes de poder configurar un

proveedor de identidades SSO. El tipo de servicio LDAP que utiliza para controlar la federación de identidades qué tipo de SSO puede implementar.

Se ha configurado el tipo de servicio LDAP	Opciones para el proveedor de identidades SSO
Active Directory	• Active Directory • Identificación de entrada • PingFederate
Identificación de entrada	Identificación de entrada

Requisitos DE AD FS

Puede utilizar cualquiera de las siguientes versiones de AD FS:

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

Windows Server 2016 debe utilizar "Actualización KB3201845" , o superior.

Requisitos adicionales

- Seguridad de la capa de transporte (TLS) 1.2 ó 1.3
- Microsoft .NET Framework, versión 3.5.1 o posterior

Consideraciones para Entra ID

Si utiliza Entra ID como tipo de SSO y los usuarios tienen nombres principales de usuario que no utilizan sAMAccountName como prefijo, pueden surgir problemas de inicio de sesión si StorageGRID pierde su conexión con el servidor LDAP. Para permitir que los usuarios inicien sesión, debe restaurar la conexión al servidor LDAP.

Requisitos de certificado de servidor

De forma predeterminada, StorageGRID utiliza un certificado de interfaz de administración en cada nodo de administración para proteger el acceso al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos. Cuando configura relaciones de confianza de usuario confiable (AD FS), aplicaciones empresariales (Entra ID) o conexiones de proveedor de servicios (PingFederate) para StorageGRID, utiliza el certificado del servidor como certificado de firma para las solicitudes de StorageGRID .

Si aún no lo ha hecho"se configuró un certificado personalizado para la interfaz de gestión", debería hacerlo ahora. Cuando instala un certificado de servidor personalizado, se utiliza para todos los nodos de administrador y puede usarlo en todas las confianzas de parte que dependen de StorageGRID, aplicaciones de empresa o conexiones del SP.

No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en la confianza de una parte que confía, la aplicación de empresa o la conexión de SP. Si el nodo falla y lo recupera, se genera un nuevo certificado de servidor predeterminado. Antes de iniciar sesión en el nodo recuperado, debe actualizar la confianza de la parte que confía, la aplicación de empresa o la conexión del SP con el nuevo certificado.

Para acceder al certificado de servidor de un nodo de administración, inicie sesión en el shell de comandos del nodo y vaya al `/var/local/mgmt-api` directorio. Se denomina a un certificado de servidor personalizado `custom-server.crt` . El certificado de servidor predeterminado del nodo se denomina `server.crt`.

Requisitos de puertos

El inicio de sesión único (SSO) no está disponible en los puertos de administrador de grid restringido o de administrador de inquilinos. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único. Consulte "Controle el acceso a un firewall externo".

Confirmar que los usuarios federados pueden iniciar sesión

Antes de habilitar el inicio de sesión único (SSO), debe confirmar que al menos un usuario federado puede iniciar sesión en Grid Manager y en el Gestor de inquilinos para cualquier cuenta de inquilino existente.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Ya ha configurado la federación de identidades.

Pasos

1. Si hay cuentas de inquilino existentes, confirme que ninguno de los inquilinos utiliza su propio origen de identidad.

   Al habilitar SSO, el origen de identidad configurado en el Administrador de inquilinos se anula mediante el origen de identidades configurado en Grid Manager. Los usuarios que pertenezcan al origen de identidad del arrendatario ya no podrán iniciar sesión a menos que tengan una cuenta con el origen de identidad de Grid Manager.

   a. Inicie sesión en el Administrador de arrendatarios para cada cuenta de arrendatario.
   b. Seleccione **Administración de acceso** > **Federación de identidades**.
   c. Confirme que la casilla de verificación **Habilitar federación de identidad** no está seleccionada.
   d. Si lo es, confirme que los grupos federados que puedan estar en uso para esta cuenta de inquilino ya no son necesarios, desactive la casilla de verificación y seleccione **Guardar**.

2. Confirme que un usuario federado puede acceder a Grid Manager:
   a. Desde Grid Manager, seleccione **Configuración** > **Control de acceso** > **Grupos de administración**.
   b. Asegúrese de que al menos un grupo federado se ha importado del origen de identidad de Active Directory y de que se le ha asignado el permiso acceso raíz.
   c. Cierre la sesión.

d. Confirme que puede volver a iniciar sesión en Grid Manager como usuario en el grupo federado.

3. Si hay cuentas de inquilino existentes, confirme que un usuario federado con permiso de acceso raíz puede iniciar sesión:
   a. Desde el Administrador de red, seleccione **Inquilinos**.
   b. Seleccione la cuenta de arrendatario y seleccione **acciones** > **Editar**.
   c. En la ficha introducir detalles, seleccione **continuar**.
   d. Si la casilla de verificación **Usar fuente de identidad propia** está seleccionada, desmarque la casilla y seleccione **Guardar**.

      Aparece la página inquilino.

   e. Seleccione la cuenta de arrendatario, seleccione **Iniciar sesión** e inicie sesión en la cuenta de arrendatario como usuario raíz local.
   f. Desde el Administrador de inquilinos, seleccione **Administración de acceso** > **Grupos**.
   g. Asegúrese de que al menos un grupo federado de Grid Manager ha sido asignado el permiso de acceso raíz para este arrendatario.
   h. Cierre la sesión.
   i. Confirme que puede volver a iniciar sesión en el inquilino como usuario en el grupo federado.

Información relacionada

- "Requisitos y consideraciones para el inicio de sesión único"
- "Gestione los grupos de administradores"
- "Usar una cuenta de inquilino"

Configurar SSO

Puede seguir el asistente de configuración de SSO e ingresar al modo sandbox para configurar y probar el inicio de sesión único (SSO) antes de habilitarlo para todos los usuarios de StorageGRID . Una vez habilitado el SSO, puede regresar al modo sandbox cuando sea necesario para cambiar o volver a probar la configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".
- Configuró la federación de identidades para el sistema StorageGRID.
- Para la federación de identidad **tipo de servicio LDAP**, seleccionó Active Directory o Entra ID, según el proveedor de identidad SSO que planea utilizar.

Se ha configurado el tipo de servicio LDAP	Opciones para el proveedor de identidades SSO
Servicio de Federación de Active Directory (AD FS)	• Active Directory • Identificación de entrada • PingFederate

Se ha configurado el tipo de servicio LDAP	Opciones para el proveedor de identidades SSO
Identificación de entrada	Identificación de entrada

Acerca de esta tarea

Cuando se habilita el inicio de sesión único y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidades de SSO. A su vez, el proveedor de identidades SSO envía una respuesta de autenticación a StorageGRID para indicar si la solicitud de autenticación se ha realizado correctamente. Para solicitudes correctas:

- La respuesta de Active Directory o PingFederate incluye un identificador único universal (UUID) para el usuario.
- La respuesta de Entra ID incluye un nombre principal de usuario (UPN).

Para permitir que StorageGRID (el proveedor de servicios) y el proveedor de identidad SSO se comuniquen de forma segura acerca de las solicitudes de autenticación de usuarios, deberá completar estas tareas:

1. Configurar ajustes en StorageGRID.
2. Utilice el software del proveedor de identidad SSO para crear una relación de confianza entre usuarios (AD FS), una aplicación empresarial (Entra ID) o un proveedor de servicios (PingFederate) para cada nodo de administración.
3. Regrese a StorageGRID para habilitar SSO.

El modo Sandbox facilita la realización de esta configuración de ida y vuelta y permite probar todas las configuraciones antes de habilitar SSO. Cuando se utiliza el modo sandbox, los usuarios no pueden iniciar sesión mediante SSO.

Acceda al asistente

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Inicio de sesión único**. Aparece la página de inicio de sesión único.

> Si el botón Configurar ajustes de SSO está deshabilitado, confirme que haya configurado el proveedor de identidad como fuente de identidad federada. Consulte "Requisitos y consideraciones para el inicio de sesión único" .

2. Seleccione **Configurar ajustes de SSO**. Aparece la página Proporcionar detalles del proveedor de identidad.

Proporcionar detalles del proveedor de identidad

Pasos

1. Seleccione **Tipo SSO** en la lista desplegable.
2. Si seleccionó Active Directory como tipo de SSO, ingrese el **Nombre del servicio de federación** para el proveedor de identidad, exactamente como aparece en el Servicio de federación de Active Directory (AD FS).

Para buscar el nombre del servicio de federación, vaya al Administrador de Windows Server. Seleccione **Herramientas** > **Administración AD FS**. En el menú Acción, seleccione **Editar propiedades del servicio de Federación**. El nombre del servicio de Federación se muestra en el segundo campo.

3. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidades envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID.
   - **Utilizar certificado CA** del sistema operativo: Utilice el certificado CA predeterminado instalado en el sistema operativo para asegurar la conexión.
   - **Utilizar certificado de CA personalizado**: Utilice un certificado de CA personalizado para proteger la conexión.

     Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.
   - **No utilice TLS**: No utilice un certificado TLS para garantizar la conexión.

     Si cambia el certificado de CA, inmediatamente "Reinicie el servicio mgmt-api en los nodos de administración" y prueba un SSO correcto en Grid Manager.
4. Seleccione **Continuar**. Aparece la página Proporcionar identificador de parte confiable.

Proporcionar identificador de parte confiable

1. Complete los campos en la página Proporcionar identificador de parte confiable según el tipo de SSO que haya seleccionado.

Active Directory

a. Especifique el **Identificador de la parte confiada** para StorageGRID. Este valor controla el nombre que utiliza para cada relación de confianza de usuario confiable en AD FS.

   - Por ejemplo, si el grid solo tiene un nodo de administración y no prevé agregar más nodos de administración en el futuro, introduzca `SG` o `StorageGRID`.
   - Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]` . Al incluir esta cadena, se genera una tabla que muestra el identificador de la parte confiable para cada nodo de administración en la cuadrícula, según el nombre de host del nodo.

   > Debe crear una confianza de parte de confianza para cada nodo de administrador en el sistema StorageGRID. Tener una confianza de parte que confía en cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura desde y hacia cualquier nodo de administración.

b. Seleccione **Guardar e ingresar al modo sandbox**.

Identificación de entrada

a. En la sección Aplicación empresarial, especifique el **nombre de la aplicación empresarial** para StorageGRID. Este valor controla el nombre que utiliza para cada aplicación empresarial en Entra ID.

   - Por ejemplo, si el grid solo tiene un nodo de administración y no prevé agregar más nodos de administración en el futuro, introduzca `SG` o `StorageGRID`.
   - Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]` . Al incluir esta cadena, se genera una tabla que muestra un nombre de aplicación empresarial para cada nodo de administración en su sistema, según el nombre de host del nodo.

   > Debe crear una aplicación empresarial para cada nodo administrador en el sistema StorageGRID. Disponer de una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administración.

b. Siga los pasos en"Crear aplicaciones empresariales en Entra ID" para crear una aplicación empresarial para cada nodo de administración enumerado en la tabla.

c. Desde Entra ID, copie la URL de metadatos de federación para cada aplicación empresarial. Luego, pegue esta URL en el campo **URL de metadatos de federación** correspondiente en StorageGRID.

d. Después de haber copiado y pegado una URL de metadatos de federación para todos los nodos de administración, seleccione **Guardar e ingresar al modo sandbox**.

PingFederate

a. En la sección Proveedor de servicios (SP), especifique **ID de conexión SP** para StorageGRID. Este valor controla el nombre que utiliza para cada conexión SP en PingFederate.

   - Por ejemplo, si el grid solo tiene un nodo de administración y no prevé agregar más nodos de administración en el futuro, introduzca `SG` o `StorageGRID`.
   - Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]`

en el identificador. Por ejemplo, `SG-[HOSTNAME]` . Al incluir esta cadena, se genera una tabla que muestra el ID de conexión de SP para cada nodo de administración en su sistema, según el nombre de host del nodo.

> Debe crear una conexión de SP para cada nodo de administrador en el sistema StorageGRID. Tener una conexión de SP para cada nodo de administrador garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administrador.

b. Especifique la dirección URL de metadatos de federación para cada nodo de administración en el campo **URL de metadatos de Federación**.

   Utilice el siguiente formato:

   ```
   https://<Federation Service
   Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
   Connection ID>
   ```

c. Seleccione **Guardar e ingresar al modo sandbox**.

Configurar las confianzas de partes de confianza, las aplicaciones de la empresa o las conexiones de SP

Después de guardar la configuración e ingresar al modo sandbox, puede completar y probar la configuración para el tipo de SSO que seleccionó.

StorageGRID puede permanecer en modo sandbox tanto tiempo como sea necesario. Sin embargo, sólo los usuarios federados y los usuarios locales pueden iniciar sesión.

Active Directory

Pasos

1. Vaya a Servicios de Federación de Active Directory (AD FS).
2. Cree una o más relaciones de confianza de usuario confiable para StorageGRID, utilizando cada identificador de usuario confiable que se muestra en la tabla de la página Configurar SSO.

   Debe crear una confianza para cada nodo de administrador que se muestra en la tabla.

   Para obtener instrucciones, vaya a "Crear confianzas de parte de confianza en AD FS".

Identificación de entrada

Pasos

1. En la página Single Sign-On del nodo de administrador al que ha iniciado sesión actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. A continuación, para cualquier otro nodo de administrador en el grid, repita estos pasos:
   a. Inicie sesión en el nodo.
   b. Seleccione **Configuración** > **Control de acceso** > **Inicio de sesión único**.
   c. Descargue y guarde los metadatos de SAML de ese nodo.
3. Vaya al portal de Azure.
4. Siga los pasos en"Crear aplicaciones empresariales en Entra ID" para cargar el archivo de metadatos SAML para cada nodo de administración en su aplicación empresarial Entra ID correspondiente.

PingFederate

Pasos

1. En la página Single Sign-On del nodo de administrador al que ha iniciado sesión actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. A continuación, para cualquier otro nodo de administrador en el grid, repita estos pasos:
   a. Inicie sesión en el nodo.
   b. Seleccione **Configuración** > **Control de acceso** > **Inicio de sesión único**.
   c. Descargue y guarde los metadatos de SAML de ese nodo.
3. Vaya a PingFederate.
4. "Cree una o varias conexiones de proveedor de servicios (SP) para StorageGRID" . Utilice el ID de conexión de SP para cada nodo de administración (que se muestra en la tabla de la página Configurar SSO) y los metadatos SAML que descargó para ese nodo de administración.

   Debe crear una conexión de SP para cada nodo de administrador que se muestra en la tabla.

Configuración de prueba

Antes de implementar el uso del inicio de sesión único para todo el sistema StorageGRID , confirme que el inicio de sesión único y el cierre de sesión único estén configurados correctamente para cada nodo de administración.

Active Directory

Pasos

1. Desde la página Configurar SSO, busque el enlace en el paso de configuración de prueba del asistente.

   La dirección URL se deriva del valor introducido en el campo **Nombre de servicio de Federación**.

2. Seleccione el enlace, o copie y pegue la URL en un navegador para acceder a la página de inicio de sesión del proveedor de identidades.
3. Para confirmar que puede utilizar SSO para iniciar sesión en StorageGRID, seleccione **Iniciar sesión en uno de los siguientes sitios**, seleccione el identificador de la parte que confía para su nodo de administración principal y seleccione **Iniciar sesión**.
4. Introduzca el nombre de usuario y la contraseña federados.
   - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.
   - Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
5. Repita estos pasos para verificar la conexión SSO para cada nodo de administrador en el grid.

Identificación de entrada

Pasos

1. Vaya a la página Single Sign-On del portal de Azure.
2. Seleccione **probar esta aplicación**.
3. Introduzca las credenciales de un usuario federado.
   - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.
   - Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
4. Repita estos pasos para verificar la conexión SSO para cada nodo de administrador en el grid.

PingFederate

Pasos

1. Desde la página Configurar SSO, seleccione el primer enlace en el mensaje del modo Sandbox.

   Seleccione y pruebe un enlace cada vez.

2. Introduzca las credenciales de un usuario federado.
   - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.
   - Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
3. Seleccione el siguiente enlace para verificar la conexión de SSO para cada nodo de administrador de la cuadrícula.

   Si ve un mensaje Página caducada, seleccione el botón **Atrás** de su explorador y vuelva a enviar sus credenciales.

Active el inicio de sesión único

Una vez que haya confirmado que puede usar SSO para iniciar sesión en cada nodo de administración, puede habilitar SSO en todo el sistema StorageGRID.

> Cuando SSO está habilitado, todos los usuarios deben utilizar SSO para acceder a Grid Manager, al arrendatario Manager, a la API de gestión de grid y a la API de gestión de inquilinos. Los usuarios locales ya no pueden acceder a StorageGRID.

Pasos

1. Desde el paso de configuración de prueba del asistente de configuración de SSO, seleccione **Habilitar SSO**.
2. Revise el mensaje de advertencia y seleccione **Habilitar SSO**.

   El inicio de sesión único ahora está habilitado. Aparece la página de inicio de sesión único y ahora incluye los detalles del SSO que acaba de configurar.

3. Para editar la configuración, seleccione **Editar**.
4. Para deshabilitar el inicio de sesión único, seleccione **Deshabilitar SSO**.

> Si usa Azure Portal y accede a StorageGRID desde la misma computadora que usa para acceder a Entra ID, asegúrese de que el usuario del portal de Azure también sea un usuario autorizado de StorageGRID (un usuario en un grupo federado que se haya importado a StorageGRID o cierre la sesión del portal de Azure antes de intentar iniciar sesión en StorageGRID).

Crear confianzas de parte de confianza en AD FS

Debe utilizar los Servicios de Federación de Active Directory (AD FS) para crear una confianza de parte de confianza para cada nodo de administración del sistema. Puede crear confianzas de parte confiando mediante comandos de PowerShell, importando los metadatos de SAML desde StorageGRID o introduciendo los datos manualmente.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y ha seleccionado **AD FS** como tipo SSO.
- Tienes"entró en modo sandbox" en el Administrador de cuadrícula.
- Conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte confiable para cada nodo de administración en su sistema. Puede encontrar estos valores en la tabla de detalles de Nodos de administración en la página Configurar SSO de StorageGRID .

> Debe crear una confianza de parte de confianza para cada nodo de administrador en el sistema StorageGRID. Tener una confianza de parte que confía en cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura desde y hacia cualquier nodo de administración.

- Tiene experiencia en la creación de confianzas de parte de confianza en AD FS o tiene acceso a la documentación de Microsoft AD FS.
- Está utilizando el complemento Administración de AD FS y pertenece al grupo Administradores.
- Si crea la confianza de la parte de confianza manualmente, tiene el certificado personalizado que se cargó

para la interfaz de gestión de StorageGRID, o sabe cómo iniciar sesión en un nodo de administrador desde el shell de comandos.

Acerca de esta tarea

Estas instrucciones se aplican a Windows Server 2016 AD FS. Si está utilizando una versión diferente de AD FS, notará ligeras diferencias en el procedimiento. Consulte la documentación de Microsoft AD FS si tiene alguna pregunta.

Cree una confianza de parte de confianza mediante Windows PowerShell

Puede utilizar Windows PowerShell para crear rápidamente una o más confianzas de parte que dependan.

Pasos

1. En el menú de inicio de Windows, seleccione con el botón derecho el icono de PowerShell y seleccione **Ejecutar como administrador**.
2. En el símbolo del sistema de PowerShell, introduzca el siguiente comando:

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - Para *Admin_Node_Identifier*, introduzca el identificador de parte de confianza para el nodo de administración, tal y como aparece en la página Conexión Única. Por ejemplo, `SG-DC1-ADM1`.
   - Para *Admin_Node_FQDN*, introduzca el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)
3. En Windows Server Manager, seleccione **Herramientas** > **Administración de AD FS**.

   Aparece la herramienta de administración de AD FS.
4. Seleccione **AD FS** > **fideicomisos de la parte**.

   Aparece la lista de confianzas de parte de confianza.
5. Agregar una directiva de control de acceso a la confianza de parte de confianza recién creada:
   a. Busque la parte de confianza que acaba de crear.
   b. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar directiva de control de acceso**.
   c. Seleccione una Política de control de acceso.
   d. Seleccione **aplicar** y seleccione **Aceptar**
6. Agregar una política de emisión de reclamaciones a la nueva confianza de parte de confianza creada:
   a. Busque la parte de confianza que acaba de crear.
   b. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar política de emisión de reclamaciones**.
   c. Seleccione **Agregar regla**.
   d. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.
   e. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID to Name ID** o **UPN to Name ID**.

f. Para el almacén de atributos, seleccione **Active Directory**.

g. En la columna Atributo LDAP de la tabla de asignación, escriba **objectGUID** o seleccione **User-Principal-Name**.

h. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.

i. Seleccione **Finalizar** y seleccione **Aceptar**.

7. Confirme que los metadatos se han importado correctamente.

a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.

b. Confirme que los campos de las fichas **puntos finales**, **identificadores** y **firma** se han rellenado.

Si faltan los metadatos, confirme que la dirección de metadatos de federación es correcta o introduzca los valores manualmente.

8. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.

9. Cuando haya terminado, regrese a StorageGRID y"Probar todos los fideicomisos de partes confiantes" para confirmar que están configurados correctamente.

Cree una confianza de parte de confianza importando metadatos de federación

Puede importar los valores de cada una de las partes que confía mediante el acceso a los metadatos de SAML de cada nodo de administrador.

Pasos

1. En Windows Server Manager, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.

2. En acciones, seleccione **Agregar confianza de parte de confianza**.

3. En la página de bienvenida, elija **Claims aware** y seleccione **Start**.

4. Seleccione **Importar datos sobre la parte que confía publicada en línea o en una red local**.

5. En **Dirección de metadatos de Federación (nombre de host o URL)**, escriba la ubicación de los metadatos SAML para este nodo de administración:

`https://Admin_Node_FQDN/api/saml-metadata`

Para *`Admin_Node_FQDN`*, introduzca el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

6. Complete el asistente Trust Party Trust, guarde la confianza de la parte que confía y cierre el asistente.

Al introducir el nombre para mostrar, utilice el identificador de parte de confianza para el nodo de administración, exactamente como aparece en la página Single Sign-On en Grid Manager. Por ejemplo, `SG-DC1-ADM1`.

7. Agregar una regla de reclamación:
   a. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar política de emisión de reclamaciones**.
   b. Seleccione **Agregar regla**:
   c. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.
   d. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

      Por ejemplo, **ObjectGUID to Name ID** o **UPN to Name ID**.

   e. Para el almacén de atributos, seleccione **Active Directory**.
   f. En la columna Atributo LDAP de la tabla de asignación, escriba **objectGUID** o seleccione **User-Principal-Name**.
   g. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
   h. Seleccione **Finalizar** y seleccione **Aceptar**.
8. Confirme que los metadatos se han importado correctamente.
   a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.
   b. Confirme que los campos de las fichas **puntos finales**, **identificadores** y **firma** se han rellenado.

      Si faltan los metadatos, confirme que la dirección de metadatos de federación es correcta o introduzca los valores manualmente.

9. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.
10. Cuando haya terminado, regrese a StorageGRID y"Probar todos los fideicomisos de partes confiantes" para confirmar que están configurados correctamente.

Cree una confianza de parte de confianza manualmente

Si elige no importar los datos de las confianzas de la pieza de confianza, puede introducir los valores manualmente.

Pasos

1. En Windows Server Manager, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En acciones, seleccione **Agregar confianza de parte de confianza**.
3. En la página de bienvenida, elija **Claims aware** y seleccione **Start**.
4. Seleccione **introducir datos sobre la parte que confía manualmente** y seleccione **Siguiente**.
5. Complete el asistente Trust Party Trust:
   a. Introduzca un nombre de visualización para este nodo de administración.

      Para obtener coherencia, utilice el identificador de parte de confianza para el nodo de administración, exactamente como aparece en la página de inicio de sesión único en Grid Manager. Por ejemplo, `SG-DC1-ADM1`.

b. Omitir el paso para configurar un certificado de cifrado de token opcional.

c. En la página Configurar URL, seleccione la casilla de verificación **Habilitar soporte para el protocolo WebSSO de SAML 2,0**.

d. Escriba la URL del extremo de servicio SAML para el nodo de administración:

`https://Admin_Node_FQDN/api/saml-response`

Para *Admin_Node_FQDN*, introduzca el nombre de dominio completo para el nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

e. En la página Configurar identificadores, especifique el identificador de parte que confía para el mismo nodo de administración:

Admin_Node_Identifier

Para *Admin_Node_Identifier*, introduzca el identificador de parte de confianza para el nodo de administración, tal y como aparece en la página Conexión Única. Por ejemplo, `SG-DC1-ADM1`.

f. Revise la configuración, guarde la confianza de la parte que confía y cierre el asistente.

Aparecerá el cuadro de diálogo Editar directiva de emisión de reclamaciones.

Si el cuadro de diálogo no aparece, haga clic con el botón derecho del ratón en la confianza y seleccione **Editar directiva de emisión de reclamaciones**.

6. Para iniciar el asistente para reglas de reclamación, seleccione **Agregar regla**:

a. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.

b. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID to Name ID** o **UPN to Name ID**.

c. Para el almacén de atributos, seleccione **Active Directory**.

d. En la columna Atributo LDAP de la tabla de asignación, escriba **objectGUID** o seleccione **User-Principal-Name**.

e. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.

f. Seleccione **Finalizar** y seleccione **Aceptar**.

7. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.

8. En la ficha **endpoints**, configure el extremo para un único cierre de sesión (SLO):

a. Seleccione **Añadir SAML**.

b. Seleccione **Tipo de extremo** > **SAML Logout**.

c. Seleccione **enlace** > **Redirigir**.

d. En el campo **Trusted URL**, introduzca la dirección URL utilizada para cerrar sesión único (SLO) desde este nodo de administración:

`https://Admin_Node_FQDN/api/saml-logout`

Para *Admin_Node_FQDN*, introduzca el nombre de dominio completo del nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

a. Seleccione **OK**.

9. En la ficha **firma**, especifique el certificado de firma para esta confianza de parte de confianza:
   a. Agregue el certificado personalizado:
      - Si posee el certificado de gestión personalizado cargado en StorageGRID, seleccione ese certificado.
      - Si no tiene el certificado personalizado, inicie sesión en el nodo de administración, vaya al `/var/local/mgmt-api` directorio del nodo de administración y agregue el `custom-server.crt` archivo de certificado.

        (`server.crt`No se recomienda utilizar el certificado por defecto del nodo de administración). Si falla el nodo de administración, el certificado predeterminado se regenerará al recuperar el nodo y deberá actualizar la confianza de la parte de confianza.

   b. Seleccione **aplicar** y seleccione **Aceptar**.

      Las propiedades de la parte de confianza se guardan y cierran.

10. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.
11. Cuando haya terminado, regrese a StorageGRID y"Probar todos los fideicomisos de partes confiantes" para confirmar que están configurados correctamente.

Crear aplicaciones empresariales en Entra ID

Utilice Entra ID para crear una aplicación empresarial para cada nodo de administración en su sistema.

Antes de empezar

- Ha comenzado a configurar el inicio de sesión único para StorageGRID y seleccionó **Entra ID** como tipo de SSO.
- Tienes"entró en modo sandbox" en el Administrador de cuadrícula.
- Tiene el **nombre de la aplicación empresarial** para cada nodo de administración en su sistema. Puede copiar estos valores de la tabla de detalles del nodo de administración en la página Configurar SSO.

  Debe crear una aplicación empresarial para cada nodo administrador en el sistema StorageGRID. Disponer de una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administración.

- Tienes experiencia en la creación de aplicaciones empresariales en Entra ID.
- Tienes una cuenta Entra ID con una suscripción activa.

- Tiene uno de los siguientes roles en la cuenta de Entra ID: Administrador global, Administrador de aplicaciones en la nube, Administrador de aplicaciones o propietario de la entidad de servicio.

Acceso Entra ID

Pasos

1. Inicie sesión en el "Portal de Azure".
2. Navegar a "Identificación de entrada" .
3. Seleccione "Aplicaciones de negocio".

Creación de aplicaciones empresariales y guardado de la configuración de SSO de StorageGRID

Para guardar la configuración de SSO para Entra ID en StorageGRID, debe usar Entra ID para crear una aplicación empresarial para cada nodo de administración. Copiará las URL de metadatos de federación de Entra ID y las pegará en los campos **URL de metadatos de federación** correspondientes en la página Configurar SSO.

Pasos

1. Repita los siguientes pasos para cada nodo de administrador.
   a. En el panel de aplicaciones de Entra ID Enterprise, seleccione **Nueva aplicación**.
   b. Seleccione **Crear su propia aplicación**.
   c. Para el nombre, ingrese el **nombre de la aplicación empresarial** que copió de la tabla de detalles del nodo de administración en la página Configurar SSO.
   d. Deje seleccionada la opción **integrar cualquier otra aplicación que no encuentre en la galería (no galería)**.
   e. Seleccione **Crear**.
   f. Seleccione el enlace **Get Started** en **2. Configure el cuadro de inicio de sesión único en** o seleccione el enlace **Single Sign-On** en el margen izquierdo.
   g. Seleccione la casilla **SAML**.
   h. Copie la URL * metadatos de Federación de aplicaciones*, que puede encontrar en **Paso 3 Certificado de firma SAML**.
   i. Vaya a la página Configurar SSO y pegue en el campo **URL de metadatos de federación** la URL que corresponde al **Nombre de la aplicación empresarial** que utilizó.
2. Después de haber pegado una URL de metadatos de federación para cada nodo de administración y realizado todos los demás cambios necesarios en la configuración de SSO, seleccione **Guardar** en la página Configurar SSO.

Descargue los metadatos de SAML para cada nodo de administración

Una vez guardada la configuración de SSO, puede descargar un archivo de metadatos SAML para cada nodo de administrador del sistema StorageGRID.

Pasos

1. Repita estos pasos para cada nodo de administración.
   a. Inicie sesión en StorageGRID desde el nodo de administrador.
   b. Seleccione **Configuración** > **Control de acceso** > **Inicio de sesión único**.
   c. Seleccione el botón para descargar los metadatos de SAML de ese nodo de administración.

d. Guarde el archivo que cargará en Entra ID.

Cargue metadatos de SAML en cada aplicación empresarial

Después de descargar un archivo de metadatos SAML para cada nodo de administración de StorageGRID , realice los siguientes pasos en Entra ID:

Pasos

1. Vuelva al portal de Azure.
2. Repita estos pasos con cada aplicación de empresa:

> Es posible que deba actualizar la página aplicaciones de empresa para ver las aplicaciones que ha agregado anteriormente en la lista.

   a. Vaya a la página Propiedades de la aplicación de empresa.
   b. Establezca **asignación requerida** en **no** (a menos que desee configurar las asignaciones por separado).
   c. Vaya a la página Single Sign-On.
   d. Complete la configuración de SAML.
   e. Seleccione el botón **Upload metadata file** y seleccione el archivo de metadatos SAML que descargó para el nodo de administración correspondiente.
   f. Después de cargar el archivo, seleccione **Guardar** y, a continuación, seleccione **X** para cerrar el panel. Volverá a la página Set up Single Sign-On with SAML.
3. "Pruebe cada aplicación" .

Cree conexiones de proveedores de servicios (SP) en PingFederate

Puede utilizar PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración del sistema. Para acelerar el proceso, importe los metadatos SAML de StorageGRID.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y ha seleccionado **Ping federate** como tipo de SSO.
- Tienes"entró en modo sandbox" en el Administrador de cuadrícula.
- Tienes el *ID de conexión SP * para cada nodo de administración en tu sistema. Puede encontrar estos valores en la tabla de detalles de Nodos de administración en la página Configurar SSO.
- Ha descargado los **metadatos SAML** de cada nodo de administración del sistema.
- Tiene experiencia en la creación de conexiones SP en PingFederate Server.
- Tiene el "Guía de referencia del administrador"servidor FOR PingFederate. La documentación de PingFederate proporciona instrucciones detalladas paso a paso y explicaciones.
- Tú tienes el"Permiso de administrador" para el servidor PingFederate.

Acerca de esta tarea

Estas instrucciones resumen cómo configurar PingFederate Server versión 10.3 como un proveedor SSO para StorageGRID. Si está utilizando otra versión de PingFederate, puede que necesite adaptar estas instrucciones. Consulte la documentación de PingFederate Server para obtener instrucciones detalladas para

su publicación.

Complete los requisitos previos en PingFederate

Antes de poder crear las conexiones SP que utilizará para StorageGRID, debe completar las tareas previas en PingFederate. Utilizará la información de estos requisitos previos al configurar las conexiones del SP.

Crear almacén de datos

Si aún no lo ha hecho, cree un almacén de datos para conectar PingFederate al servidor LDAP de AD FS. Use los valores que utilizó en "configurando la federación de identidades"StorageGRID.

- **Tipo**: Directorio (LDAP)
- **Tipo LDAP**: Active Directory
- **Nombre del atributo binario**: Introduzca **objectGUID** en la ficha atributos binarios LDAP exactamente como se muestra.

Crear validador de credenciales de contraseña

Si todavía no lo ha hecho, cree un validador de credencial de contraseña.

- **Tipo**: Validador de credenciales de nombre de usuario de LDAP
- **Almacén de datos**: Seleccione el almacén de datos que creó.
- **Search base**: Introduzca la información de LDAP (por ejemplo, DC=saml,DC=sgws).
- **Filtro de búsqueda**: SAMAccountName=${username}
- **Ámbito**: Subárbol

Crear instancia de adaptador IDP[[instancia de adaptador]]

Si todavía no lo ha hecho, cree una instancia de adaptador de IDP.

Pasos

1. Vaya a **autenticación** > **integración** > **Adaptadores IDP**.
2. Seleccione **Crear nueva instancia**.
3. En la ficha Tipo, seleccione **adaptador IDP de formulario HTML**.
4. En la ficha adaptador IDP, seleccione **Agregar una nueva fila a 'Validadores de credenciales'**.
5. Seleccione elvalidador de credenciales de contraseña tu creaste
6. En la ficha atributos del adaptador, seleccione el atributo **nombre de usuario** para **seudónimo**.
7. Seleccione **Guardar**.

Crear o importar un certificado de firma[[certificado de firma]]

Si todavía no lo ha hecho, cree o importe el certificado de firma.

Pasos

1. Vaya a **Seguridad** > **claves y certificados de firma y descifrado**.
2. Cree o importe el certificado de firma.

Cree una conexión SP en PingFederate

Cuando crea una conexión del SP en PingFederate, importe los metadatos SAML que ha descargado de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos necesarios.

> Debe crear una conexión de SP para cada nodo de administrador en su sistema de StorageGRID, de modo que los usuarios puedan iniciar sesión desde y hacia cualquier nodo de forma segura. Utilice estas instrucciones para crear la primera conexión del SP. A continuación, vaya a Cree conexiones adicionales del SP para crear las conexiones adicionales que necesite.

Elija el tipo de conexión del SP

Pasos

1. Vaya a **aplicaciones** > **integración** > **conexiones SP**.
2. Seleccione **Crear conexión**.
3. Seleccione **no utilice una plantilla para esta conexión**.
4. Seleccione **Examinador SSO Profiles** y **SAML 2.0** como protocolo.

Importe los metadatos de SP

Pasos

1. En la ficha Importar metadatos, seleccione **Archivo**.
2. Elija el archivo de metadatos SAML que descargó de la página Configurar SSO para el nodo de administración.
3. Revise el resumen de metadatos y la información proporcionada en la pestaña Información general.

   El ID de entidad del partner y el nombre de conexión se establecen en el ID de conexión de StorageGRID SP. (Por ejemplo, 10.96.105.200-DC1-ADM1-105-200). La URL base es la IP del nodo de administrador de StorageGRID.

4. Seleccione **Siguiente**.

Configure el SSO del explorador IDP

Pasos

1. En la ficha SSO del explorador, seleccione **Configurar SSO del explorador**.
2. En la ficha Perfiles de SAML, seleccione las opciones **SSO iniciado por el SP**, **SLO inicial de SP**, **SSO iniciado por IDP** y **SLO iniciado por IDP**.
3. Seleccione **Siguiente**.
4. En la ficha ciclo de vida de las aserción, no realice cambios.
5. En la ficha creación de aserción, seleccione **Configurar creación de aserción**.
   a. En la ficha asignación de identidades, seleccione **Estándar**.
   b. En la ficha Contrato de atributo, utilice el formato **SAML_SUBJECT** como atributo Contract y el formato de nombre no especificado que se importó.
6. Para Extender el contrato, seleccione **Eliminar** para eliminar el `urn:oid`, que no se utiliza.

Asigne la instancia del adaptador

Pasos

1. En la ficha asignación de origen de autenticación, seleccione **asignar nueva instancia de adaptador**.
2. En el separador Instancia de Adaptador, seleccione el instancia del adaptador que ha creado.
3. En la ficha método de asignación, seleccione **recuperar atributos adicionales de un almacén de datos**.
4. En la ficha origen del atributo y Búsqueda del usuario, seleccione **Agregar origen del atributo**.
5. En la pestaña Almacén de datos, proporcione una descripción y seleccione la que almacén de datos ha agregado.
6. En la ficha Búsqueda de directorios LDAP:
   - Introduzca el **DN base**, que debe coincidir exactamente con el valor especificado en StorageGRID para el servidor LDAP.
   - Para el ámbito de búsqueda, seleccione **Subtree**.
   - Para la clase de objeto raíz, busque y agregue cualquiera de estos atributos: **ObjectGUID** o **userPrincipalName**.
7. En la ficha tipos de codificación de atributos binarios LDAP , seleccione **Base64** para el atributo **objectGUID** .
8. En la ficha filtro LDAP, introduzca **sAMAccountName=${username}**.
9. En la pestaña Cumplimiento de contrato de atributo, seleccione **LDAP (atributo)** en la lista desplegable Origen y seleccione **objectGUID** o **userPrincipalName** en la lista desplegable Valor.
10. Revise y, a continuación, guarde el origen del atributo.
11. En la ficha origen del atributo Failsave, seleccione **Anular la transacción SSO**.
12. Revise el resumen y seleccione **hecho**.
13. Seleccione **Listo**.

Configure los ajustes de protocolo

Pasos

1. En la ficha **Conexión SP** > **SSO del navegador** > **Configuración de protocolo**, seleccione **Configurar ajustes de protocolo**.
2. En la pestaña URL de servicio al consumidor de aserción, acepte los valores predeterminados, que se importaron desde los metadatos de SAML de StorageGRID (**POST** para enlace y `/api/saml-response` para URL de punto final).
3. En la pestaña URL del servicio de SLO, acepte los valores predeterminados, que se importaron desde los metadatos de SAML de StorageGRID (**REDIRECT** para enlace y `/api/saml-logout` para URL de punto final.
4. En la pestaña Enlaces SAML permitidos, desactive **ARTEFACTO** y **SOAP**. Sólo se requieren **POST** y **REDIRECT**.
5. En la pestaña Política de firma, deje las casillas de verificación **Requerir que se firmen las solicitudes AUTHN** y **Siempre firmar afirmación** seleccionadas.
6. En la ficha Directiva de cifrado, seleccione **Ninguno**.
7. Revise el resumen y seleccione **hecho** para guardar la configuración del protocolo.
8. Revise el resumen y seleccione **hecho** para guardar la configuración de SSO del explorador.

Configurar credenciales

Pasos

1. En la ficha Conexión SP, seleccione **credenciales**.
2. En la ficha credenciales, seleccione **Configurar credenciales**.
3. Seleccione elcertificado de firma usted creó o importó.
4. Seleccione **Siguiente** para ir a **gestionar ajustes de verificación de firma**.
   a. En la ficha Modelo de confianza, seleccione **sin anclar**.
   b. En la pestaña Certificado de verificación de firma, revise la información de certificación de firma, que se importó de los metadatos SAML de StorageGRID.
5. Revise las pantallas de resumen y seleccione **Guardar** para guardar la conexión SP.

Cree conexiones adicionales del SP

Puede copiar la primera conexión de SP para crear las conexiones de SP que necesita para cada nodo de administrador de su grid. Se cargan metadatos nuevos para cada copia.

> Las conexiones SP para diferentes nodos de administración utilizan valores idénticos, a excepción del ID de entidad del partner, la URL base, el ID de conexión, el nombre de conexión, la verificación de firma, Y URL de respuesta de SLO.

Pasos

1. Seleccione **Acción** > **Copiar** para crear una copia de la conexión SP inicial para cada nodo de administración adicional.
2. Introduzca el ID de conexión y el nombre de conexión para la copia y seleccione **Guardar**.
3. Elija el archivo de metadatos que corresponde al nodo de administración:
   a. Seleccione **Acción** > **Actualizar con metadatos**.
   b. Seleccione **elegir archivo** y cargue los metadatos.
   c. Seleccione **Siguiente**.
   d. Seleccione **Guardar**.
4. Resuelva el error debido al atributo no utilizado:
   a. Seleccione la nueva conexión.
   b. Seleccione **Configurar SSO del explorador > Configurar creación de aserción > Contrato de atributo**.
   c. Elimine la entrada para **urn:oid**.
   d. Seleccione **Guardar**.

Deshabilitar SSO

Si ya no desea usar esta funcionalidad, puede deshabilitar el inicio de sesión único (SSO). Debe deshabilitar el inicio de sesión único antes de poder deshabilitar la federación de identidades.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".

- Tienes "permisos de acceso específicos".

Pasos

1. Seleccione **Configuración** > **Control de acceso** > **Inicio de sesión único**.

   Aparece la página Single Sign-On.

2. Seleccione **Deshabilitar SSO**.
3. Seleccione **Sí**.

   Aparece un mensaje de advertencia que indica que los usuarios locales podrán iniciar sesión.

La próxima vez que inicie sesión en StorageGRID, aparecerá la página Inicio de sesión en StorageGRID, donde deberá introducir el nombre de usuario y la contraseña de un usuario de StorageGRID local o federado.

Deshabilitar y volver a habilitar temporalmente el SSO para un nodo de administración

Es posible que no pueda iniciar sesión en Grid Manager si se desactiva el sistema de inicio de sesión único (SSO). En este caso, puede deshabilitar y volver a habilitar SSO para un nodo de administración. Para deshabilitar y, a continuación, volver a habilitar SSO, debe acceder al shell de comandos del nodo.

Antes de empezar

- Tienes "permisos de acceso específicos".
- Tiene el `Passwords.txt` archivo.
- Conoce la contraseña del usuario raíz local.

Acerca de esta tarea

Después de deshabilitar SSO para un nodo de administración, puede iniciar sesión en Grid Manager como usuario raíz local. Para proteger el sistema StorageGRID, tiene que utilizar el shell de comandos del nodo para volver a habilitar SSO en el nodo de administración tan pronto como cierre la sesión.

> La deshabilitación de SSO para un nodo de administrador no afecta la configuración de SSO para ningún otro nodo de administrador que esté en el grid. La casilla de verificación **Enable SSO** en la página Single Sign-On en Grid Manager permanece seleccionada y se mantienen todas las configuraciones de SSO existentes a menos que las actualice.

Pasos

1. Inicie sesión en un nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a raíz: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

      Al iniciar sesión como root, la petición de datos cambia de `$` a `#`.

2. Ejecute el siguiente comando:`disable-saml`

Un mensaje indica que el comando se aplica únicamente a este nodo de administrador.

3. Confirme que desea deshabilitar SSO.

   Un mensaje indica que el inicio de sesión único está deshabilitado en el nodo.

4. Desde un explorador web, acceda a Grid Manager en el mismo nodo de administración.

   Ahora se muestra la página de inicio de sesión de Grid Manager porque SSO se ha desactivado.

5. Inicie sesión con la raíz del nombre de usuario y la contraseña del usuario raíz local.
6. Si deshabilitó temporalmente SSO debido a que debe corregir la configuración de SSO:
   a. Seleccione **Configuración** > **Control de acceso** > **Inicio de sesión único**.
   b. Cambie la configuración incorrecta o obsoleta de SSO.
   c. Seleccione **Guardar**.

      Al seleccionar **Guardar** en la página de inicio de sesión único, se vuelve a activar SSO automáticamente para toda la cuadrícula.

7. Si ha desactivado SSO temporalmente porque necesita acceder a Grid Manager por algún otro motivo:
   a. Realice cualquier tarea o tarea que necesite realizar.
   b. Seleccione **Cerrar sesión** y cierre Grid Manager.
   c. Vuelva a habilitar SSO en el nodo de administrador. Puede realizar cualquiera de los siguientes pasos:

      - Ejecute el siguiente comando: `enable-saml`

        Un mensaje indica que el comando se aplica únicamente a este nodo de administrador.

      Confirme que desea habilitar SSO.

   Un mensaje indica que el inicio de sesión único está habilitado en el nodo.

      - Reinicie el nodo de cuadrícula: `reboot`
8. Desde un explorador web, acceda a Grid Manager desde el mismo nodo de administración.
9. Confirme que aparece la página de inicio de sesión de StorageGRID y que debe introducir sus credenciales de SSO para acceder a Grid Manager.

Usar federación de grid

¿Qué es GRID federation?

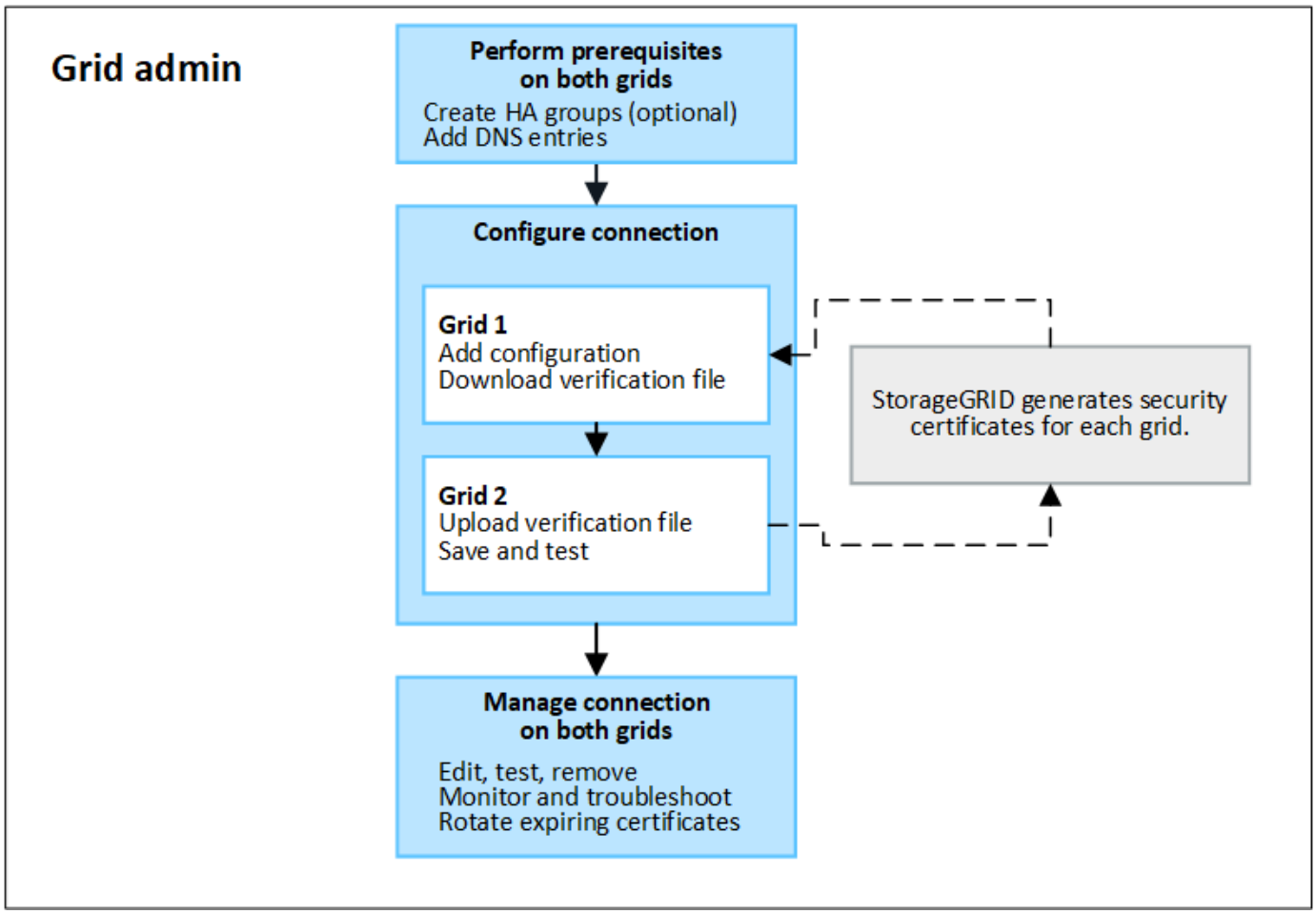
Puede utilizar la federación de grid para clonar inquilinos y replicar sus objetos entre dos sistemas StorageGRID para la recuperación ante desastres.

¿Qué es una conexión de federación de grid?

Una conexión de federación de grid es una conexión bidireccional, de confianza y segura entre los nodos de administración y puerta de enlace en dos sistemas StorageGRID.

Flujo de trabajo de federación de grid

El diagrama de flujo de trabajo resume los pasos para configurar una conexión de federación de grid entre dos cuadrículas.



Consideraciones y requisitos para las conexiones de federación de grid

- Los grids utilizados para la federación de grid deben ejecutar versiones de StorageGRID que sean idénticas o que no tengan más de una diferencia principal entre ellas.

  Para obtener más información sobre los requisitos de la versión, consulte la "Notas de la versión".

- Un grid puede tener una o más conexiones de federación de grid a otras grids. Cada conexión de federación de grid es independiente de cualquier otra conexión. Por ejemplo, si Grid 1 tiene una conexión con Grid 2 y una segunda conexión con Grid 3, no hay ninguna conexión implícita entre Grid 2 y Grid 3.
- Las conexiones de federación de grid son bidireccionales. Una vez establecida la conexión, puede supervisar y gestionar la conexión desde cualquiera de las dos redes.
- Debe existir al menos una conexión de federación de grid para poder utilizar "clon de cuenta" o."replicación entre grid"

Requisitos de redes y dirección IP

- Las conexiones de federación de grid se pueden producir en la red de grid, la red de administración o la red de cliente.
- Una conexión de federación de grid conecta un grid a otro. La configuración de cada grid especifica un

extremo de federación de grid en el otro grid que consta de nodos de administración, nodos de puerta de enlace o ambos.

- La práctica recomendada es la conexión de "Grupos de alta disponibilidad"nodos de administración y puerta de enlace en cada grid. El uso de grupos de alta disponibilidad ayuda a garantizar que las conexiones de federación de grid permanecerán en línea en caso de que los nodos dejen de estar disponibles. Si la interfaz activa en cualquiera de los grupos de alta disponibilidad falla, la conexión puede usar una interfaz de backup.
- No se recomienda crear una conexión de federación de grid que utilice la dirección IP de un único nodo de administración o nodo de pasarela. Si el nodo deja de estar disponible, la conexión de federación de grid también no estará disponible.
- "Replicación entre grid" De objetos requiere que los nodos de almacenamiento de cada grid puedan acceder a los nodos de administración y puerta de enlace configurados en el otro grid. En cada grid, confirme que todos los nodos de almacenamiento tienen una ruta de ancho de banda alto a los nodos de administración o puerta de enlace utilizados para la conexión.

Utilice FQDN para equilibrar la carga de la conexión

En un entorno de producción, utilice nombres de dominio completamente cualificados (FQDN) para identificar cada cuadrícula en la conexión. A continuación, cree las entradas DNS apropiadas, de la siguiente manera:

- El FQDN para Grid 1 se asignó a una o más direcciones IP virtuales (VIP) para grupos de alta disponibilidad en Grid 1, o a la dirección IP de uno o más nodos de administración o puerta de enlace en Grid 1.
- El FQDN para Grid 2 asignado a una o más direcciones VIP para Grid 2 o a la dirección IP de uno o más nodos de administración o puerta de enlace en Grid 2.

Cuando utiliza varias entradas DNS, las solicitudes para utilizar la conexión se equilibran de carga, de la siguiente manera:

- Las entradas de DNS que se asignan a las direcciones VIP de varios grupos de alta disponibilidad se equilibran la carga entre los nodos activos de los grupos de alta disponibilidad.
- Las entradas de DNS que se asignan a las direcciones IP de varios nodos de administración o nodos de pasarela se equilibran la carga entre los nodos asignados.

Requisitos de puertos

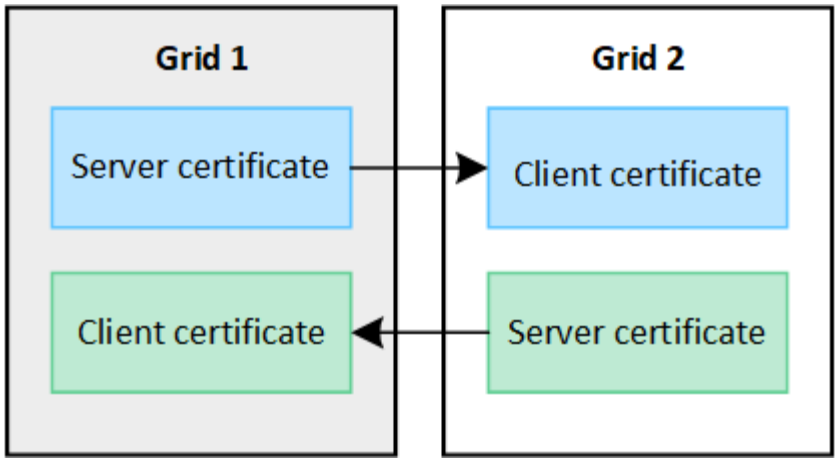
Al crear una conexión de federación de grid, puede especificar cualquier número de puerto no utilizado de 23000 a 23999. Ambas rejillas de esta conexión utilizarán el mismo puerto.

Debe asegurarse de que ningún nodo de ninguno de los grid utilice este puerto para otras conexiones.

Requisitos de certificado

Cuando se configura una conexión de federación de grid, StorageGRID genera automáticamente cuatro certificados SSL:

- Certificados de servidor y cliente para autenticar y cifrar la información enviada desde la cuadrícula 1 a la cuadrícula 2
- Certificados de servidor y cliente para autenticar y cifrar la información enviada desde la cuadrícula 2 a la cuadrícula 1



Por defecto, los certificados son válidos durante 730 días (2 años). Cuando estos certificados se acercan a su fecha de vencimiento, la alerta **Vencimiento del certificado de federación de grid** le recuerda que debe rotar los certificados, lo que puede hacer con el Administrador de grid.

> Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar. La replicación de datos estará pendiente hasta que se actualicen los certificados.

Leer más

- "Crear conexiones de federación de grid"
- "Gestionar conexiones de federación de grid"
- "Solucionar errores de federación de grid"

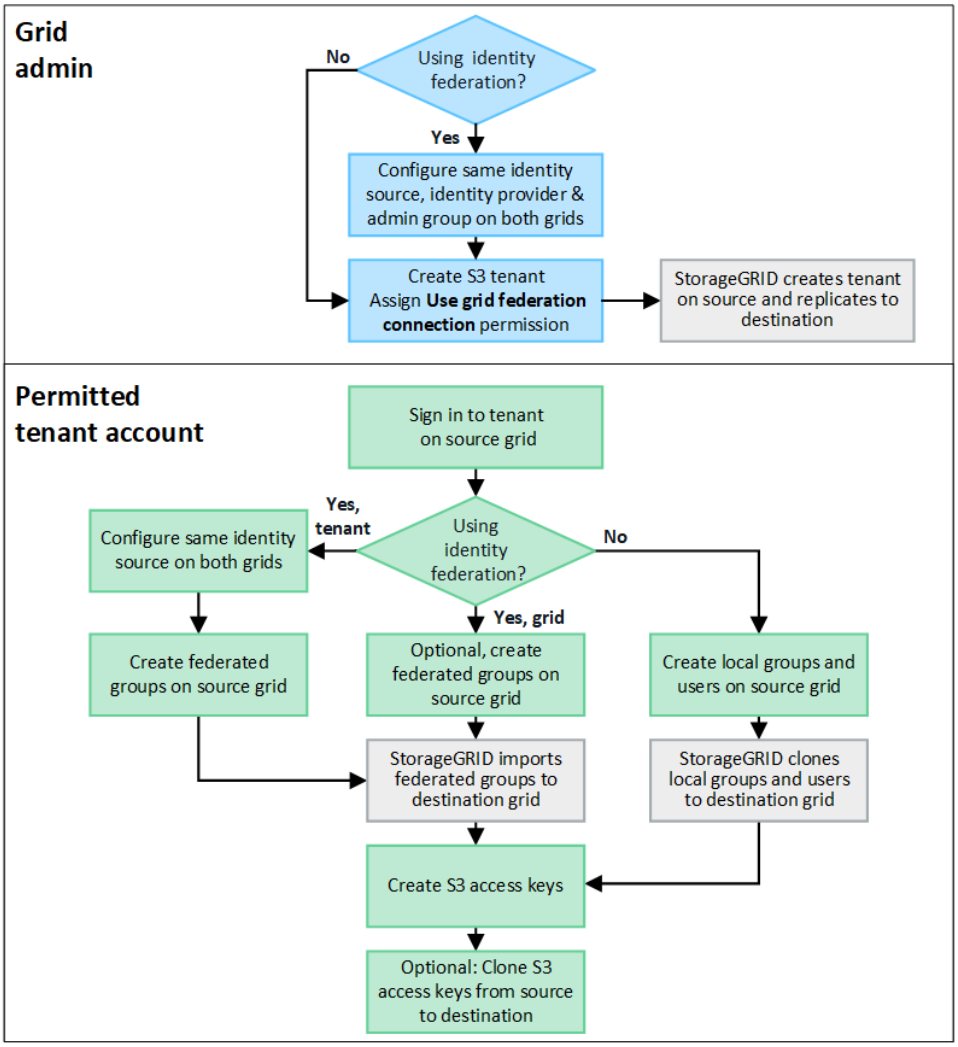
¿Qué es el clon de cuenta?

El clon de cuenta es la replicación automática de una cuenta de inquilino, grupos de inquilinos, usuarios de inquilinos y, opcionalmente, claves de acceso S3 entre los sistemas StorageGRID de una "conexión de federación de grid".

La clonación de cuenta es necesaria para "replicación entre grid". Al clonar la información de la cuenta desde un sistema StorageGRID de origen a un sistema StorageGRID de destino se garantiza que los usuarios y grupos inquilinos puedan acceder a los bloques y objetos correspondientes en cualquiera de los grid.

Flujo de trabajo del clon de cuenta

El diagrama de flujo de trabajo muestra los pasos que realizarán los administradores de grid y los inquilinos permitidos para configurar el clon de cuenta. Estos pasos se realizan después de la "la conexión de federación de grid está configurada".



Flujo de trabajo del administrador de grid

Los pasos que realizan los administradores de grid dependen de si los sistemas de StorageGRID en el "conexión de federación de grid" uso de inicio de sesión único (SSO) o federación de identidades.

Configurar SSO para el clon de cuenta (opcional)

Si alguno de los sistemas StorageGRID de la conexión de federación de grid utiliza SSO, ambos grids deben utilizar SSO. Antes de crear las cuentas de inquilino para la federación de grid, los administradores de grid de origen y destino del inquilino deben realizar estos pasos.

Pasos

1. Configure el mismo origen de identidad para ambas cuadrículas. Consulte "Usar la federación de identidades".
2. Configure el mismo proveedor de identidad SSO (IdP) para ambas redes. Ver "Configurar el inicio de sesión único" .
3. "Cree el mismo grupo de administración" en ambas cuadrículas importando el mismo grupo federado.

   Al crear el inquilino, seleccionará este grupo para que tenga el permiso inicial de acceso raíz para las cuentas de inquilino de origen y de destino.

Si este grupo de administración no existe en ambas cuadrículas antes de crear el arrendatario, el arrendatario no se replica en el destino.

Configurar federación de identidades a nivel de cuadrícula para el clon de cuenta (opcional)

Si alguno de los sistemas StorageGRID utiliza la federación de identidades sin SSO, ambas cuadrículas deben utilizar la federación de identidades. Antes de crear las cuentas de inquilino para la federación de grid, los administradores de grid de origen y destino del inquilino deben realizar estos pasos.

Pasos

1. Configure el mismo origen de identidad para ambas cuadrículas. Consulte "Usar la federación de identidades".
2. Opcionalmente, si un grupo federado tendrá permiso de acceso raíz inicial para las cuentas de arrendatario de origen y de destino, "cree el mismo grupo de administración" en ambas cuadrículas importando el mismo grupo federado.

   Si asigna permiso de acceso raíz a un grupo federado que no existe en ambas cuadrículas, el inquilino no se replica en la cuadrícula de destino.

3. Si no desea que un grupo federado tenga permiso de acceso raíz inicial para ambas cuentas, especifique una contraseña para el usuario raíz local.

Cree una cuenta de inquilino de S3 permitida

Después de configurar, de manera opcional, el inicio de sesión único o la federación de identidades, un administrador de grid lleva a cabo estos pasos para determinar qué inquilinos pueden replicar objetos del bloque en otros sistemas StorageGRID.

Pasos

1. Determine qué grid desea que sea la cuadrícula de origen del inquilino para las operaciones de clonación de cuentas.

   La cuadrícula donde se creó originalmente el inquilino se conoce como *source grid* del inquilino. La cuadrícula donde se replica el inquilino se conoce como *grid de destino* del inquilino.

2. En esa cuadrícula, cree una nueva cuenta de inquilino de S3 o edite una cuenta existente.
3. Asigne el permiso **Use grid federation connection**.
4. Si la cuenta de inquilino administrará sus propios usuarios federados, asigne el permiso **Usar propia fuente de identidad**.

   Si se asigna este permiso, tanto las cuentas de arrendatario de origen como las de destino deben configurar el mismo origen de identidad antes de crear grupos federados. Los grupos federados agregados al inquilino de origen no se pueden clonar en el inquilino de destino a menos que ambas cuadrículas utilicen el mismo origen de identidad.

5. Seleccione una conexión de federación de cuadrícula específica.
6. Guarde el inquilino nuevo o modificado.

   Cuando se guarda un nuevo inquilino con el permiso **Usar conexión de federación de grid**, StorageGRID crea automáticamente una réplica de ese inquilino en la otra cuadrícula, de la siguiente manera:

- Ambas cuentas de inquilino tienen el mismo ID de cuenta, nombre, cuota de almacenamiento y permisos asignados.
- Si seleccionó un grupo federado para tener permiso de acceso raíz para el inquilino, ese grupo se clona en el inquilino de destino.
- Si seleccionó un usuario local para que tenga permiso de acceso raíz para el inquilino, ese usuario se clona en el inquilino de destino. Sin embargo, la contraseña para ese usuario no está clonada.

Para obtener más información, consulte "Gestionar inquilinos permitidos para la federación de grid".

Flujo de trabajo de cuenta de inquilino permitido

Después de que un inquilino con el permiso **Usar conexión de federación de grid** se replica en la cuadrícula de destino, las cuentas de inquilino permitidas pueden realizar estos pasos para clonar grupos de inquilinos, usuarios y claves de acceso S3.

Pasos

1. Inicie sesión en la cuenta de inquilino en la cuadrícula de origen del inquilino.
2. Si está permitido, configure Identify federation tanto en las cuentas de arrendatario de origen como en las de destino.
3. Cree grupos y usuarios en el arrendatario de origen.

   Cuando se crean nuevos grupos o usuarios en el inquilino de origen, StorageGRID los clona automáticamente en el inquilino de destino, pero no se produce ningún clonado del destino al origen.
4. Crear claves de acceso S3.
5. Opcionalmente, clone las claves de acceso S3 del inquilino de origen al inquilino de destino.

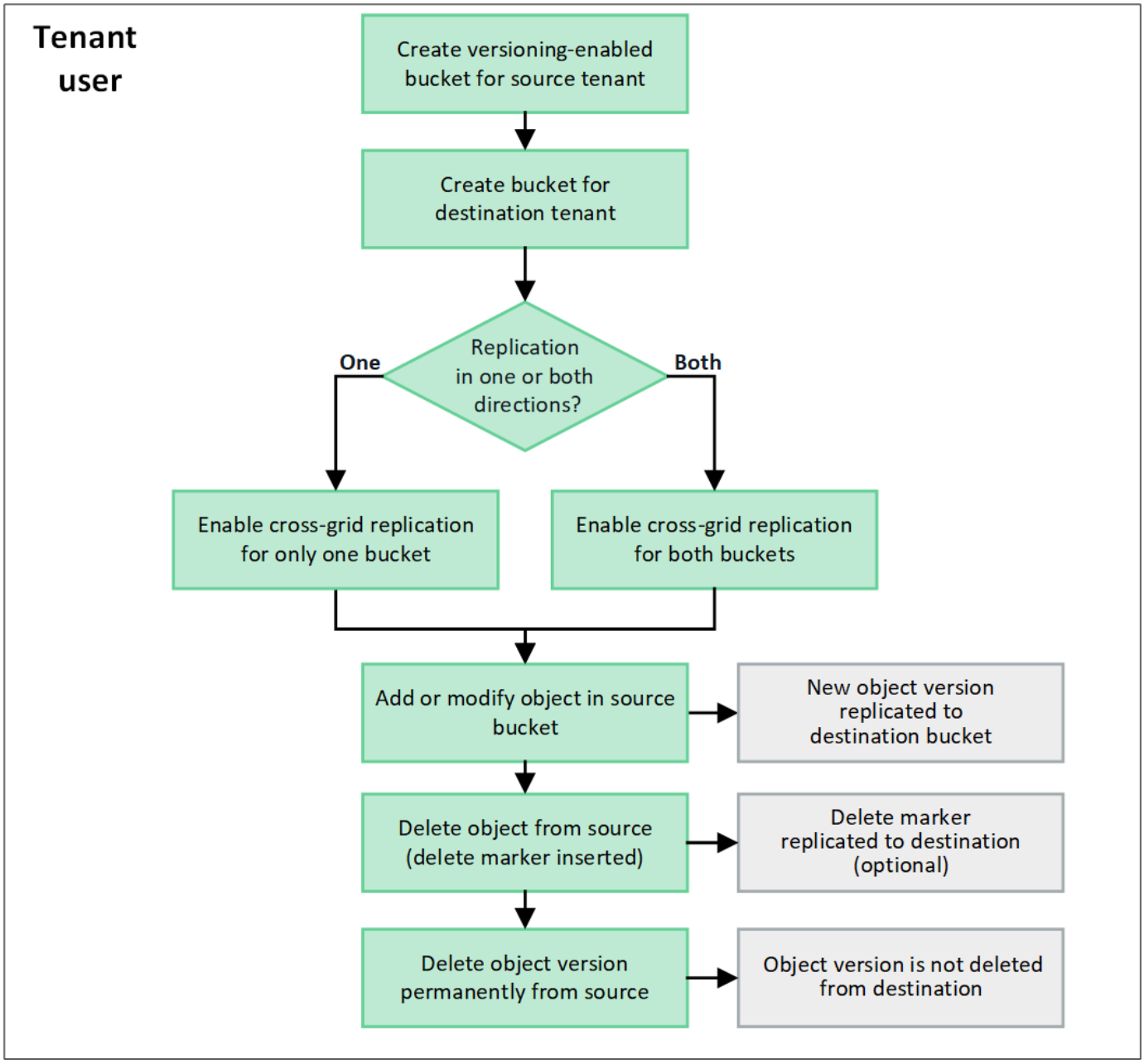
Para obtener detalles sobre el flujo de trabajo de la cuenta de inquilino permitido y para obtener información sobre cómo se clonan los grupos, los usuarios y las claves de acceso S3, consulte "Clone los usuarios y los grupos de inquilinos" y "Clone las claves de acceso S3 mediante la API".

¿Qué es la replicación entre grid?

La replicación entre grid es la replicación automática de objetos entre buckets S3 seleccionados en dos sistemas StorageGRID que están conectados en un "conexión de federación de grid". "Clon de cuenta" es necesario para la replicación entre grid.

Flujo de trabajo de replicación entre grid

El diagrama de flujo de trabajo resume los pasos para configurar la replicación entre redes entre depósitos en dos redes.



Requisitos de la replicación entre grid

Si una cuenta de inquilino tiene el permiso **Usar conexión de federación de red** para usar una o más"conexiones de federación de grid" Un usuario inquilino con permiso de acceso raíz puede crear depósitos en las cuentas de inquilino correspondientes en cada red. Estos cubos:

- Pueden tener nombres diferentes entre sí
- Puede tener diferentes regiones
- Debe tener el control de versiones activado
- Debe estar vacío

Una vez creados ambos bloques, la replicación entre grid se puede configurar para uno o ambos bloques.

Leer más

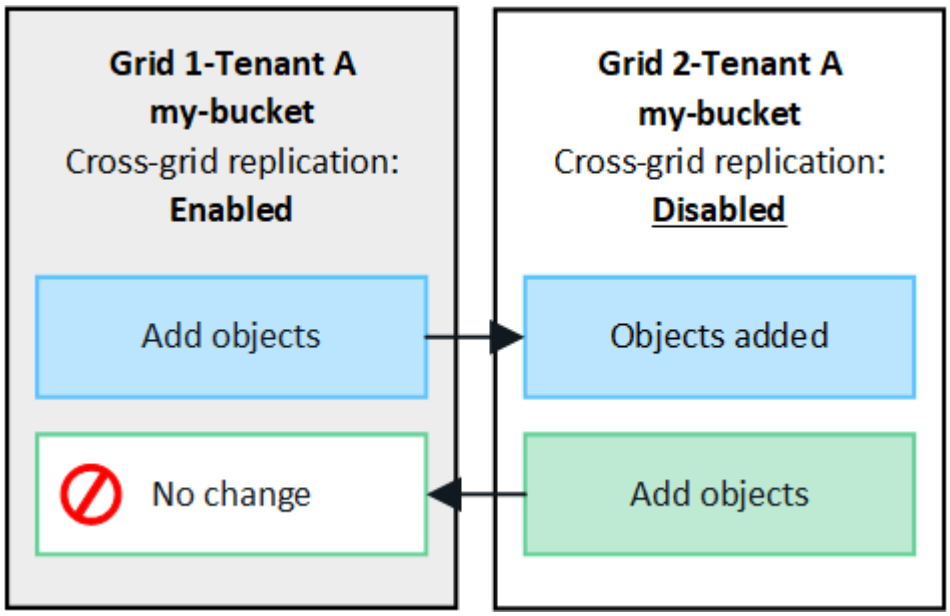
"Gestionar la replicación entre grid"

Funcionamiento de la replicación entre grid

Puede configurar la replicación entre redes para que se produzca en una dirección o en ambas direcciones.

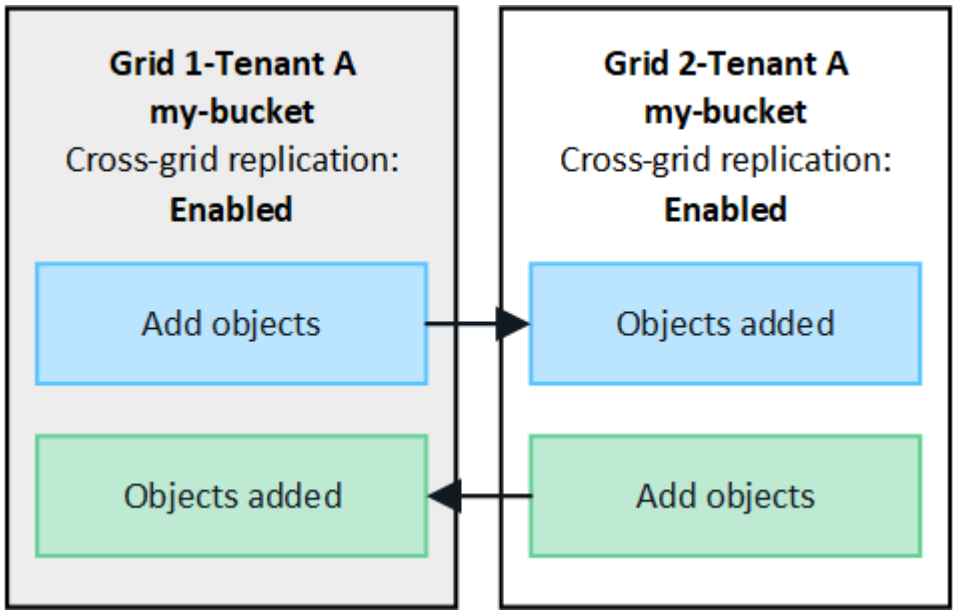
Replicación en una dirección

Si habilita la replicación entre cuadrículas para un depósito en una sola cuadrícula, los objetos agregados a ese depósito (el depósito de origen) se replican en el depósito correspondiente en la otra cuadrícula (el depósito de destino). Sin embargo, los objetos agregados al depósito de destino no se replican en el origen. En la figura, la replicación entre redes está habilitada para `my-bucket` de la cuadrícula 1 a la cuadrícula 2, pero no está habilitado en la otra dirección.



Replicación en ambas direcciones

Si habilita la replicación entre grid para el mismo bucket en ambos grids, los objetos agregados a cada bucket se replican en el otro grid. En la figura, la replicación entre grid está activada en `my-bucket` ambas direcciones.



¿Qué sucede cuando se ingieren objetos?

Cuando un cliente S3 agrega un objeto a un bloque que tiene habilitada la replicación entre grid, sucede lo siguiente:

1. StorageGRID replica automáticamente el objeto del bloque de origen al de destino. El tiempo para realizar esta operación de replicación en segundo plano depende de varios factores, incluidos la cantidad de otras operaciones de replicación pendientes.

   El cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud GetObject o HeadObject. La respuesta incluye un StorageGRID específico `x-ntap-sg-cgr-replication-status` encabezado de respuesta, que tiene uno de los siguientes valores:

Cuadrícula	Estado de replicación
Origen	• **COMPLETADO**: La replicación fue exitosa para todas las conexiones de red. • **PENDIENTE**: El objeto no ha sido replicado en al menos una conexión de red. • **FALLO**: La replicación no está pendiente para ninguna conexión a la red y al menos una falló con una falla permanente. Un usuario debe resolver el error.
Destino	**REPLICA**: El objeto fue replicado desde la cuadrícula de origen.

   > StorageGRID no es compatible con `x-amz-replication-status` encabezamiento.

2. StorageGRID utiliza las políticas de ILM activas de cada grid para gestionar los objetos, al igual que lo haría con cualquier otro objeto. Por ejemplo, el objeto A en Grid 1 se puede almacenar como dos copias replicadas y conservarse permanentemente, mientras que la copia del objeto A replicado en Grid 2 se puede almacenar con el código de borrado 2+1 y eliminarse después de tres años.

¿Qué sucede cuando se eliminan los objetos?

Como se describe en "Eliminar flujo de datos", StorageGRID puede suprimir un objeto por cualquiera de los siguientes motivos:

- El cliente S3 emite una solicitud de eliminación.
- Un usuario del gestor de inquilinos selecciona "Suprimir objetos del depósito"la opción para eliminar todos los objetos de un depósito.
- El bloque tiene una configuración del ciclo de vida que caduca.
- El último periodo de tiempo de la regla de ILM para el objeto finaliza, y no se han especificado más ubicaciones.

Cuando StorageGRID elimina un objeto debido a una operación Eliminar objetos en el bloque, la caducidad del ciclo de vida del bloque o la caducidad de la ubicación de ILM, el objeto replicado nunca se elimina del otro grid en una conexión de la federación de grid. Sin embargo, los marcadores de borrado que se han añadido al bloque de origen mediante eliminaciones de clientes de S3 se pueden replicar opcionalmente en el bloque de destino.

Para comprender qué sucede cuando un cliente S3 elimina objetos de un bloque que tiene habilitada la

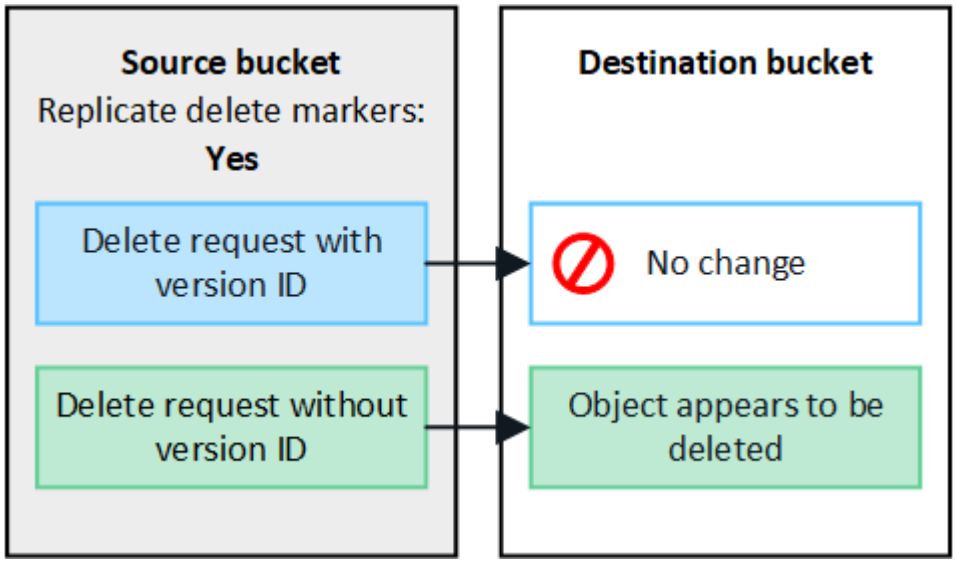
replicación entre grid, revise cómo los clientes S3 eliminan objetos de los bloques que tienen el control de versiones activado, de la siguiente manera:

- Si un cliente S3 emite una solicitud de eliminación que incluye un ID de versión, esa versión del objeto se elimina de forma permanente. No se ha añadido ningún marcador de borrado al depósito.
- Si un cliente S3 emite una solicitud de eliminación que no incluye un ID de versión, StorageGRID no elimina ninguna versión de objeto. En lugar de ello, agrega un marcador de eliminación al depósito. El marcador de eliminación hace que StorageGRID actúe como si el objeto hubiera sido eliminado:
  - Una solicitud GetObject sin un ID de versión falla con `404 No Object Found`
  - Una solicitud GetObject con un ID de versión válido tiene éxito y devuelve la versión del objeto solicitada.

Cuando un cliente S3 elimina un objeto de un bloque que tiene habilitada la replicación entre grid, StorageGRID determina si desea replicar la solicitud de eliminación en el destino, de la siguiente manera:

- Si la solicitud de eliminación incluye un ID de versión, esa versión del objeto se elimina de forma permanente de la cuadrícula de origen. Sin embargo, StorageGRID no replica las solicitudes de eliminación que incluyen un ID de versión, por lo que la misma versión del objeto no se elimina del destino.
- Si la solicitud de eliminación no incluye un ID de versión, StorageGRID puede replicar opcionalmente el marcador de eliminación, según cómo esté configurada la replicación entre redes para el depósito:
  - Si decide replicar marcadores de eliminación (valor predeterminado), se agrega un marcador de eliminación al bloque de origen y se replica en el bloque de destino. De hecho, el objeto parece eliminarse en ambas cuadrículas.
  - Si elige no replicar los marcadores de eliminación, se agrega un marcador de eliminación al depósito de origen, pero no se replica en el depósito de destino. En efecto, los objetos que se eliminan en la cuadrícula de origen no se eliminan en la cuadrícula de destino.

En la figura, **Replicar marcadores de eliminación** se configuró en **Sí** cuando"se ha activado la replicación entre grid" . Las solicitudes de eliminación del depósito de origen que incluyen un ID de versión no eliminan objetos del depósito de destino. Las solicitudes de eliminación del depósito de origen que no incluyen un ID de versión parecen eliminar objetos en el depósito de destino.



Si desea mantener las eliminaciones de objetos sincronizadas entre las cuadrículas, cree las correspondientes "Configuraciones de ciclo de vida de S3" para los depósitos en ambas cuadrículas.

Cómo se replican los objetos cifrados

Cuando se utiliza la replicación entre grid para replicar objetos entre grids, se pueden cifrar objetos individuales, utilizar el cifrado de bucket predeterminado o configurar el cifrado de toda la grid. Puede agregar, modificar o eliminar la configuración de cifrado predeterminada de bloque o de grid antes o después de habilitar la replicación entre grid para un bloque.

Para cifrar objetos individuales, puede utilizar SSE (cifrado del lado del servidor con claves gestionadas por StorageGRID) al agregar los objetos al depósito de origen. Utilice `x-amz-server-side-encryption` la cabecera de solicitud y especifique `AES256`. Consulte "Usar cifrado del servidor".

El uso de SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente) no es compatible con la replicación entre redes. La operación de ingesta fallará.

Para utilizar el cifrado predeterminado para un depósito, utilice una solicitud PutBucketEncryption y defina el `SSEAlgorithm` parámetro en `AES256`. El cifrado de nivel de bloque se aplica a cualquier objeto ingerido sin `x-amz-server-side-encryption` la cabecera de solicitud. Consulte "Operaciones en bloques".

Para utilizar el cifrado a nivel de cuadrícula, establezca la opción **cifrado de objetos almacenados** en **AES-256**. El cifrado a nivel de grid se aplica a cualquier objeto que no esté cifrado en el nivel de bucket o que se ingiera sin la `x-amz-server-side-encryption` cabecera de solicitud. Consulte "Configure las opciones de red y objeto".

SSE no admite AES-128. Si la opción **Cifrado de objetos almacenados** está habilitada para la cuadrícula de origen que utiliza la opción **AES-128**, el uso del algoritmo AES-128 no se propaga al objeto replicado. En su lugar, el objeto replicado utiliza el depósito predeterminado del destino o la configuración de cifrado a nivel de cuadrícula, si está disponible.

Al determinar cómo cifrar los objetos de origen, StorageGRID aplica estas reglas:

1. Utilice `x-amz-server-side-encryption` el encabezado de ingesta, si existe.
2. Si no hay un encabezado de ingesta presente, utilice la configuración de cifrado predeterminada del depósito, si está configurada.
3. Si no se configura una configuración de depósito, utilice la configuración de cifrado de toda la red, si está configurada.
4. Si no hay una configuración para toda la cuadrícula, no cifre el objeto de origen.

Al determinar cómo cifrar los objetos replicados, StorageGRID aplica estas reglas en este orden:

1. Use el mismo cifrado que el objeto de origen, a menos que ese objeto utilice cifrado AES-128.
2. Si el objeto de origen no está cifrado o utiliza AES-128, utilice la configuración de cifrado predeterminada del depósito de destino, si está configurada.
3. Si el depósito de destino no tiene una configuración de cifrado, utilice la configuración de cifrado de toda la red del destino, si está configurada.
4. Si no hay una configuración para toda la cuadrícula, no cifre el objeto de destino.

Replicación entre cuadrículas con S3 Object Lock

Puede configurar la replicación entre redes entre depósitos StorageGRID con S3 Object Lock habilitado en las siguientes circunstancias.

Cuando el bloqueo de objetos S3 en el depósito de origen es…	Y el bloqueo de objetos S3 en el depósito de destino es…
Habilitado	Habilitado
Desactivado	Habilitado

Cuando el bloqueo de objetos S3 en el depósito de origen está habilitado:

- Los objetos se bloquean con configuraciones de retención en el destino en este orden:
  a. Valores del encabezado de retención del objeto de origen para:

     `x-amz-object-lock-mode`

     `x-amz-object-lock-retain-until-date`

  b. La retención predeterminada del depósito de origen, si está configurada.
  c. La retención predeterminada del depósito de destino, si está configurada.

  La retención predeterminada del depósito de destino no anula la configuración de retención replicada desde el objeto de origen.
- Puede establecer el estado de retención legal para el objeto de destino mediante `x-amz-object-lock-legal-hold` al cargar el objeto.
- Se produce un error si el inquilino o el depósito de destino no admiten la configuración de bloqueo de objetos S3 del objeto de origen. Consulte "Alertas y errores de replicación entre redes."

Cuando el bloqueo de objetos S3 en el depósito de origen está deshabilitado:

- Puede configurar la retención predeterminada en el depósito de destino para aplicar la configuración de retención de Bloqueo de objetos S3 al objeto de destino.
- El objeto de destino no puede establecer un estado de retención legal.

PutObjectTagging y DeleteObjectTagging no son compatibles

Las solicitudes PutObjectTagging y DeleteObjectTagging no están soportadas para los objetos de los depósitos que tienen activada la replicación entre grid.

Si un cliente S3 emite una solicitud PutObjectTagging o DeleteObjectTagging, `501 Not Implemented` se devuelve. El mensaje es `Put(Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured.`

PutObjectRetention y PutObjectLegalHold no son compatibles

Las solicitudes PutObjectRetention y PutObjectLegalHold no son totalmente compatibles con los objetos en depósitos que tienen habilitada la replicación entre cuadrículas.

Si un cliente S3 emite una solicitud PutObjectRetention o PutObjectLegalHold, se modifican las configuraciones del objeto de origen, pero los cambios no se aplican al destino.

Cómo se replican los objetos segmentados

El tamaño máximo de segmento de la cuadrícula de origen se aplica a los objetos replicados en la cuadrícula de destino. Cuando los objetos se replican en otra cuadrícula, la configuración **Tamaño máximo de segmento** (**Configuración** > **Sistema** > **Opciones de almacenamiento**) de la cuadrícula de origen se utiliza en ambas cuadrículas. Por ejemplo, supongamos que el tamaño máximo de segmento para la cuadrícula de origen es 1 GB, mientras que el tamaño máximo de segmento de la cuadrícula de destino es 50 MB. Si ingiere un objeto de 2 GB en la cuadrícula de origen, ese objeto se guarda como dos segmentos de 1 GB. También se replica en la red de destino como dos segmentos de 1 GB, aunque el tamaño máximo de segmento de esa red es de 50 MB.

Compare la replicación entre grid y la replicación de CloudMirror

A medida que comience a utilizar la federación de cuadrícula, revise las similitudes y diferencias entre "replicación entre grid" y el "Servicio de replicación CloudMirror de StorageGRID".

> ⓘ No puedes usar CloudMirror en un bucket replicado mediante replicación entre redes, y viceversa.

	Replicación entre grid	Servicio de replicación de CloudMirror
¿Cuál es el objetivo principal?	Un sistema StorageGRID actúa como sistema de recuperación ante desastres. Los objetos de un depósito se pueden replicar entre las cuadrículas en una o en ambas direcciones.	Permite que un inquilino replique automáticamente objetos de un bloque en StorageGRID (origen) a un bloque S3 externo (destino). La replicación de CloudMirror crea una copia independiente de un objeto en una infraestructura S3 independiente. Esta copia independiente no se utiliza como copia de seguridad, sino que a menudo se procesa en la nube.
¿Cómo se configura?	1. Configure una conexión de federación de grid entre dos cuadrículas. 2. Agregar nuevas cuentas de inquilino, que se clonan automáticamente en el otro grid. 3. Añadir usuarios y grupos de inquilinos nuevos que también se clonan. 4. Crea los bloques correspondientes en cada grid y permite que la replicación entre grid se realice en una o en ambas direcciones.	1. Un usuario de inquilino configura la replicación de CloudMirror definiendo un extremo de CloudMirror (dirección IP, credenciales, etc.) mediante el administrador de inquilinos o la API de S3. 2. Se puede configurar cualquier bloque que pertenezca a esa cuenta de inquilino para que apunte al extremo de CloudMirror.

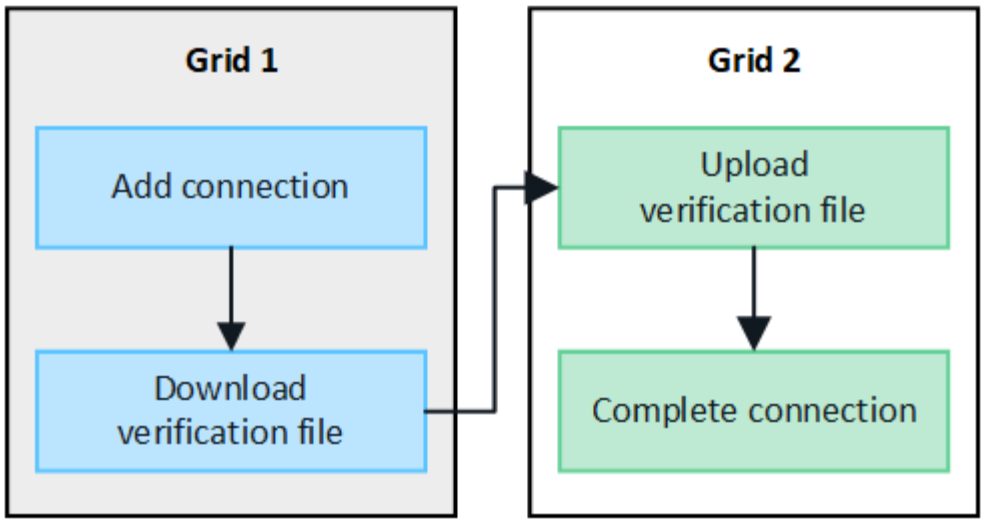
	Replicación entre grid	Servicio de replicación de CloudMirror
¿Quién es responsable de su configuración ?	• Un administrador de grid configura la conexión y los inquilinos. • Los usuarios inquilinos configuran los grupos, los usuarios, las claves y los buckets.	Normalmente, un usuario inquilino.
¿Cuál es el destino?	Un bloque de S3 correspondiente e idéntico en el otro sistema StorageGRID de la conexión de federación de grid.	• Cualquier infraestructura S3 compatible (incluido Amazon S3). • Google Cloud Platform (GCP)
¿Se requiere el control de versiones de objetos?	Sí, tanto los depósitos de origen como de destino deben tener activado el control de versiones de objetos.	No, la replicación de CloudMirror admite cualquier combinación de buckets sin versiones y con versiones tanto en el origen como en el destino.
¿Qué hace que los objetos se muevan al destino?	Los objetos se replican automáticamente cuando se añaden a un bloque que tiene habilitada la replicación entre grid.	Los objetos se replican automáticamente cuando se añaden a un bloque que se ha configurado con un extremo de CloudMirror. Los objetos que existían en el bloque de origen antes de que se configurara con el extremo de CloudMirror no se replican, a menos que se modifiquen.
¿Cómo se replican los objetos?	La replicación entre grid crea objetos con versiones y replica el identificador de versión del bloque de origen al bloque de destino. Esto permite mantener el orden de versión en ambas cuadrículas.	La replicación de CloudMirror no requiere buckets habilitados para el control de versiones, por lo que CloudMirror solo puede mantener el pedido de una clave dentro de un sitio. No hay garantías de que el pedido se mantendrá para las solicitudes a un objeto en un sitio diferente.
¿Qué pasa si un objeto no se puede replicar?	El objeto se pone en cola para la replicación, sujeto a los límites de almacenamiento de metadatos.	El objeto se pone en cola para la replicación, sujeto a los límites de servicios de plataforma (consulte "Recomendaciones para el uso de servicios de plataformas").
¿Se replican los metadatos del sistema del objeto?	Sí, cuando un objeto se replica en la otra cuadrícula, sus metadatos del sistema también se replican. Los metadatos serán idénticos en ambas cuadrículas.	No, cuando un objeto se replica en el depósito externo, sus metadatos del sistema se actualizan. Los metadatos variarán entre ubicaciones, en función del tiempo de procesamiento y del comportamiento de la infraestructura S3 independiente.

	Replicación entre grid	Servicio de replicación de CloudMirror
¿Cómo se recuperan los objetos?	Las aplicaciones pueden recuperar o leer objetos mediante la realización de una solicitud al depósito en cualquier cuadrícula.	Las aplicaciones pueden recuperar o leer objetos realizando una solicitud en StorageGRID o en el destino de S3. Por ejemplo, supongamos que usa la replicación de CloudMirror para reflejar objetos en una organización asociada. El partner puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario usar StorageGRID.
¿Qué sucede si se elimina un objeto?	• Las solicitudes de supresión que incluyan un ID de versión nunca se replican en la cuadrícula de destino. • Las solicitudes de eliminación que no incluyen un ID de versión agregan un marcador de eliminación al depósito de origen, que opcionalmente se puede replicar en la cuadrícula de destino. • Si la replicación entre grid se configura para una sola dirección, los objetos del bucket de destino se pueden eliminar sin afectar al origen.	Los resultados variarán en función del estado de control de versiones de los depósitos de origen y destino (que no necesitan ser los mismos): • Si ambos cubos están versionados, una solicitud de eliminación agregará un marcador de eliminación en ambas ubicaciones. • Si sólo se ha versionado el depósito de origen, una solicitud de supresión agregará un marcador de supresión al origen pero no al destino. • Si ninguno de los depósitos está versionado, una solicitud de supresión suprimirá el objeto del origen pero no del destino. Del mismo modo, los objetos del bloque de destino se pueden eliminar sin que ello afecte al origen.

Crear conexiones de federación de grid

Puede crear una conexión de federación de grid entre dos sistemas StorageGRID si desea clonar detalles de inquilinos y replicar datos de objetos.

Como se muestra en la figura, la creación de una conexión de federación de cuadrícula incluye pasos en ambas cuadrículas. Agrega la conexión en una cuadrícula y la completa en la otra. Puede empezar desde cualquiera de las dos cuadrículas.



Antes de empezar

- Ha revisado el "consideraciones y requisitos" para configurar las conexiones de federación de grid.
- Si planea utilizar nombres de dominio completos (FQDN) para cada cuadrícula en lugar de direcciones IP o VIP, sabrá qué nombres utilizar y confirmará que el servidor DNS de cada cuadrícula tiene las entradas adecuadas.
- Está utilizando una "navegador web compatible".
- Dispone de permiso de acceso raíz y la frase de acceso de aprovisionamiento para ambas cuadrículas.

Agregar conexión

Realice estos pasos en cualquiera de los dos sistemas StorageGRID.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal de cualquiera de las cuadrículas.
2. Seleccione **Configuración** > **Sistema** > **Federación de red**.
3. Selecciona **Añadir conexión**.
4. Introduzca los detalles de la conexión.

Campo	Descripción
Nombre de conexión	Un nombre único para ayudarle a reconocer esta conexión, por ejemplo, “Grid 1-Grid 2”.
FQDN o IP para este grid	Uno de los siguientes: • El FQDN del grid en el que está conectado actualmente • Dirección VIP de un grupo de alta disponibilidad en esta cuadrícula • La dirección IP de un nodo de administración o un nodo de pasarela en este grid. La IP puede estar en cualquier red a la que pueda acceder la cuadrícula de destino.

Campo	Descripción
Puerto	Puerto que desea utilizar para esta conexión. Puede introducir cualquier número de puerto no utilizado del 23000 al 23999. Ambas rejillas de esta conexión utilizarán el mismo puerto. Debe asegurarse de que ningún nodo de ninguno de los grid utilice este puerto para otras conexiones.
Días válidos de certificado para esta cuadrícula	El número de días que desea que los certificados de seguridad de esta cuadrícula de la conexión sean válidos. El valor predeterminado es 730 días (2 años), pero puede introducir cualquier valor de 1 a 762 días. StorageGRID genera automáticamente certificados de cliente y de servidor para cada grid al guardar la conexión.
Aprovisionamiento de la clave de acceso para este grid	La clave de acceso de aprovisionamiento para el grid en el que ha iniciado sesión.
FQDN o IP para el otro grid	Uno de los siguientes: • El FQDN del grid al que desea conectarse • Una dirección VIP de un grupo de alta disponibilidad en la otra cuadrícula • Una dirección IP de un nodo de administración o nodo de pasarela en el otro grid. La IP puede estar en cualquier red a la que pueda acceder la red de origen.

5. Selecciona **Guardar y continuar**.
6. Para el paso Descargar archivo de verificación, seleccione **Descargar archivo de verificación**.

   Una vez completada la conexión en la otra cuadrícula, ya no podrá descargar el archivo de verificación de ninguna de las dos.

7. Busque el archivo descargado (*`connection-name`*`.grid-federation`) y guárdelo en una ubicación segura.

   > ⚠ Este archivo contiene secretos (enmascarados como *****) y otros detalles confidenciales y debe almacenarse y transmitirse de forma segura.

8. Selecciona **Cerrar** para volver a la página de Grid federation.
9. Confirme que se muestra la nueva conexión y que su **estado de conexión** está **esperando para conectarse**.
10. Proporcione *`connection-name`*`.grid-federation` el archivo al administrador de grid para el otro grid.

Conexión completa

Realice estos pasos en el sistema StorageGRID al que se está conectando (la otra cuadrícula).

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Seleccione **Configuración** > **Sistema** > **Federación de red**.
3. Seleccione **Cargar archivo de verificación** para acceder a la página Cargar.
4. Seleccione **Cargar archivo de verificación**. A continuación, busque y seleccione el archivo que se descargó de la primera cuadrícula (*connection-name*`.grid-federation`).

   Se muestran los detalles de la conexión.

5. Opcionalmente, introduzca un Núm. Diferente de días válidos para los certificados de seguridad de esta cuadrícula. La entrada **Certificate Valid Days** establece por defecto el valor que ingresaste en la primera cuadrícula, pero cada cuadrícula puede usar diferentes fechas de vencimiento.

   En general, utilice el mismo número de días para los certificados en ambos lados de la conexión.

   > Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar y las replicaciones estarán pendientes hasta que se actualicen los certificados.

6. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que está conectado actualmente.
7. Seleccione **Guardar y probar**.

   Los certificados se generan y se prueba la conexión. Si la conexión es válida, aparece un mensaje de éxito y la nueva conexión se muestra en la página federación de Cuadrícula. El **Estado de conexión** será **Conectado**.

   Si aparece un mensaje de error, solucione cualquier problema. Consulte "Solucionar errores de federación de grid".

8. Vaya a la página Grid federation en la primera cuadrícula y actualice el explorador. Confirme que el **Estado de conexión** es ahora **Conectado**.
9. Una vez establecida la conexión, elimine de forma segura todas las copias del archivo de verificación.

   Si edita esta conexión, se creará un nuevo archivo de verificación. No se puede volver a utilizar el archivo original.

Después de terminar

- Revise las consideraciones para "gestión de inquilinos permitidos".
- "Cree una o más cuentas de arrendatario nuevas", Asigne el permiso **Use grid federation connection** y seleccione la nueva conexión.
- "Gestionar la conexión" según sea necesario. Puede editar valores de conexión, probar una conexión, rotar certificados de conexión o eliminar una conexión.
- "Supervise la conexión" Como parte de sus actividades normales de monitoreo de StorageGRID.
- "Solucione los problemas de la conexión", incluyendo la resolución de alertas y errores relacionados con la clonación de cuentas y la replicación entre redes.

Gestionar conexiones de federación de grid

La gestión de las conexiones de federación de grid entre sistemas StorageGRID incluye editar detalles de conexión, girar los certificados, eliminar permisos de inquilinos y eliminar conexiones que no se utilizan.

Antes de empezar

- Ha iniciado sesión en Grid Manager en cualquiera de las cuadrículas mediante una "navegador web compatible".
- Tiene "Permiso de acceso raíz"el para la cuadrícula en la que ha iniciado sesión.

Edite una conexión de federación de cuadrícula

Puede editar una conexión de federación de grid iniciando sesión en el nodo de administración principal en cualquier cuadrícula de la conexión. Después de realizar cambios en la primera cuadrícula, debe descargar un nuevo archivo de verificación y cargarlo en la otra cuadrícula.

> Mientras se edita la conexión, las solicitudes de clonación de cuentas o replicación entre cuadrículas seguirán utilizando la configuración de conexión existente. Las ediciones que realice en la primera cuadrícula se guardan localmente, pero no se utilizan hasta que se hayan cargado en la segunda cuadrícula, se hayan guardado y probado.

Comience a editar la conexión

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal de cualquiera de las cuadrículas.
2. Seleccione **Nodos** y confirme que todos los demás nodos de administración en su sistema estén en línea.

> Cuando edita una conexión de federación de grid, StorageGRID intenta guardar un archivo de configuración de candidato en todos los nodos de administración de la primera cuadrícula. Si este archivo no se puede guardar en todos los nodos de administración, aparecerá un mensaje de advertencia al seleccionar **Guardar y probar**.

3. Seleccione **Configuración** > **Sistema** > **Federación de red**.
4. Edite los detalles de la conexión utilizando el menú **Acciones** de la página de federación de cuadrícula o la página de detalles de una conexión específica. Consulte "Crear conexiones de federación de grid" para ver qué introducir.

Menú Actions

a. Seleccione el botón de opción para la conexión.
b. Selecciona **Acciones** > **Editar**.
c. Introduzca la nueva información.

Detalles

a. Seleccione un nombre de conexión para mostrar sus detalles.
b. Seleccione **Editar**.
c. Introduzca la nueva información.

5. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que ha iniciado sesión.
6. Selecciona **Guardar y continuar**.

   Los nuevos valores se guardan, pero no se aplicarán a la conexión hasta que haya cargado el nuevo archivo de verificación en la otra cuadrícula.

7. Seleccione **Descargar archivo de verificación**.

   Para descargar este archivo más adelante, vaya a la página de detalles de la conexión.

8. Busque el archivo descargado (*`connection-name`*`.grid-federation`) y guárdelo en una ubicación segura.

   > El archivo de verificación contiene secretos y debe almacenarse y transmitirse de forma segura.

9. Selecciona **Cerrar** para volver a la página de Grid federation.
10. Confirme que el **Estado de conexión** es **Edición pendiente**.

    > Si el estado de la conexión no era **Connected** cuando comenzó a editar la conexión, no cambiará a **Pending edit**.

11. Proporcione *`connection-name`*`.grid-federation` el archivo al administrador de grid para el otro grid.

Termine de editar la conexión

Termine de editar la conexión cargando el archivo de verificación en la otra cuadrícula.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Seleccione **Configuración** > **Sistema** > **Federación de red**.
3. Seleccione **Cargar archivo de verificación** para acceder a la página de carga.
4. Seleccione **Cargar archivo de verificación**. A continuación, busque y seleccione el archivo que se descargó de la primera cuadrícula.
5. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que está conectado actualmente.
6. Seleccione **Guardar y probar**.

   Si la conexión se puede establecer mediante los valores editados, aparece un mensaje de éxito. De lo contrario, aparecerá un mensaje de error. Revise el mensaje y resuelva cualquier problema.

7. Cierre el asistente para volver a la página Grid federation.
8. Confirme que el **Estado de conexión** es **Conectado**.
9. Vaya a la página Grid federation en la primera cuadrícula y actualice el explorador. Confirme que el **Estado de conexión** es ahora **Conectado**.
10. Una vez establecida la conexión, elimine de forma segura todas las copias del archivo de verificación.

Pruebe una conexión de federación de grid

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Seleccione **Configuración** > **Sistema** > **Federación de red**.
3. Pruebe la conexión utilizando el menú **Acciones** de la página de Grid federation o la página de detalles de una conexión específica.

   Menú Actions

   a. Seleccione el botón de opción para la conexión.

   b. Selecciona **Acciones** > **Prueba**.

   Detalles

   a. Seleccione un nombre de conexión para mostrar sus detalles.

   b. Seleccione **probar conexión**.

4. Revise el estado de conexión:

Estado de conexión	Descripción
Conectado	Ambas rejillas están conectadas y se comunican con normalidad.
Error	La conexión está en estado de error. Por ejemplo, un certificado ha caducado o un valor de configuración ya no es válido.
Edición pendiente	Ha editado la conexión en esta cuadrícula, pero la conexión sigue utilizando la configuración existente. Para completar la edición, cargue el nuevo archivo de verificación en la otra cuadrícula.
Esperando conexión	Ha configurado la conexión en esta cuadrícula, pero la conexión no se ha completado en la otra. Descargue el archivo de verificación de esta cuadrícula y cárguelo en la otra cuadrícula.
Desconocido	La conexión está en estado desconocido, posiblemente debido a un problema de red o a un nodo sin conexión.

5. Si el estado de la conexión es **Error**, resuelva cualquier problema. A continuación, seleccione **Probar conexión** de nuevo para confirmar que el problema se ha solucionado.

Girar certificados de conexión

Cada conexión de federación de grid utiliza cuatro certificados SSL generados automáticamente para proteger la conexión. Cuando los dos certificados para cada cuadrícula se acercan a su fecha de vencimiento, la alerta **Caducidad del certificado de federación de cuadrícula** le recuerda que debe rotar los certificados.

> Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar y las replicaciones estarán pendientes hasta que se actualicen los certificados.

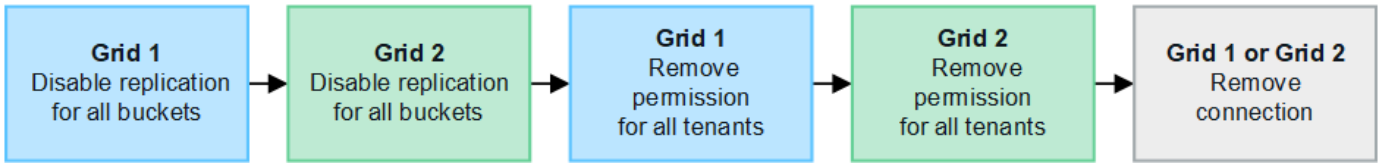
Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal de cualquiera de las cuadrículas.
2. Seleccione **Configuración** > **Sistema** > **Federación de red**.
3. En cualquiera de los separadores de la página Grid federation, seleccione el nombre de la conexión para mostrar sus detalles.
4. Seleccione la ficha **certificados**.
5. Seleccione **Girar certificados**.
6. Especifique cuántos días deben ser válidos los certificados nuevos.
7. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que ha iniciado sesión.
8. Seleccione **Girar certificados**.
9. Si es necesario, repita estos pasos en la otra cuadrícula de la conexión.

   En general, utilice el mismo número de días para los certificados en ambos lados de la conexión.

Elimine una conexión de federación de cuadrícula

Puede eliminar una conexión de federación de cuadrícula de cualquiera de las dos cuadrículas de la conexión. Como se muestra en la figura, debe realizar los pasos de requisitos previos en ambas cuadrículas para confirmar que la conexión no está siendo utilizada por ningún inquilino en ninguna de las cuadrículas.



Antes de eliminar una conexión, tenga en cuenta lo siguiente:

- La eliminación de una conexión no elimina ningún elemento que ya se haya copiado entre las cuadrículas. Por ejemplo, los usuarios, grupos y objetos de arrendatarios que existen en ambas cuadrículas no se eliminan de ninguna de las cuadrículas cuando se elimina el permiso del arrendatario. Si desea eliminar estos elementos, debe eliminarlos manualmente de ambas cuadrículas.
- Al eliminar una conexión, cualquier objeto que esté pendiente de replicación (ingerido pero que aún no se haya replicado en la otra cuadrícula) tendrá un fallo permanente en su replicación.

Desactive la replicación para todos los bloques de inquilinos

Pasos

1. A partir de cualquier cuadrícula, inicie sesión en Grid Manager desde el nodo de administración principal.
2. Seleccione **Configuración** > **Sistema** > **Federación de red**.
3. Seleccione el nombre de la conexión para mostrar sus detalles.
4. En la pestaña **Arrendatarios permitidos**, determine si la conexión está siendo utilizada por algún inquilino.
5. Si se muestra algún arrendatario, indique a todos los arrendatarios que "desactive la replicación entre grid" para todos sus depósitos en ambas cuadrículas de la conexión.

No puede eliminar el permiso **Usar conexión de federación de grid** si algún depósito de inquilino tiene habilitada la replicación entre grid. Cada cuenta de inquilino debe deshabilitar la replicación entre grid en sus bloques en ambos grids.

Eliminar permiso para cada inquilino

Después de que la replicación entre redes se haya desactivado para todos los depósitos de inquilinos, elimine el permiso **Usar federación de grid** de todos los inquilinos en ambas cuadrículas.

Pasos

1. Seleccione **Configuración** > **Sistema** > **Federación de red**.
2. Seleccione el nombre de la conexión para mostrar sus detalles.
3. Para cada inquilino en la pestaña **Arrendatarios permitidos**, elimine el permiso **Usar conexión de federación de grid** de cada inquilino. Consulte "Gestionar inquilinos permitidos".
4. Repita estos pasos para los inquilinos permitidos en la otra cuadrícula.

Retire la conexión

Pasos

1. Cuando ningún inquilino de ninguna de las dos rejillas esté usando la conexión, seleccione **Eliminar**.
2. Revise el mensaje de confirmación y seleccione **Eliminar**.
   - Si se puede eliminar la conexión, se muestra un mensaje de éxito. La conexión de federación de cuadrícula se elimina ahora de ambas cuadrículas.
   - Si la conexión no se puede eliminar (por ejemplo, aún está en uso o hay un error de conexión), se muestra un mensaje de error. Puede realizar una de las siguientes acciones:
     - Resuelva el error (recomendado). Consulte "Solucionar errores de federación de grid".
     - Retire la conexión por la fuerza. Consulte la siguiente sección.

Elimine una conexión de federación de cuadrícula por fuerza

Si es necesario, puede forzar la eliminación de una conexión que no tiene el estado **CONECTADA**.

La eliminación forzada sólo elimina la conexión de la rejilla local. Para eliminar completamente la conexión, realice los mismos pasos en ambas rejillas.

Pasos

1. En el cuadro de diálogo de confirmación, selecciona **Forzar eliminación**.

   Aparece un mensaje de éxito. Esta conexión de federación de grid ya no se puede utilizar. Sin embargo, es posible que los bloques de inquilinos aún tengan habilitada la replicación entre grid, y es posible que algunas copias de objeto ya se hayan replicado entre los grids en la conexión.

2. Desde la otra cuadrícula de la conexión, inicie sesión en Grid Manager desde el nodo de administración principal.
3. Seleccione **Configuración** > **Sistema** > **Federación de red**.
4. Seleccione el nombre de la conexión para mostrar sus detalles.
5. Selecciona **Eliminar** y **Sí**.

6. Seleccione **Forzar eliminación** para eliminar la conexión de esta cuadrícula.

Gestione los inquilinos permitidos para la federación de grid

Puede permitir que las cuentas de inquilino de S3 usen una conexión de federación de grid entre dos sistemas StorageGRID. Cuando se permite a los inquilinos utilizar una conexión, se requieren pasos especiales para editar los detalles del arrendatario o para eliminar permanentemente el permiso de un arrendatario para usar la conexión.

Antes de empezar

- Ha iniciado sesión en Grid Manager en cualquiera de las cuadrículas mediante una "navegador web compatible".
- Tiene "Permiso de acceso raíz"el para la cuadrícula en la que ha iniciado sesión.
- Hay "se ha creado una conexión de federación de grid" entre dos cuadrículas.
- Ha revisado los flujos de trabajo para "clon de cuenta" y."replicación entre grid"
- Según sea necesario, ya ha configurado Single Sign-On (SSO) o Identify federation para ambas cuadrículas en la conexión. Consulte "Qué es el clon de cuenta".

Cree un inquilino permitido

Si desea permitir que una cuenta de inquilino nueva o existente utilice una conexión de federación de grid para la clonación de cuentas y la replicación entre grid, siga las instrucciones generales de "Cree un nuevo inquilino S3" o "edite una cuenta de inquilino"tenga en cuenta lo siguiente:

- Puede crear el inquilino desde cualquier cuadrícula en la conexión. La cuadrícula donde se crea un inquilino es la cuadrícula de origen del *tenant*.
- El estado de la conexión debe ser **Conectado**.
- Cuando el inquilino se crea o edita para habilitar el permiso **Usar conexión de federación de grid** y luego se guarda en la primera cuadrícula, un inquilino idéntico se replica automáticamente en la otra cuadrícula. La cuadrícula en la que se replica el inquilino es la cuadrícula de destino del *tenant*.
- Los inquilinos de ambas cuadrículas tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos. Opcionalmente, puede utilizar el campo **Descripción** para ayudar a identificar cuál es el inquilino de origen y cuál es el inquilino de destino. Por ejemplo, esta descripción para un inquilino creado en Grid 1 también aparecerá para el inquilino replicado en Grid 2: «Este inquilino se creó en Grid 1».
- Por motivos de seguridad, la contraseña de un usuario raíz local no se copia en la cuadrícula de destino.

Antes de que un usuario raíz local pueda iniciar sesión en el inquilino replicado en la cuadrícula de destino, un administrador de grid para ese grid debe "cambie la contraseña del usuario raíz local".

- Una vez que el arrendatario nuevo o editado esté disponible en ambas cuadrículas, los usuarios del arrendatario pueden realizar estas operaciones:
  - A partir del grid de origen del inquilino, cree grupos y usuarios locales que se clonan automáticamente en el grid de destino del inquilino. Consulte "Clone los usuarios y los grupos de inquilinos".
  - Crear nuevas claves de acceso S3, que se pueden clonar opcionalmente en el grid de destino del inquilino. Consulte "Clone las claves de acceso S3 mediante la API".
  - Cree depósitos idénticos en ambas cuadrículas de la conexión y habilite la replicación entre

cuadrículas en una dirección o en ambas direcciones. Consulte "Gestionar la replicación entre grid".

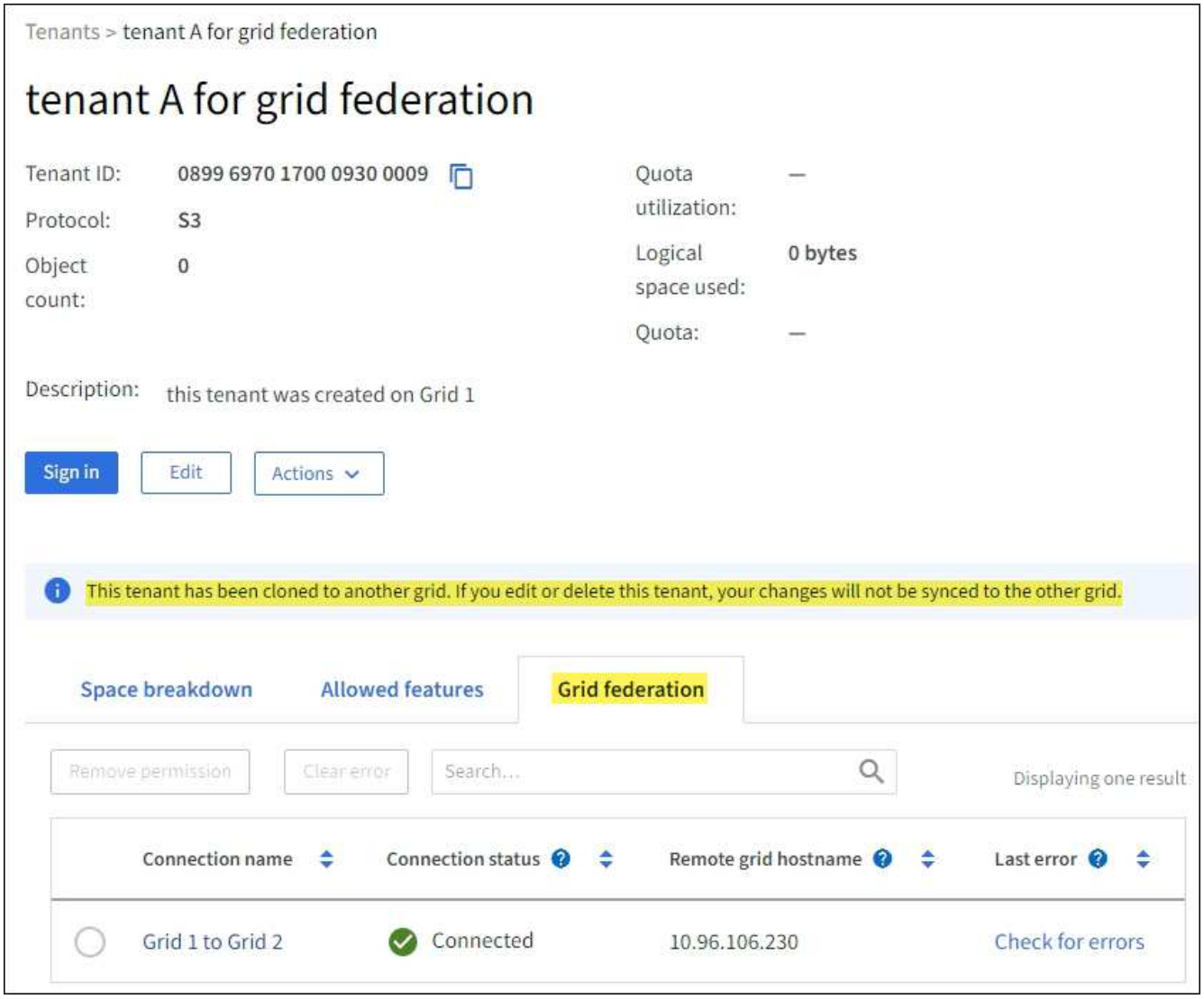
Ver un inquilino permitido

Puede ver los detalles de un inquilino con permiso para utilizar una conexión de federación de grid.

Pasos

1. Seleccione **Inquilinos**.
2. En la página Tenedores, seleccione el nombre del arrendatario para ver la página de detalles del arrendatario.

   Si se trata de la cuadrícula de origen del inquilino (es decir, si el inquilino se creó en esta cuadrícula), aparece un banner para recordarle que el inquilino se clonó en otra cuadrícula. Si edita o elimina este arrendatario, los cambios no se sincronizarán con la otra cuadrícula.



3. Opcionalmente, seleccione la pestaña **Grid federation** en "supervise la conexión de federación de grid".

Editar un arrendatario permitido

Si necesita editar un inquilino que tiene el permiso **Usar conexión de federación de grid**, siga las instrucciones generales para "editar una cuenta de inquilino" y tenga en cuenta lo siguiente:

- Si un inquilino tiene el permiso **Usar conexión de federación de grid**, puede editar los detalles del inquilino desde cualquier cuadrícula en la conexión. Sin embargo, los cambios que realice no se copiarán en la otra cuadrícula. Si desea mantener sincronizados los detalles del arrendatario entre las cuadrículas, debe realizar las mismas modificaciones en ambas cuadrículas.
- No puede borrar el permiso **Usar conexión de federación de grid** cuando está editando un inquilino.
- No puede seleccionar una conexión de federación de grid diferente al editar un inquilino.

Suprimir un arrendatario permitido

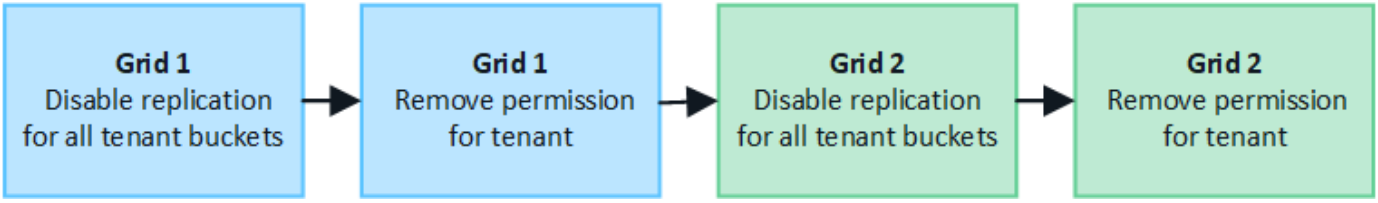
Si necesita eliminar un inquilino que tiene el permiso **Usar conexión de federación de grid**, siga las instrucciones generales para "eliminación de una cuenta de inquilino" y tenga en cuenta lo siguiente:

- Antes de poder eliminar el arrendatario original en la cuadrícula de origen, debe eliminar todos los depósitos de la cuenta en la cuadrícula de origen.
- Para poder quitar el inquilino clonado en la cuadrícula de destino, debe eliminar todos los buckets de la cuenta de la cuadrícula de destino.
- Si quita el inquilino original o el clonado, la cuenta ya no se puede usar para la replicación entre grid.
- Si va a eliminar el inquilino original en la cuadrícula de origen, los grupos de inquilinos, usuarios o las claves que se hayan clonado en el grid de destino no se verán afectados. Puede eliminar el inquilino clonado o permitir que gestione sus propios grupos, usuarios, claves de acceso y bloques.
- Si va a quitar el inquilino clonado en la cuadrícula de destino, se producirán errores de clonado si se añaden usuarios o grupos nuevos al inquilino original.

  Para evitar estos errores, elimine el permiso del inquilino para utilizar la conexión de federación de grid antes de eliminar el inquilino de esta cuadrícula.

Eliminar el permiso de conexión Usar federación de grid

Para evitar que un inquilino utilice una conexión de federación de grid, debe eliminar el permiso **Usar conexión de federación de grid**.



Antes de eliminar el permiso de un inquilino para utilizar una conexión de federación de grid, tenga en cuenta lo siguiente:

- No puede eliminar el permiso **Usar conexión de federación de grid** si alguno de los depósitos del inquilino tiene habilitada la replicación entre grid. La cuenta de inquilino debe deshabilitar primero la replicación entre grid en todos sus bloques.
- Eliminar el permiso **Usar conexión de federación de cuadrícula** no elimina ningún elemento que ya se haya replicado entre las cuadrículas. Por ejemplo, los usuarios, grupos y objetos de arrendatarios que existen en ambas cuadrículas no se eliminan de ninguna de las cuadrículas cuando se elimina el permiso del arrendatario. Si desea eliminar estos elementos, debe eliminarlos manualmente de ambas cuadrículas.
- Si desea volver a habilitar este permiso con la misma conexión de federación de grid, suprima primero este inquilino en la cuadrícula de destino; de lo contrario, si vuelve a habilitar este permiso, se producirá un error.

Al volver a habilitar el permiso **Usar conexión de federación de grid**, la cuadrícula local se convierte en la cuadrícula de origen y activa la clonación en la cuadrícula remota especificada por la conexión de federación de grid seleccionada. Si la cuenta de inquilino ya existe en la cuadrícula remota, la clonación provocará un error de conflicto.

Antes de empezar

- Está utilizando una "navegador web compatible".
- Dispone de "Permiso de acceso raíz" para ambas cuadrículas.

Desactive la replicación para bloques de clientes

Como primer paso, deshabilite la replicación entre grid para todos los buckets de inquilinos.

Pasos

1. A partir de cualquier cuadrícula, inicie sesión en Grid Manager desde el nodo de administración principal.
2. Seleccione **Configuración** > **Sistema** > **Federación de red**.
3. Seleccione el nombre de la conexión para mostrar sus detalles.
4. En la pestaña **Arrendatarios permitidos**, determine si el inquilino está usando la conexión.
5. Si el arrendatario aparece en la lista, indíquele que lo "desactive la replicación entre grid"haga para todos sus cubos en ambas cuadrículas de la conexión.

No puede eliminar el permiso **Usar conexión de federación de grid** si algún depósito de inquilino tiene habilitada la replicación entre grid. El inquilino debe deshabilitar la replicación entre grid en sus buckets en ambas grids.

Eliminar permiso para arrendatario

Una vez deshabilitada la replicación entre grid para bloques de inquilinos, puede eliminar el permiso del inquilino para utilizar la conexión de federación de grid.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Elimine el permiso de las páginas Grid federation o Tenants.

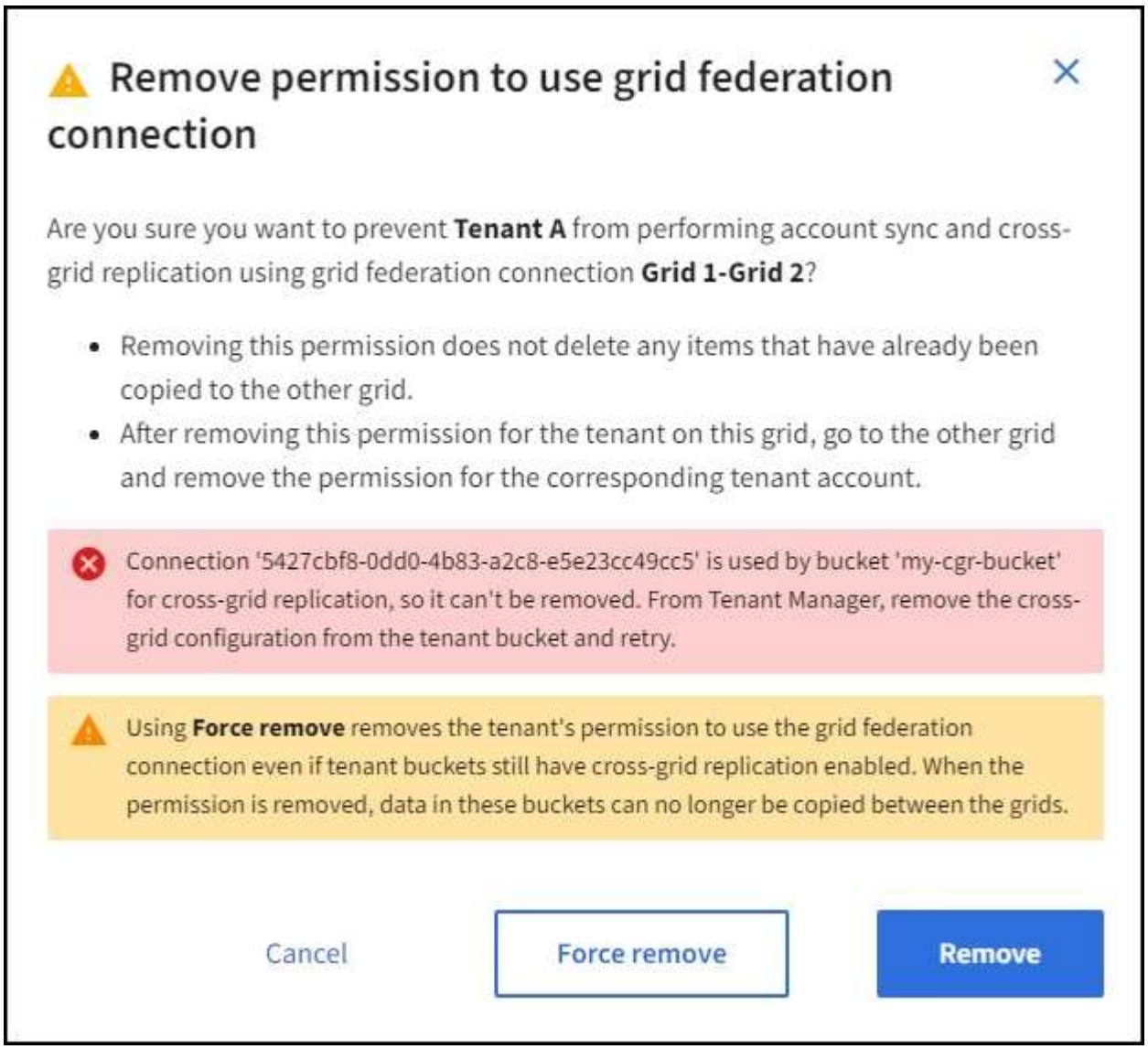
Página de federación de grid

a. Seleccione **Configuración** > **Sistema** > **Federación de red**.
b. Seleccione el nombre de la conexión para mostrar su página de detalles.
c. En la pestaña **Arrendatarios permitidos**, seleccione el botón de radio para el inquilino.
d. Selecciona **Eliminar permiso**.

Inquilinos

a. Seleccione **Inquilinos**.
b. Seleccione el nombre del arrendatario para mostrar la página de detalles.
c. En la pestaña **Grid federation**, seleccione el botón de radio para la conexión.
d. Selecciona **Eliminar permiso**.

3. Revise las advertencias en el cuadro de diálogo de confirmación y seleccione **Eliminar**.
   - Si el permiso se puede eliminar, volverá a la página de detalles y aparecerá un mensaje de éxito. Este inquilino ya no puede utilizar la conexión de federación de grid.
   - Si uno o más bloques de inquilinos aún tienen habilitada la replicación entre grid, se muestra un error.



   Puede realizar una de las siguientes acciones:

   - (Recomendado). Inicie sesión en el Gestor de inquilinos y deshabilite la replicación para cada uno de los buckets del inquilino. Consulte "Gestionar la replicación entre grid". Luego, repita los pasos para eliminar el permiso **Usar conexión a la cuadrícula**.
   - Elimine el permiso por la fuerza. Consulte la siguiente sección.
4. Vaya a la otra cuadrícula y repita estos pasos para eliminar el permiso para el mismo inquilino en la otra cuadrícula.

Elimine el permiso por la fuerza

Si es necesario, puede forzar la eliminación del permiso de un inquilino para utilizar una conexión de federación de grid incluso si los buckets de inquilinos tienen habilitada la replicación entre grid.

Antes de eliminar el permiso de un inquilino por la fuerza, tenga en cuenta las consideraciones generales paraeliminando el permiso, así como las siguientes consideraciones adicionales:

- Si elimina el permiso **Usar conexión de federación de grid** por fuerza, cualquier objeto que esté pendiente de replicación en la otra cuadrícula (ingerido pero no replicado aún) seguirá siendo replicado. Para evitar que estos objetos en curso lleguen al depósito de destino, también debe eliminar el permiso del inquilino en la otra cuadrícula.
- Cualquier objeto ingerido en el depósito de origen después de eliminar el permiso **Usar conexión de federación de grid** nunca se replicará en el depósito de destino.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Seleccione **Configuración** > **Sistema** > **Federación de red**.
3. Seleccione el nombre de la conexión para mostrar su página de detalles.
4. En la pestaña **Arrendatarios permitidos**, seleccione el botón de radio para el inquilino.
5. Selecciona **Eliminar permiso**.
6. Revise las advertencias en el cuadro de diálogo de confirmación y seleccione **Forzar eliminación**.

   Aparece un mensaje de éxito. Este inquilino ya no puede utilizar la conexión de federación de grid.

7. Según sea necesario, vaya a la otra cuadrícula y repita estos pasos para forzar la eliminación del permiso para la misma cuenta de inquilino en la otra cuadrícula. Por ejemplo, debe repetir estos pasos en la otra cuadrícula para evitar que los objetos en curso lleguen al depósito de destino.

Solucionar errores de federación de grid

Es posible que deba solucionar alertas y errores relacionados con las conexiones de federación de grid, el clon de cuenta y la replicación entre grid.

Alertas y errores de conexión de federación de grid

Es posible que reciba alertas o se produzcan errores con las conexiones de federación de grid.

Después de realizar cualquier cambio para resolver un problema de conexión, pruebe la conexión para asegurarse de que el estado de la conexión vuelva a **CONECTADA**. Para obtener instrucciones, consulte "Gestionar conexiones de federación de grid".

Alerta de fallo de conexión de federación de grid

Problema

Se ha activado la alerta de error de conexión **Grid federation**.

Detalles

Esta alerta indica que la conexión de federación de rejilla entre las cuadrículas no funciona.

Acciones recomendadas

1. Revise la configuración en la página Grid Federation para ambas cuadrículas. Confirme que todos los valores son correctos. Consulte "Gestionar conexiones de federación de grid".
2. Revise los certificados utilizados para la conexión. Asegúrese de que no haya alertas para los certificados de federación de grid vencidos y que los detalles de cada certificado sean válidos. Consulte las

instrucciones para rotar certificados de conexión en "Gestionar conexiones de federación de grid".

3. Confirme que todos los nodos ADMIN y Gateway de ambas cuadrículas están en línea y disponibles. Resuelva las alertas que puedan estar afectando a estos nodos y vuelva a intentarlo.
4. Si proporcionó un nombre de dominio completo (FQDN) para la cuadrícula local o remota, confirme que el servidor DNS esté en línea y disponible. "¿Qué es GRID federation?"Consulte para ver los requisitos de redes, dirección IP y DNS.

La alerta de caducidad del certificado de federación de grid

Problema

Se activó la alerta **Expiración del certificado de federación de red**.

Detalles

Esta alerta indica que uno o más certificados de federación de grid están a punto de caducar.

Acciones recomendadas

Consulte las instrucciones para rotar certificados de conexión en "Gestionar conexiones de federación de grid".

Error al editar una conexión de federación de cuadrícula

Problema

Al editar una conexión de federación de grid, aparece el siguiente mensaje de advertencia cuando selecciona **Guardar y probar**: “No se pudo crear un archivo de configuración de candidato en uno o más nodos”.

Detalles

Cuando edita una conexión de federación de grid, StorageGRID intenta guardar un archivo de configuración de candidato en todos los nodos de administración de la primera cuadrícula. Aparece un mensaje de advertencia si este archivo no se puede guardar en todos los nodos de administración, por ejemplo, porque un nodo de administración está fuera de línea.

Acciones recomendadas

1. Desde la cuadrícula que está utilizando para editar la conexión, seleccione **Nodos**.
2. Confirmar que todos los nodos de administración de ese grid están en línea.
3. Si alguno de los nodos está sin conexión, vuelva a conectarlo e intente editar nuevamente la conexión.

Errores de clonación de cuenta

No se puede iniciar sesión en una cuenta de inquilino clonada

Problema

No puede iniciar sesión en una cuenta de inquilino clonada. El mensaje de error de la página de inicio de sesión del gestor de inquilinos indica que las credenciales de esta cuenta no son válidas. Inténtelo de nuevo.

Detalles

Por motivos de seguridad, cuando se clona una cuenta de inquilino desde la cuadrícula de origen del inquilino a la cuadrícula de destino del inquilino, la contraseña que configuró para el usuario raíz local del inquilino no se clona. De la misma forma, cuando un inquilino crea usuarios locales en su grid de origen, las contraseñas de usuario local no se clonan en el grid de destino.

Acciones recomendadas

Antes de que el usuario root pueda iniciar sesión en la cuadrícula de destino del inquilino, un administrador de grid debe primero en "cambie la contraseña del usuario raíz local"la cuadrícula de destino.

Antes de que un usuario local clonado pueda iniciar sesión en la red de destino del inquilino, el usuario raíz del inquilino clonado debe agregar una contraseña para el usuario en la red de destino. Para obtener instrucciones, consulte"Gestionar usuarios" en las instrucciones para utilizar el Administrador de inquilinos.

Inquilino creado sin un clon

Problema

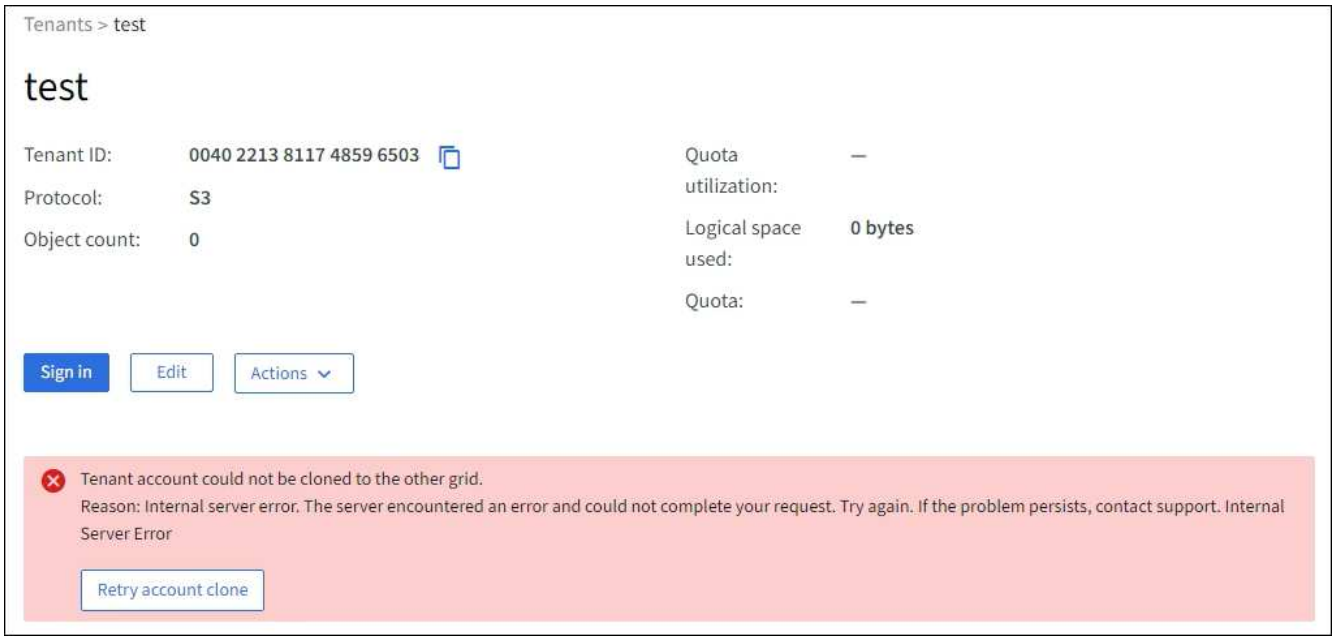
Puede ver el mensaje “Tenant created without a clone” después de crear un nuevo inquilino con el permiso **use grid federation connection**.

Detalles

Este problema puede ocurrir si las actualizaciones del estado de conexión se retrasan, lo que podría provocar que una conexión no saludable se listara como **Connected**.

Acciones recomendadas

1. Revise el motivo que aparece en el mensaje de error y resuelva cualquier problema de red u otros problemas que puedan impedir el funcionamiento de la conexión. Consulte Alertas y errores de conexión de federación de grid.
2. Siga las instrucciones para probar una conexión de federación de rejilla en "Gestionar conexiones de federación de grid" para confirmar que se ha solucionado el problema.
3. Desde la cuadrícula de origen del inquilino, seleccione **Inquilinos**.
4. Localice la cuenta de inquilino que no se pudo clonar.
5. Seleccione el nombre del arrendatario para mostrar la página de detalles.
6. Seleccione **Reintentar clon de cuenta**.



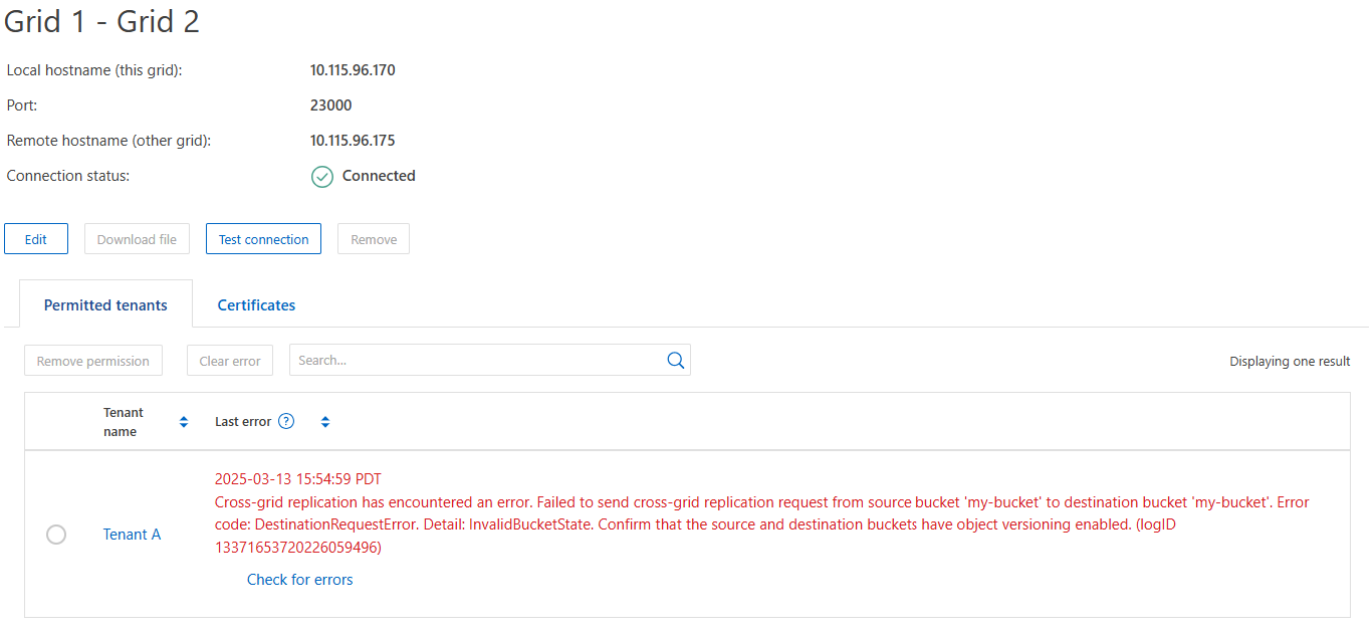
Si se ha resuelto el error, la cuenta de inquilino se clonará ahora en la otra cuadrícula.

Alertas y errores de replicación entre grid

Último error mostrado para conexión o arrendatario

Problema

Cuando "visualización de una conexión de federación de grid" (o cuando "gestión de los inquilinos permitidos" se trata de una conexión), nota un error en la columna **Último error** de la página de detalles de la conexión. Por ejemplo:



Detalles

Para cada conexión de federación de red, la columna **Último error** muestra el error más reciente que ocurrió, si lo hubo, cuando los datos de un inquilino se estaban replicando a la otra red. Esta columna muestra únicamente el último error de replicación entre redes que ocurrió; no se muestran los errores anteriores que podrían haber ocurrido. Un error en esta columna podría ocurrir por una de estas razones:

- No se encontró la versión del objeto de origen.
- No se encontró el depósito de origen.
- Se ha suprimido el depósito de destino.
- Una cuenta diferente ha vuelto a crear el bloque de destino.
- Se ha suspendido el control de versiones del bloque de destino.
- La misma cuenta ha vuelto a crear el depósito de destino, pero ahora no tiene versiones.
- El objeto de origen tiene configuraciones de bloqueo de objetos S3 que no cumplen con las configuraciones de retención a nivel de inquilino de la red de destino.
- El objeto de origen tiene configuraciones de Bloqueo de objetos S3, y el Bloqueo de objetos S3 está deshabilitado en el depósito de destino.

Acciones recomendadas

Si aparece un mensaje de error en la columna **Último error**, siga estos pasos:

1. Revise el texto del mensaje.
2. Realice las acciones recomendadas. Por ejemplo, si se suspendió el control de versiones en el bloque de

destino para la replicación entre grid, vuelva a habilitar el control de versiones para ese bloque.

3. Seleccione la conexión o la cuenta de inquilino de la tabla.
4. Seleccione **Borrar error**.
5. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espere 5-6 minutos e incorpore un objeto nuevo en el bloque. Confirme que el mensaje de error no vuelve a aparecer.

   Para asegurarse de que el mensaje de error se borra, espere al menos 5 minutos después de la marca de tiempo del mensaje antes de introducir un nuevo objeto.

   Después de borrar el error, puede aparecer un nuevo **last error** si los objetos se ingieren en un depósito diferente que también tiene un error.

7. Para determinar si se ha producido un fallo en la replicación de algún objeto debido al error del depósito, consulte "Identifique y vuelva a intentar operaciones de replicación fallidas".

Alerta de error permanente de replicación entre grid

Problema

Se activó la alerta de error permanente de replicación cruzada de la red*.

Detalles

Esta alerta indica que los objetos de arrendatario no se pueden replicar entre los buckets de dos cuadrículas por un motivo que requiere la intervención del usuario para resolverlos. Esta alerta suele deberse a un cambio en el depósito de origen o de destino.

Acciones recomendadas

1. Inicie sesión en la cuadrícula donde se activó la alerta.
2. Vaya a **Configuración** > **Sistema** > **Federación de red** y localice el nombre de la conexión que aparece en la alerta.
3. En la pestaña de inquilinos permitidos, mire la columna **Último error** para determinar qué cuentas de inquilino tienen errores.
4. Para obtener más información sobre el fallo, consulte las instrucciones de "Supervisar las conexiones de federación de grid" para revisar las métricas de replicación entre grid.
5. Para cada cuenta de inquilino afectada:
   a. Consulte las instrucciones de la "Supervise la actividad de los inquilinos"para confirmar que el inquilino no ha superado su cuota en la cuadrícula de destino para la replicación entre grid.
   b. Según sea necesario, aumente la cuota del inquilino en la cuadrícula de destino para permitir guardar nuevos objetos.
6. Para cada inquilino afectado, inicie sesión en el Gestor de inquilinos en ambas cuadrículas, de modo que pueda comparar la lista de bloques.
7. Para cada bloque que tiene habilitada la replicación entre grid, confirme lo siguiente:
   - Hay un depósito correspondiente para el mismo inquilino en la otra cuadrícula (debe usar el nombre exacto).
   - Ambos cubos tienen activado el control de versiones de objetos (el control de versiones no se puede suspender en ninguna cuadrícula).

- Ninguno de los depósitos está en el estado **Deleting objects: Read-only**.

8. Para confirmar que se ha resuelto el problema, consulte las instrucciones de "Supervisar las conexiones de federación de grid" para revisar las métricas de replicación entre grid o realice estos pasos:

   a. Vuelva a la página Grid federation.
   b. Seleccione el inquilino afectado y seleccione **Borrar error** en la columna **Último error**.
   c. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
   d. Espere 5-6 minutos e incorpore un objeto nuevo en el bloque. Confirme que el mensaje de error no vuelve a aparecer.

   > Para asegurarse de que el mensaje de error se borra, espere al menos 5 minutos después de la marca de tiempo del mensaje antes de introducir un nuevo objeto.

   > Puede que la alerta tarde hasta un día en borrarse una vez que se resuelve.

   a. Vaya a "Identifique y vuelva a intentar operaciones de replicación fallidas" para identificar cualquier objeto o eliminar marcadores que no se hayan podido replicar en la otra cuadrícula y para volver a intentar la replicación según sea necesario.

Alerta no disponible del recurso de replicación entre grid

Problema

Se activó la alerta **Cross-grid replication resource unavailable**.

Detalles

Esta alerta indica que las solicitudes de replicación entre grid están pendientes porque un recurso no está disponible. Por ejemplo, puede haber un error de red.

Acciones recomendadas

1. Supervise la alerta para ver si el problema se resuelve por sí solo.
2. Si el problema persiste, determine si cualquiera de las redes tiene una alerta de **Error de conexión de federación de red** para la misma conexión o una alerta de **No se puede comunicar con el nodo** para un nodo. Es posible que esta alerta se resuelva al resolver esas alertas.
3. Para obtener más información sobre el fallo, consulte las instrucciones de "Supervisar las conexiones de federación de grid" para revisar las métricas de replicación entre grid.
4. Si no puede resolver la alerta, póngase en contacto con el soporte técnico.

La replicación entre cuadrículas continuará con normalidad una vez resuelto el problema.

Identifique y vuelva a intentar operaciones de replicación fallidas

Después de resolver la alerta de error permanente * de replicación entre redes, debe determinar si algún objeto o marcador de borrado no se pudo replicar en la otra cuadrícula. A continuación, puede volver a ingerir estos objetos o utilizar la API de administración de grid para volver a intentar la replicación.

La alerta de error permanente * de replicación cruzada de la red indica que los objetos del inquilino no se pueden replicar entre los depósitos en dos cuadrículas por una razón que requiere la intervención del usuario para resolverlos. Esta alerta suele deberse a un cambio en el depósito de origen o de destino. Para obtener

más información, consulte "Solucionar errores de federación de grid".

Determine si se ha producido un fallo en la replicación de algún objeto

Para determinar si algún objeto o marcador de borrado no se ha replicado en la otra cuadrícula, puede buscar mensajes en el registro de auditoría"CGRR (Solicitud de Replicación entre Grid)". Este mensaje se agrega al registro cuando StorageGRID no puede replicar un objeto, un objeto multiparte o un marcador de eliminación en el bloque de destino.

Puede utilizar "herramienta audit-explain"para traducir los resultados a un formato más fácil de leer.

Antes de empezar

- Tiene permiso de acceso raíz.
- Tiene el `Passwords.txt` archivo.
- Conoce la dirección IP del nodo de administración principal.

Pasos

1. 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 el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a raíz: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

   Al iniciar sesión como root, la petición de datos cambia de `$` a `#`.

2. Busque en audit.log mensajes CGRR y utilice la herramienta audit-explain para dar formato a los resultados.

   Por ejemplo, este comando greps para todos los mensajes CGRR en los últimos 30 minutos y utiliza la herramienta audit-explain.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   Los resultados del comando se parecerán a este ejemplo, que tiene entradas para seis mensajes CGRR. En el ejemplo, todas las solicitudes de replicación entre grid devolvieron un error general porque el objeto no se pudo replicar. Los tres primeros errores son para las operaciones de «objeto de réplica», y los tres últimos errores son para las operaciones de «marcador de borrado de réplica».

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Cada entrada contiene la siguiente información:

Campo	Descripción
Solicitud de Replicación de Cuadrícula Cruzada de CGRR	Nombre de la solicitud
inquilino	El ID de cuenta del inquilino
conexión	El ID de la conexión de federación de grid
funcionamiento	Tipo de operación de replicación que se intentó: • replicar objeto • replicar marcador de borrado • replicar objeto de varias partes
cucharón	El nombre del cubo
objeto	El nombre del objeto
versión	El ID de versión del objeto

Campo	Descripción
error	Tipo de error. Si se produce un error en la replicación entre cuadrículas, el error es Error general.

Vuelva a intentar las replicaciones fallidas

Después de generar una lista de objetos y de eliminar marcadores que no se han replicado en el depósito de destino y resolver los problemas subyacentes, puede volver a intentar la replicación de una de las dos formas siguientes:

- Vuelva a ingerir cada objeto en el bloque de origen.
- Utilice la API privada de Grid Management, tal y como se describe.

Pasos

1. En la parte superior de Grid Manager, selecciona el icono de ayuda y selecciona **Documentación de API**.
2. Seleccione **Ir a documentación privada de API**.

   > Los extremos de la API de StorageGRID marcados como «privados» están sujetos a cambios sin previo aviso. Los extremos privados de StorageGRID también ignoran la versión de API de la solicitud.

3. En la sección **cross-grid-replication-advanced**, seleccione el siguiente punto final:

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Seleccione **probar**.
5. En el cuadro de texto **body**, reemplace la entrada de ejemplo para **versionID** por un ID de versión del audit.log que corresponda a una solicitud fallida de replicación cruzada.

   Asegúrese de conservar las comillas dobles alrededor de la cadena.

6. Seleccione **Ejecutar**.
7. Confirme que el código de respuesta del servidor es **204**, lo que indica que el objeto o marcador de borrado se ha marcado como pendiente para la replicación de cuadrícula cruzada a la otra cuadrícula.

   > Pendiente significa que la solicitud de replicación entre grid se ha agregado a la cola interna para su procesamiento.

Supervisar reintentos de replicación

Debe supervisar las operaciones de reintento de replicación para asegurarse de que se completen.

> Puede que un objeto o marcador de eliminación tarde varias horas o más en la otra cuadrícula.

Es posible supervisar las operaciones de reintento de dos maneras:

- Utilice un S3 "Objeto principal" o "GetObject" una solicitud. La respuesta incluye el encabezado de respuesta específico de StorageGRID `x-ntap-sg-cgr-replication-status`, que tendrá uno de los

siguientes valores:

Cuadrícula	Estado de replicación
Origen	• **COMPLETADO**: La replicación fue exitosa. • **PENDIENTE**: El objeto aún no ha sido replicado. • **FALLO**: La replicación falló con un fallo permanente. Un usuario debe resolver el error.
Destino	**REPLICA**: El objeto fue replicado desde la cuadrícula de origen.

- Utilice la API privada de Grid Management, tal y como se describe.

Pasos

1. En la sección **cross-grid-replication-advanced** de la documentación de la API privada, seleccione el siguiente punto final:

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. Seleccione **probar**.
3. En la sección Parámetro, introduzca el ID de versión que utilizó en la `cross-grid-replication-retry-failed` solicitud.
4. Seleccione **Ejecutar**.
5. Confirme que el código de respuesta del servidor es **200**.
6. Revise el estado de replicación, que será uno de los siguientes:
   - **PENDIENTE**: El objeto aún no ha sido replicado.
   - **COMPLETADO**: La replicación fue exitosa.
   - **ERROR**: La replicación falló con un fallo permanente. Un usuario debe resolver el error.

Gestionar la seguridad

Gestionar la seguridad

Puede configurar varias opciones de seguridad desde Grid Manager para ayudar a proteger el sistema StorageGRID.

Gestione el cifrado

StorageGRID ofrece varias opciones para el cifrado de datos. "revise los métodos de cifrado disponibles"Debe determinar cuáles cumplen con sus requisitos de protección de datos.

Gestionar certificados

Puede "configurar y gestionar los certificados de servidor" utilizar para conexiones HTTP o los certificados de cliente utilizados para autenticar una identidad de cliente o usuario en el servidor.

Configuración de servidores de gestión de claves

El uso de A "servidor de gestión de claves"permite proteger los datos de StorageGRID incluso si se ha quitado un dispositivo del centro de datos. Una vez que se han cifrado los volúmenes del dispositivo, no podrá acceder a ningún dato del dispositivo a menos que el nodo se pueda comunicar con el KMS.

> Para utilizar la administración de claves de cifrado, debe activar el ajuste **cifrado de nodos** para cada dispositivo durante la instalación, antes de agregar el dispositivo a la cuadrícula.

Administrar la configuración de proxy

Si utiliza servicios de plataforma S3 o pools de Cloud Storage, puede configurar "servidor proxy de almacenamiento"un entre nodos de almacenamiento y los extremos externos S3. Si envía paquetes AutoSupport con HTTPS o HTTP, puede configurar una "servidor proxy de administración" entre nodos de administrador y el soporte técnico.

Controle los firewalls

Para mejorar la seguridad de su sistema, puede controlar el acceso a los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en la "firewall externo". También puede controlar el acceso de red a cada nodo configurando su "firewall interno". Puede evitar el acceso a todos los puertos, excepto a los necesarios para la implementación.

Consulte los métodos de cifrado de StorageGRID

StorageGRID ofrece varias opciones para el cifrado de datos. Debe revisar los métodos disponibles para determinar qué métodos cumplen sus requisitos de protección de datos.

La tabla proporciona un resumen de alto nivel de los métodos de cifrado disponibles en StorageGRID.

Opción de cifrado	Cómo funciona	Se aplica a.
Servidor de gestión de claves (KMS) en Grid Manager	"configurar un servidor de gestión de claves"Para el sitio StorageGRID y "habilite el cifrado de nodos para el dispositivo". A continuación, un nodo de dispositivo se conecta al KMS para solicitar una clave de cifrado (KEK). Esta clave cifra y descifra la clave de cifrado de datos (DEK) en cada volumen.	Nodos de dispositivo con **cifrado de nodos** activado durante la instalación. Todos los datos del dispositivo están protegidos frente a la pérdida física o la eliminación del centro de datos. **Nota**: La gestión de claves de cifrado con un KMS solo es compatible con los nodos de almacenamiento y los dispositivos de servicios.

Opción de cifrado	Cómo funciona	Se aplica a.
Página de cifrado de unidades de Installer de dispositivos de StorageGRID	Si el dispositivo contiene unidades que admiten el cifrado de hardware, puede establecer una frase de acceso de la unidad durante la instalación. Cuando se configura una clave de acceso de la unidad, es imposible que nadie recupere datos válidos de las unidades que se han eliminado del sistema, a menos que conozcan la clave de acceso. Antes de iniciar la instalación, vaya a **Configurar hardware** > **Cifrado de unidades** para establecer una frase de contraseña de la unidad que se aplique a todas las unidades de cifrado automático gestionadas por StorageGRID en un nodo.	Dispositivos que contienen unidades de autocifrado. Todos los datos de las unidades seguras están protegidos frente a la pérdida física o eliminación del centro de datos. El cifrado de unidades no se aplica a las unidades gestionadas por SANtricity. Si tiene un dispositivo de almacenamiento con unidades de cifrado automático y controladoras SANtricity, puede habilitar la seguridad de unidades en SANtricity.
Drive Security en SANtricity System Manager	Si la función Drive Security está habilitada para el dispositivo StorageGRID, se puede usar "Administrador del sistema de SANtricity" para crear y gestionar la clave de seguridad. Se requiere la clave para acceder a los datos en las unidades seguras.	Los dispositivos de almacenamiento que tienen unidades de cifrado de disco completo (FDE) o unidades de autocifrado. Todos los datos de las unidades seguras están protegidos frente a la pérdida física o eliminación del centro de datos. No se puede usar con algunos dispositivos de almacenamiento ni con ningún dispositivo de servicios.
Cifrado de objetos almacenados	Puede activar "Cifrado de objetos almacenados"la opción en Grid Manager. Cuando se habilita, todos los objetos nuevos que no se cifren a nivel de bucket o de objeto se cifran durante la ingesta.	Datos de objetos S3 recién ingeridos. Los objetos almacenados existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados.

Opción de cifrado	Cómo funciona	Se aplica a.
Cifrado de bloques de S3	Emite una solicitud PutBucketEncryption para habilitar el cifrado para el depósito. Todos los objetos nuevos que no se cifren en el nivel de objeto se cifran durante la ingesta.	Solo datos de objetos S3 procesados recientemente. Debe especificarse el cifrado para el bloque. Los objetos de cubo existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados. "Operaciones en bloques"
Cifrado del lado del servidor de objetos S3 (SSE)	Emite una solicitud S3 para almacenar un objeto e incluir `x-amz-server-side-encryption` la cabecera de solicitud.	Solo datos de objetos S3 procesados recientemente. Se debe especificar el cifrado para el objeto. Los metadatos de los objetos y otros datos confidenciales no están cifrados. StorageGRID gestiona las claves. "Usar cifrado del servidor"
Cifrado del lado del servidor de objetos S3 con claves proporcionadas por el cliente (SSE-C)	Se emite una solicitud S3 para almacenar un objeto e incluir tres encabezados de solicitud. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Solo datos de objetos S3 procesados recientemente. Se debe especificar el cifrado para el objeto. Los metadatos de los objetos y otros datos confidenciales no están cifrados. Las claves se gestionan fuera de StorageGRID. "Usar cifrado del servidor"
Cifrado de volúmenes o almacenes de datos externos	Si la plataforma de implementación lo admite, puede utilizar un método de cifrado fuera de StorageGRID para cifrar un volumen o almacén de datos completo.	Todos los datos de objetos, metadatos y datos de configuración del sistema, suponiendo que se cifre cada volumen o almacén de datos. Un método de cifrado externo proporciona un control más estricto sobre los algoritmos y claves de cifrado. Se puede combinar con los otros métodos enumerados.

Opción de cifrado	Cómo funciona	Se aplica a.
Cifrado de objetos fuera de StorageGRID	Se utiliza un método de cifrado fuera de StorageGRID para cifrar los metadatos y los datos de objetos antes de que se ingieran en StorageGRID.	Solo datos de objetos y metadatos (los datos de configuración del sistema no están cifrados). Un método de cifrado externo proporciona un control más estricto sobre los algoritmos y claves de cifrado. Se puede combinar con los otros métodos enumerados. "Amazon Simple Storage Service - Guía del usuario: Protección de datos mediante cifrado del lado del cliente"

Utilice varios métodos de cifrado

En función de los requisitos, puede utilizar más de un método de cifrado a la vez. Por ejemplo:

- Se puede usar un KMS para proteger los nodos del dispositivo y también para usar la función de seguridad de la unidad en el administrador del sistema de SANtricity para «cifrar dos veces» los datos en las unidades de autocifrado del mismo dispositivo.
- Puede utilizar un KMS para proteger los datos en los nodos del dispositivo y también utilizar la opción de cifrado de objetos almacenados para cifrar todos los objetos cuando se ingieren.

Si solo una pequeña parte de los objetos requiere cifrado, considere la posibilidad de controlar el cifrado en el nivel de bloque o de objeto individual. Habilitar varios niveles de cifrado tiene un coste de rendimiento adicional.

Información relacionada

"Conozca las opciones de cifrado con certificación FIPS"

Gestionar certificados

Gestionar certificados de seguridad

Los certificados de seguridad son archivos de datos pequeños que se utilizan para crear conexiones seguras y de confianza entre componentes de StorageGRID y entre componentes de StorageGRID y sistemas externos.

StorageGRID utiliza dos tipos de certificados de seguridad:

- **Se requieren certificados de servidor** cuando se utilizan conexiones HTTPS. Los certificados de servidor se utilizan para establecer conexiones seguras entre clientes y servidores, autenticar la identidad de un servidor a sus clientes y proporcionar una ruta de comunicación segura para los datos. Cada servidor y el cliente tienen una copia del certificado.
- **Los certificados de cliente** autentican una identidad de cliente o usuario al servidor, proporcionando una autenticación más segura que las contraseñas solamente. Los certificados de cliente no cifran datos.

Cuando un cliente se conecta al servidor mediante HTTPS, el servidor responde con el certificado del servidor,

que contiene una clave pública. El cliente compara la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión con el servidor utilizando la misma clave pública.

StorageGRID funciona como servidor para algunas conexiones (como el extremo de equilibrio de carga) o como cliente para otras conexiones (como el servicio de replicación de CloudMirror).

Certificado de CA de cuadrícula predeterminado

StorageGRID tiene una autoridad de certificación (CA) incorporada que genera un certificado CA de Grid interno durante la instalación del sistema. El certificado CA de Grid se utiliza, de forma predeterminada, para proteger el tráfico interno de StorageGRID . Una autoridad de certificación (CA) externa puede emitir certificados personalizados que cumplan totalmente con las políticas de seguridad de la información de su organización.

Utilice el certificado CA de Grid para entornos que no sean de producción. Para la producción, utilice certificados personalizados firmados por una autoridad de certificación externa. Se admiten conexiones no seguras sin certificado, pero no se recomiendan.

- Los certificados de CA personalizados no eliminan los certificados internos; sin embargo, los certificados personalizados deben ser los especificados para verificar las conexiones del servidor.
- Todos los certificados personalizados deben cumplir con el "directrices de fortalecimiento del sistema para los certificados de servidor".
- StorageGRID admite la agrupación de certificados de una CA en un único archivo (conocido como paquete de certificados de CA).

> ⓘ StorageGRID también incluye certificados de CA del sistema operativo que son los mismos en todos los entornos Grid. En los entornos de producción, asegúrese de especificar un certificado personalizado firmado por una entidad de certificación externa en lugar del certificado de CA del sistema operativo.

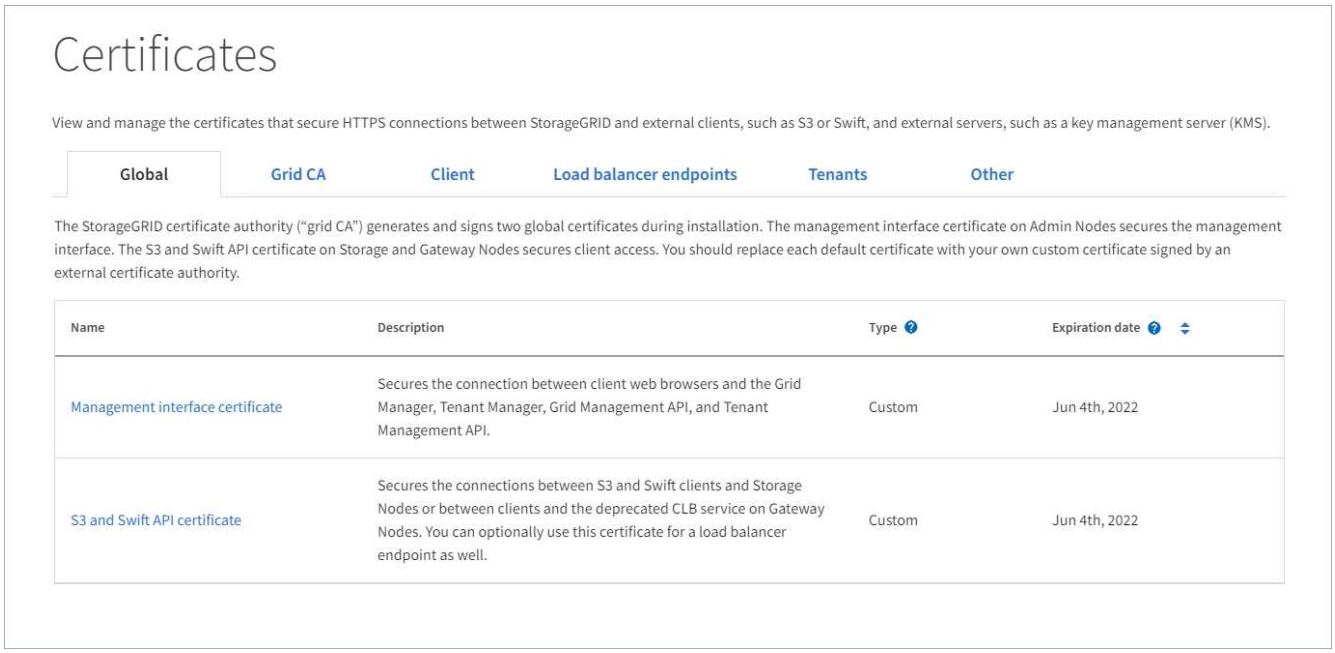
Las variantes de los tipos de certificado de servidor y cliente se implementan de varias maneras. Es necesario tener preparados todos los certificados necesarios para la configuración específica de StorageGRID antes de configurar el sistema.

Acceda a los certificados de seguridad

Puede acceder a información sobre todos los certificados de StorageGRID en una única ubicación, junto con enlaces al flujo de trabajo de configuración de cada certificado.

Pasos

1. Desde Grid Manager, seleccione **Configuración** > **Seguridad** > **Certificados**.



2. Seleccione una ficha en la página certificados para obtener información sobre cada categoría de certificado y para acceder a la configuración de certificado. Puede acceder a una pestaña si tiene el "permiso apropiado".

   - **Global**: Protege el acceso a StorageGRID desde navegadores web y clientes API externos.
   - **Grid CA**: Protege el tráfico interno de StorageGRID.
   - **Cliente**: Protege las conexiones entre clientes externos y la base de datos Prometheus de StorageGRID.
   - **Puntos Finales de Equilibrador de Carga**: Asegura las conexiones entre los clientes S3 y el Equilibrador de Carga StorageGRID.
   - **Arrendatarios**: Protege las conexiones a servidores de federación de identidades o desde extremos de servicio de plataforma a recursos de almacenamiento S3.
   - **Otros**: Protege las conexiones StorageGRID que requieren certificados específicos.

     Cada una de las pestañas se describe a continuación con enlaces a detalles de certificados adicionales.

Global

Los certificados globales protegen el acceso a StorageGRID desde exploradores web y clientes API S3 externos. La autoridad de certificados StorageGRID genera inicialmente dos certificados globales durante la instalación. La práctica recomendada para un entorno de producción es usar certificados personalizados firmados por una entidad de certificación externa.

- Certificado de interfaz de gestión: Protege las conexiones del navegador web del cliente a las interfaces de administración de StorageGRID.
- Certificado API S3: Protege las conexiones de API del cliente a los nodos de almacenamiento, nodos de administración y nodos de gateway, que las aplicaciones cliente S3 utilizan para cargar y descargar datos de objetos.

Entre la información sobre los certificados globales instalados se incluyen:

- **Nombre**: Nombre del certificado con enlace a la administración del certificado.
- **Descripción**
- **Tipo**: Personalizado o predeterminado. + debe usar siempre un certificado personalizado para mejorar la seguridad de la cuadrícula.
- **Fecha de vencimiento**: Si se utiliza el certificado predeterminado, no se muestra ninguna fecha de vencimiento.

Podrá:

- Sustituya los certificados predeterminados por certificados personalizados firmados por una autoridad de certificado externa para mejorar la seguridad de la cuadrícula:
  - "Reemplace el certificado de interfaz de gestión generado por StorageGRID predeterminado" Se utiliza para las conexiones de Grid Manager y de Tenant Manager.
  - "Reemplace el certificado API S3" Se utiliza para las conexiones de extremo del balanceador de carga y del nodo de almacenamiento (opcional).
- "Restaure el certificado de interfaz de gestión predeterminado".
- "Restaure el certificado API S3 predeterminado".
- "Use un script para generar un nuevo certificado de interfaz de gestión autofirmado".
- Copie o descargue el "certificado de interfaz de gestión" o "Certificado API S3".

CA de grid

El Certificado de CA de grid, generado por la autoridad de certificación de StorageGRID durante la instalación de StorageGRID, protege todo el tráfico interno de StorageGRID.

La información del certificado incluye la fecha de caducidad del certificado y el contenido del mismo.

Puedes"Copie o descargue el certificado de Grid CA", pero no puedes cambiarlo.

Cliente

Certificados de cliente, Generado por una autoridad de certificación externa, asegure las conexiones entre las herramientas de monitoreo externo y la base de datos de StorageGRID Prometheus.

La tabla de certificados tiene una fila para cada certificado de cliente configurado e indica si el certificado se puede utilizar para el acceso a la base de datos Prometheus, junto con la fecha de caducidad del certificado.

Podrá:

- "Cargar o generar un nuevo certificado de cliente."
- Seleccione un nombre de certificado para mostrar los detalles del certificado, donde podrá:
  - "Cambie el nombre del certificado de cliente."
  - "Establezca el permiso de acceso Prometheus."
  - "Cargue y reemplace el certificado de cliente."
  - "Copie o descargue el certificado de cliente."
  - "Quite el certificado de cliente."
- Seleccione **Acciones** para rápidamente "editar", "asociar"o "quitar" un certificado de cliente. Puede seleccionar hasta 10 certificados de cliente y eliminarlos a la vez utilizando **acciones** > **Quitar**.

Puntos finales del equilibrador de carga

Certificados de punto final de equilibrador de carga Proteja las conexiones entre los clientes S3 y el servicio de equilibrador de carga de StorageGRID en los nodos de la puerta de enlace y los nodos de administración.

La tabla de puntos finales de equilibrio de carga tiene una fila para cada punto final de equilibrio de carga configurado e indica si se está utilizando el certificado de API global S3 o un certificado de punto final de equilibrio de carga personalizado para el punto final. También se muestra la fecha de caducidad de cada certificado.

> Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Podrá:

- "Ver un punto final de equilibrio de carga", incluyendo sus detalles de certificado.
- "Especifique un certificado de extremo de equilibrio de carga para FabricPool."
- "Utilice el certificado API global S3" en lugar de generar un nuevo certificado de punto final del equilibrador de carga.

Clientes

Los inquilinos pueden usar certificados de servidor de federación de identidades o certificados de extremo de servicio de plataformaproteger sus conexiones con StorageGRID.

La tabla de arrendatarios tiene una fila para cada arrendatario e indica si cada arrendatario tiene permiso para utilizar su propio origen de identidad o servicios de plataforma.

Podrá:

- "Seleccione un nombre de inquilino para iniciar sesión en el Administrador de inquilinos"
- "Seleccione un nombre de inquilino para ver los detalles de la federación de identidades del inquilino"
- "Seleccione el nombre de un inquilino para ver los detalles de los servicios de la plataforma de inquilino"
- "Especifique un certificado de extremo de servicio de plataforma durante la creación del extremo"

Otros

StorageGRID utiliza otros certificados de seguridad con fines específicos. Estos certificados se enumeran por su nombre funcional. Otros certificados de seguridad incluyen:

- Certificados de Cloud Storage Pool
- Certificados de notificación de alertas por correo electrónico
- Certificados de servidor de syslog externos
- Certificados de conexión de federación de grid
- Certificados de federación de identidades
- Certificados de servidor de gestión de claves (KMS)
- Certificados de inicio de sesión único

La información indica el tipo de certificado que una función utiliza y sus fechas de vencimiento del certificado de servidor y cliente, según corresponda. Al seleccionar un nombre de función, se abre una pestaña del navegador en la que puede ver y editar los detalles del certificado.

> Solo puede ver y acceder a la información de otros certificados si tiene el "permiso apropiado".

Podrá:

- "Especifique un certificado de Cloud Storage Pool para S3, C2S S3 o Azure"
- "Especifique un certificado para notificaciones de alertas por correo electrónico"
- "Use un certificado para un servidor de syslog externo"
- "Rotar certificados de conexión de federación de cuadrícula"
- "Ver y editar un certificado de federación de identidades"
- "Cargar certificados de servidor de gestión de claves (KMS) y de cliente"
- "Especifique manualmente un certificado SSO para una confianza de parte de confianza"

Detalles del certificado de seguridad

Cada tipo de certificado de seguridad se describe a continuación, con enlaces a las instrucciones de implementación.

Certificado de interfaz de gestión

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los exploradores web del cliente y la interfaz de gestión de StorageGRID, lo que permite a los usuarios acceder a Grid Manager y al Gestor de inquilinos sin advertencias de seguridad. Este certificado también autentica las conexiones API de gestión de grid y API de gestión de inquilinos. Puede usar el certificado predeterminado creado durante la instalación o cargar un certificado personalizado.	**Configuración** > **Seguridad** > **Certificados**, seleccione la pestaña **Global** y luego seleccione **Certificado de interfaz de administración**	"Configure los certificados de interfaz de gestión"

Certificado API S3

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica las conexiones de clientes S3 seguras a un nodo de almacenamiento y a los extremos del balanceador de carga (opcional).	**Configuración** > **Seguridad** > **Certificados**, seleccione la pestaña **Global** y luego seleccione **Certificado API S3**	"Configure los certificados de API S3"

Certificado de CA de grid

Consulte la Descripción de certificado de CA de cuadrícula predeterminada.

Certificado de cliente de administrador

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Cliente	Instalado en cada cliente, lo que permite que StorageGRID autentique el acceso de los clientes externos. • Permite a los clientes externos autorizados acceder a la base de datos Prometheus de StorageGRID. • Permite una supervisión segura de StorageGRID mediante herramientas externas.	**Configuración** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**	"Configurar certificados de cliente"

Certificado de punto final de equilibrador de carga

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre clientes S3 y el servicio de equilibrador de carga de StorageGRID en los nodos de puerta de enlace y los nodos de administración. Puede cargar o generar un certificado de equilibrador de carga al configurar un extremo de equilibrador de carga. Las aplicaciones cliente utilizan el certificado de equilibrador de carga al conectarse a StorageGRID para guardar y recuperar datos de objeto. También puede usar una versión personalizada del certificado global Certificado API S3para autenticar las conexiones al servicio de Equilibrador de Carga. Si el certificado global se utiliza para autenticar las conexiones del equilibrador de carga, no es necesario cargar ni generar un certificado independiente para cada punto final del equilibrador de carga. **Nota:** el certificado utilizado para la autenticación del equilibrador de carga es el certificado más utilizado durante el funcionamiento normal de StorageGRID.	**Configuración** > **Red** > **Puntos finales del balanceador de carga**	• "Configurar puntos finales del equilibrador de carga" • "Cree un extremo de equilibrador de carga para FabricPool"

Certificado de extremo de Cloud Storage Pool

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión de un pool de almacenamiento en cloud de StorageGRID a una ubicación de almacenamiento externa, como S3 Glacier o el almacenamiento blob de Microsoft Azure. Se necesita un certificado diferente para cada tipo de proveedor de cloud.	**ILM** > **piscinas de almacenamiento**	"Cree un pool de almacenamiento en el cloud"

Certificado de notificación de alertas por correo electrónico

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre un servidor de correo electrónico SMTP y una StorageGRID que se usa para notificaciones de alerta. • Si las comunicaciones con el servidor SMTP requieren Transport Layer Security (TLS), debe especificar el certificado de CA del servidor de correo electrónico. • Especifique un certificado de cliente solo si el servidor de correo SMTP requiere certificados de cliente para la autenticación.	**Alertas** > **Configuración de correo electrónico**	"Configure notificaciones por correo electrónico para las alertas"

Certificado de servidor de syslog externo

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión TLS o RELP/TLS entre un servidor syslog externo que registra eventos en StorageGRID. **Nota:** no se requiere un certificado de servidor syslog externo para conexiones TCP, RELP/TCP y UDP a un servidor syslog externo.	**Configuración** > **Monitoreo** > **Servidor de auditoría y syslog**	"Use un servidor de syslog externo"

Certificado de conexión de la federación de cuadrícula

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autenticar y cifrar la información enviada entre el sistema de StorageGRID actual y otro grid en una conexión de federación de grid.	**Configuración** > **Sistema** > **Federación de red**	• "Crear conexiones de federación de grid" • "Rotar certificados de conexión"

Certificado de federación de identidades

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre StorageGRID y un proveedor de identidades externo, como Active Directory, OpenLDAP u Oracle Directory Server. Se utiliza para la federación de identidades, lo que permite que los grupos de administración y los usuarios sean gestionados por un sistema externo.	**Configuración** > **Control de acceso** > **Federación de identidades**	"Usar la federación de identidades"

Certificado de servidor de gestión de claves (KMS)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre StorageGRID y un servidor de gestión de claves (KMS) externo, que proporciona claves de cifrado a los nodos de los dispositivos StorageGRID.	**Configuración** > **Seguridad** > **Servidor de administración de claves**	"Añadir servidor de gestión de claves (KMS)"

Certificado de extremo de servicios de plataforma

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión desde el servicio de plataforma StorageGRID a un recurso de almacenamiento S3.	**Administrador de inquilinos** > **ALMACENAMIENTO (S3)** > **terminales de servicios de plataforma**	"Cree un extremo de servicios de plataforma" "Editar extremo de servicios de plataforma"

Certificado de inicio de sesión único (SSO)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los servicios de federación de identidades, como Active Directory Federation Services (AD FS), y StorageGRID, que se utilizan para solicitudes de inicio de sesión único (SSO).	**Configuración** > **Control de acceso** > **Inicio de sesión único**	"Configurar el inicio de sesión único"

Ejemplos de certificados

Ejemplo 1: Servicio de equilibrador de carga

En este ejemplo, StorageGRID actúa como servidor.

1. Se configura un extremo de equilibrador de carga y se carga o genera un certificado de servidor en StorageGRID.
2. Debe configurar una conexión de cliente S3 al extremo del equilibrador de carga y cargar el mismo certificado al cliente.
3. Cuando el cliente desea guardar o recuperar datos, se conecta al extremo de equilibrio de carga mediante HTTPS.

4. StorageGRID responde con el certificado de servidor, que contiene una clave pública y una firma basada en la clave privada.
5. El cliente compara la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión utilizando la misma clave pública.
6. El cliente envía datos de objeto a StorageGRID.

Ejemplo 2: Servidor de gestión de claves externo (KMS)

En este ejemplo, StorageGRID actúa como cliente.

1. Con el software de servidor de gestión de claves externo, configura StorageGRID como un cliente KMS y obtiene un certificado de servidor firmado por CA, un certificado de cliente público y la clave privada del certificado de cliente.
2. Con el Administrador de grid, configura un servidor KMS y carga los certificados de servidor y cliente y la clave privada de cliente.
3. Cuando un nodo StorageGRID necesita una clave de cifrado, realiza una solicitud al servidor KMS que incluye datos del certificado y una firma basada en la clave privada.
4. El servidor KMS valida la firma del certificado y decide que puede confiar en StorageGRID.
5. El servidor KMS responde mediante la conexión validada.

Tipos de certificado de servidor admitidos

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

> El tipo de cifrado de la política de seguridad debe coincidir con el tipo de certificado del servidor. Por ejemplo, los cifrados RSA requieren certificados RSA y los cifrados ECDSA requieren certificados ECDSA. Consulte "Gestionar certificados de seguridad". Si configura una política de seguridad personalizada que no es compatible con el certificado del servidor, puede "vuelva temporalmente a la política de seguridad predeterminada".

Para obtener más información sobre cómo StorageGRID protege las conexiones de cliente, consulte "Seguridad para clientes S3".

Configure los certificados de interfaz de gestión

Puede reemplazar el certificado de interfaz de gestión predeterminado por un único certificado personalizado que permite a los usuarios acceder a Grid Manager y al Gestor de inquilinos sin tener que encontrar advertencias de seguridad. También puede revertir al certificado de interfaz de gestión predeterminado o generar una nueva.

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 una sola clave privada correspondiente y un certificado de interfaz de gestión personalizado común.

Dado que se utiliza un único certificado de interfaz de gestión 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 la CA de cuadrícula en el explorador Web que utilizarán para acceder a Grid Manager y al gestor de inquilinos.

Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, se activa la alerta **Expiración del certificado de servidor para la interfaz de administración** cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **Configuración** > **Seguridad** > **Certificados** y mirando la fecha de vencimiento del certificado de la interfaz de administración en la pestaña Global.

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 de la interfaz de gestión personalizada caduca.
- Ustedrevertir de un certificado de interfaz de gestión personalizado al certificado de servidor predeterminado.

Añada un certificado de interfaz de gestión personalizado

Para agregar un certificado de interfaz de gestión personalizado, puede proporcionar su propio certificado o generar uno mediante el Gestor de cuadrícula.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **utilizar certificado personalizado**.
4. Cargue o genere el certificado.

Cargue el certificado

Cargue los archivos de certificado de servidor requeridos.

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

- **Certificado de servidor**: El archivo de certificado de servidor personalizado (codificado con PEM).
- **Clave privada del certificado**: 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 opcional 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.

c. Expanda **Detalles del certificado** para ver los metadatos de cada certificado que haya cargado. Si cargó un paquete de CA opcional, cada certificado aparece en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

  Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

d. Seleccione **Guardar**. + el certificado de interfaz de gestión personalizada se utiliza para todas las nuevas conexiones posteriores a la API de Grid Manager, de arrendatario Manager, de Grid Manager o de arrendatario Manager.

Generar certificado

Genere los archivos de certificado de servidor.

> La práctica recomendada para un entorno de producción es usar un certificado de interfaz de gestión personalizado firmado por una entidad de certificación externa.

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o varios nombres de dominio completos que se deben incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.

Campo	Descripción
IP	Una o más direcciones IP que se incluirán en el certificado.
Asunto (opcional)	X,509 Asunto o nombre distinguido (DN) del propietario del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la dirección IP como nombre común del asunto (CN).
Días válidos	Núm. De días después de la creación que caduca el certificado.
Agregue extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de claves y uso de claves ampliado se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. **Nota**: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyen estas extensiones.

c. Seleccione **generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

   - Seleccione **Descargar certificado** para guardar el archivo de certificado.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

e. Seleccione **Guardar**. + el certificado de interfaz de gestión personalizada se utiliza para todas las nuevas conexiones posteriores a la API de Grid Manager, de arrendatario Manager, de Grid Manager o de arrendatario Manager.

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

   Tras cargar o generar un nuevo certificado, permita que se borren las alertas de caducidad de los certificados relacionados.

6. Después de añadir un certificado de interfaz de gestión personalizado, la página de certificado de interfaz de gestión muestra información detallada sobre certificados que están en uso. + puede descargar o copiar el certificado PEM según sea necesario.

Restaure el certificado de interfaz de gestión predeterminado

Puede volver a utilizar el certificado de interfaz de gestión predeterminado para las conexiones de Grid Manager y de arrendatario Manager.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **utilizar certificado predeterminado**.

   Cuando restaura el certificado de interfaz de gestión predeterminado, los archivos de certificado del servidor personalizados que configuró se eliminan y no pueden recuperarse del sistema. El certificado de la interfaz de gestión predeterminado se utiliza para todas las conexiones de clientes nuevas subsiguientes.

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

Use un script para generar un nuevo certificado de interfaz de gestión autofirmado

Si se requiere una validación estricta del nombre de host, puede usar un script para generar el certificado de la interfaz de gestión.

Antes de empezar

- Tienes "permisos de acceso específicos".
- Tiene el `Passwords.txt` archivo.

Acerca de esta tarea

La práctica recomendada para un entorno de producción es usar un certificado firmado por una entidad de certificación externa.

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 el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a raíz: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

      Al iniciar sesión como root, la petición de datos cambia de `$` a `#`.

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 de administración. Por ejemplo, `*.ui.storagegrid.example.com` utiliza el comodín * para representar `admin1.ui.storagegrid.example.com` y `admin2.ui.storagegrid.example.com`.
   - Establezca esta opción `--type management` para configurar el certificado de interfaz de gestión, que

utiliza Grid Manager y Tenant Manager.

- De forma predeterminada, los certificados generados son válidos durante un año (365 días) y deben volver a crearse antes de que expiren. Puede utilizar `--days` el argumento para sustituir el período de validez por defecto.

> El período de validez de un certificado comienza cuando `make-certificate` se ejecuta. Debe asegurarse de que el cliente 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 720
```

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** > **Seguridad** > **Certificados**
   c. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
7. Configure el cliente de administración para que utilice el certificado público que ha copiado. Incluya las etiquetas INICIAL Y FINAL.

Descargue o copie el certificado de la interfaz de gestión

Puede guardar o copiar el contenido del certificado de la interfaz de administración para utilizarlo en otro lugar.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione la ficha **servidor** o **paquete CA** y, a continuación, descargue o copie el certificado.

Descargue el archivo de certificado o el paquete de CA

Descargue el certificado o el archivo del bundle de CA `.pem`. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Descargar certificado** o **Descargar paquete de CA**.

   Si está descargando un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se descargan como un solo archivo.

b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Copie el certificado o el paquete de CA PEM

Copie el texto del certificado que se va a pegar en otro lugar. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM**.

   Si va a copiar un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se copian al mismo tiempo.

b. Pegue el certificado copiado en un editor de texto.

c. Guarde el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Configure los certificados de API S3

Es posible reemplazar o restaurar el certificado de servidor que se utiliza para las conexiones de cliente S3 a los nodos de almacenamiento o para extremos de equilibrador de carga. El certificado de servidor personalizado de reemplazo es específico de su organización.

Se han eliminado los detalles de Swift de esta versión del sitio del documento. Consulte "StorageGRID 11,8: Configure los certificados de API S3 y Swift".

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 también necesite instalar el certificado

de Grid CA en el cliente API S3 que utilizará para acceder al sistema, según la autoridad de certificación (CA) raíz que esté utilizando.

> Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, la alerta **Expiración del certificado de servidor global para la API S3** se activa cuando el certificado del servidor raíz está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **Configuración** > **Seguridad** > **Certificados** y mirando la fecha de vencimiento del certificado de API S3 en la pestaña Global.

Puede cargar o generar un certificado API personalizado de S3.

Agregue un certificado API S3 personalizado

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, seleccione **S3 certificado API**.
3. Seleccione **utilizar certificado personalizado**.
4. Cargue o genere el certificado.

Cargue el certificado

Cargue los archivos de certificado de servidor requeridos.

a. Seleccione **cargar certificado**.
b. Cargue los archivos de certificado de servidor requeridos:
   - **Certificado de servidor**: El archivo de certificado de servidor personalizado (codificado con PEM).
   - **Clave privada del certificado**: 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 opcional que contiene los certificados de cada autoridad de certificación de emisión intermedia. 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.
c. Seleccione los detalles del certificado para mostrar los metadatos y el PEM de cada certificado de API S3 personalizado que se cargó. Si cargó un paquete de CA opcional, cada certificado aparece en su propia pestaña.
   - Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

     Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
d. Seleccione **Guardar**.

   El certificado de servidor personalizado se utiliza para las nuevas conexiones de cliente S3 posteriores.

Generar certificado

Genere los archivos de certificado de servidor.

a. Seleccione **generar certificado**.
b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o varios nombres de dominio completos que se deben incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.

Campo	Descripción
IP	Una o más direcciones IP que se incluirán en el certificado.
Asunto (opcional)	X,509 Asunto o nombre distinguido (DN) del propietario del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la dirección IP como nombre común del asunto (CN).
Días válidos	Núm. De días después de la creación que caduca el certificado.
Agregue extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de claves y uso de claves ampliado se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. **Nota**: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyen estas extensiones.

c. Seleccione **generar**.

d. Seleccione **Detalles del certificado** para mostrar los metadatos y PEM para el certificado API S3 personalizado que se generó.

   - Seleccione **Descargar certificado** para guardar el archivo de certificado.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

     Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

e. Seleccione **Guardar**.

   El certificado de servidor personalizado se utiliza para las nuevas conexiones de cliente S3 posteriores.

5. Seleccione una pestaña para mostrar los metadatos del certificado de servidor StorageGRID predeterminado, un certificado firmado de una CA que se cargó o un certificado personalizado generado.

   Tras cargar o generar un nuevo certificado, permita que se borren las alertas de caducidad de los certificados relacionados.

6. Actualice la página para garantizar que se actualice el explorador web.
7. Después de añadir un certificado de API S3 personalizado, la página de certificado de API S3 muestra

información de certificados detallada para el certificado de API S3 personalizado que está en uso. + puede descargar o copiar el certificado PEM según sea necesario.

Restaure el certificado API S3 predeterminado

Se puede revertir a utilizar el certificado de API S3 predeterminado para conexiones de cliente S3 a los nodos de almacenamiento. Sin embargo, no puede usar el certificado de API S3 predeterminado para un punto final de equilibrio de carga.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, seleccione **S3 certificado API**.
3. Seleccione **utilizar certificado predeterminado**.

   Cuando restaura la versión predeterminada del certificado de API global S3, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. El certificado de API S3 predeterminado se utilizará para las siguientes conexiones de cliente nuevos S3 a nodos de almacenamiento.

4. Seleccione **OK** para confirmar la advertencia y restaurar el certificado API S3 predeterminado.

   Si tiene permiso de acceso raíz y se ha utilizado el certificado de API S3 personalizado para las conexiones de punto final del equilibrador de carga, se muestra una lista de puntos finales del equilibrador de carga a los que ya no se podrá acceder utilizando el certificado de API S3 predeterminado. Vaya a "Configurar puntos finales del equilibrador de carga" para editar o eliminar los puntos finales afectados.

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

Descargue o copie el certificado API S3

Puede guardar o copiar el contenido del certificado API de S3 para utilizarlo en cualquier otro lugar.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, seleccione **S3 certificado API**.
3. Seleccione la ficha **servidor** o **paquete CA** y, a continuación, descargue o copie el certificado.

Descargue el archivo de certificado o el paquete de CA

Descargue el certificado o el archivo del bundle de CA `.pem`. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Descargar certificado** o **Descargar paquete de CA**.

   Si está descargando un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se descargan como un solo archivo.

b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Copie el certificado o el paquete de CA PEM

Copie el texto del certificado que se va a pegar en otro lugar. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM**.

   Si va a copiar un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se copian al mismo tiempo.

b. Pegue el certificado copiado en un editor de texto.

c. Guarde el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Información relacionada

- "USE LA API DE REST DE S3"
- "Configure los nombres de dominio de punto final S3"

Copie el certificado de la CA de cuadrícula

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "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** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Grid CA**.

2. En la sección **Certificado PEM**, descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el archivo de certificado `.pem`.

a. Seleccione **Descargar certificado**.

b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

PEM de certificado de copia

Copie el texto del certificado que se va a pegar en otro lugar.

a. Seleccione **Copiar certificado PEM**.

b. Pegue el certificado copiado en un editor de texto.

c. Guarde el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Configure los certificados StorageGRID para FabricPool

Para los clientes S3 que realizan una validación estricta del nombre de host y no admiten la desactivación de la validación estricta del nombre de host, como los clientes ONTAP que usan FabricPool, puede generar o cargar un certificado de servidor al configurar el punto final del equilibrador de carga.

Antes de empezar

- Tienes "permisos de acceso específicos".
- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".

Acerca de esta tarea

Al crear un extremo de equilibrador de carga, se 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 más información y procedimientos, consulte "Configure StorageGRID para 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 equilibrio de carga HTTPS, se le solicita que cargue el certificado de servidor, la clave privada de certificado y el paquete de CA opcional.

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.

Configurar certificados de cliente

Los certificados de cliente permiten a los clientes externos autorizados acceder a la base de datos Prometheus de StorageGRID, lo que proporciona una forma segura de que las herramientas externas supervisen StorageGRID.

Si necesita acceder a StorageGRID mediante una herramienta de supervisión externa, debe cargar o generar un certificado de cliente mediante el Gestor de cuadrícula y copiar la información de certificado a la herramienta externa.

Consulte "Gestionar certificados de seguridad" y "Configurar certificados de servidor personalizados".

Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, se activa la alerta **Expiración de certificados de cliente configurados en la página Certificados** cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **Configuración** > **Seguridad** > **Certificados** y mirando la fecha de vencimiento del certificado del cliente en la pestaña Cliente.

Si utiliza un servidor de gestión de claves (KMS) para proteger los datos en nodos de dispositivos especialmente configurados, consulte la información específica sobre "Cargando un certificado de cliente KMS".

Antes de empezar

- Tiene permiso de acceso raíz.
- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Para configurar un certificado de cliente:
  - Tiene la dirección IP o el nombre de dominio del nodo de administrador.
  - Si configuró el certificado de interfaz de gestión StorageGRID, tiene la CA, el certificado de cliente y la clave privada utilizadas para configurar el certificado de interfaz de gestión.
  - Para cargar su propio certificado, la clave privada del certificado está disponible en su equipo local.
  - La clave privada debe haberse guardado o registrado en el momento de su creación. Si no tiene la clave privada original, debe crear una nueva.
- Para editar un certificado de cliente:
  - Tiene la dirección IP o el nombre de dominio del nodo de administrador.
  - Para cargar su propio certificado o un nuevo certificado, la clave privada, el certificado de cliente y la CA (si se utiliza) están disponibles en su equipo local.

Añada certificados de cliente

Para agregar el certificado de cliente, use uno de estos procedimientos:

- El certificado de interfaz de gestión ya está configurado
- CERTIFICADO de cliente emitido por CA
- Certificado generado desde Grid Manager

El certificado de interfaz de gestión ya está configurado

Utilice este procedimiento para agregar un certificado de cliente si ya se ha configurado un certificado de interfaz de gestión mediante una CA proporcionada por el cliente, un certificado de cliente y una clave privada.

Pasos

1. En el Administrador de cuadrícula, seleccione **Configuración** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.
5. Seleccione **continuar**.
6. Para el paso **Adjuntar certificados**, cargue el certificado de la interfaz de administración.
   a. Seleccione **cargar certificado**.
   b. Seleccione **Examinar** y seleccione el archivo de certificado de la interfaz de gestión (`.pem`).
      - Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.
      - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
   c. Seleccione **Crear** para guardar el certificado en Grid Manager.

      El nuevo certificado aparece en la ficha Cliente.
7. Configurar una herramienta de supervisión externa, Como Grafana.

CERTIFICADO de cliente emitido por CA

Utilice este procedimiento para agregar un certificado de cliente de administrador si no se ha configurado un certificado de interfaz de gestión y tiene previsto agregar un certificado de cliente para Prometheus que utilice un certificado de cliente emitido por CA y una clave privada.

Pasos

1. Realice los pasos a "configure un certificado de interfaz de gestión".
2. En el Administrador de cuadrícula, seleccione **Configuración** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.
3. Seleccione **Agregar**.
4. Introduzca un nombre de certificado.
5. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione

Permitir prometheus.

6. Seleccione **continuar**.
7. Para el paso **Adjuntar certificados**, cargue el certificado de cliente, la clave privada y los archivos del paquete de CA:
   a. Seleccione **cargar certificado**.
   b. Seleccione **Examinar** y seleccione el certificado de cliente, la clave privada y los archivos del paquete de CA (`.pem`).
      - Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.
      - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
   c. Seleccione **Crear** para guardar el certificado en Grid Manager.

      Los nuevos certificados aparecen en la ficha Cliente.
8. Configurar una herramienta de supervisión externa, Como Grafana.

Certificado generado desde Grid Manager

Utilice este procedimiento para agregar un certificado de cliente de administrador si no se ha configurado un certificado de interfaz de gestión y planea agregar un certificado de cliente para Prometheus que utilice la función generar certificado en Grid Manager.

Pasos

1. En el Administrador de cuadrícula, seleccione **Configuración** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.
5. Seleccione **continuar**.
6. Para el paso **Adjuntar certificados**, selecciona **Generar certificado**.
7. Especifique la información del certificado:
   - **Tema** (opcional): X,509 Sujeto o nombre distinguido (DN) del titular del certificado.
   - **Días válidos**: El número de días que el certificado generado es válido, comenzando en el momento en que se genera.
   - **Agregar extensiones de uso de claves**: Si se selecciona (predeterminado y recomendado), el uso de claves y las extensiones de uso de claves extendidas se agregan al certificado generado.

     Estas extensiones definen el propósito de la clave contenida en el certificado.

     Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.
8. Seleccione **generar**.

9. Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.

   No podrá ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copie o descargue la clave en una ubicación segura.

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
   - Seleccione **Descargar certificado** para guardar el archivo de certificado.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

     Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar clave privada** para copiar la clave privada del certificado para pegarla en otro lugar.
   - Seleccione **Descargar clave privada** para guardar la clave privada como archivo.

     Especifique el nombre del archivo de clave privada y la ubicación de descarga.

10. Seleccione **Crear** para guardar el certificado en Grid Manager.

    El nuevo certificado aparece en la ficha Cliente.

11. En el Administrador de cuadrícula, seleccione **Configuración** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Global**.
12. Seleccione **Certificado de interfaz de administración**.
13. Seleccione **utilizar certificado personalizado**.
14. Cargue los archivos certificate.pem y private_key.pem desde el detalles del certificado de cliente paso. No es necesario cargar un paquete de CA.
    a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
    b. Cargar cada archivo de certificado (`.pem`).
    c. Seleccione **Guardar** para guardar el certificado en Grid Manager.

       El nuevo certificado se muestra en la página del certificado de interfaz de gestión.

15. Configurar una herramienta de supervisión externa, Como Grafana.

Configure una herramienta de monitorización externa

Pasos

1. Configure los siguientes ajustes en su herramienta de supervisión externa, como Grafana.
   a. **Nombre**: Escriba un nombre para la conexión.

      StorageGRID no requiere esta información, pero se debe proporcionar un nombre para probar la conexión.

   b. **URL**: Introduzca el nombre de dominio o la dirección IP del nodo de administración. Especifique HTTPS y el puerto 9091.

Por ejemplo: `https://admin-node.example.com:9091`

c. Activar **Licencia de cliente TLS** y **con CA Cert**.

d. En Detalles de autenticación TLS/SSL, copie y pegue:

- El certificado de CA de la interfaz de administración para **CA Cert**
- El certificado de cliente para **Cliente Cert**
- La clave privada de **clave de cliente**

e. **ServerName**: Introduzca el nombre de dominio del nodo Admin.

Servername debe coincidir con el nombre de dominio tal y como aparece en el certificado de la interfaz de gestión.

2. Guarde y pruebe el certificado y la clave privada que copió desde StorageGRID o un archivo local.

Ahora puede acceder a la métrica Prometheus desde StorageGRID con su herramienta de supervisión externa.

Para obtener información sobre las métricas, consulte la "Instrucciones para supervisar StorageGRID".

Editar certificados de cliente

Puede editar un certificado de cliente de administrador para cambiar su nombre, habilitar o deshabilitar el acceso a Prometheus, o cargar un nuevo certificado cuando el actual haya caducado.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.

Las fechas de caducidad de los certificados y los permisos de acceso a Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya ha caducado, aparecerá un mensaje en la tabla y se activará una alerta.

2. Seleccione el certificado que desea editar.
3. Seleccione **Editar** y, a continuación, seleccione **Editar nombre y permiso**
4. Introduzca un nombre de certificado.
5. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.
6. Seleccione **continuar** para guardar el certificado en Grid Manager.

El certificado actualizado se muestra en la ficha Cliente.

Adjunte un nuevo certificado de cliente

Puede cargar un nuevo certificado cuando el actual haya caducado.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.

Las fechas de caducidad de los certificados y los permisos de acceso a Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya ha caducado, aparecerá un mensaje en la tabla y se activará una alerta.

2. Seleccione el certificado que desea editar.
3. Seleccione **Editar** y, a continuación, seleccione una opción de edición.

Cargue el certificado

Copie el texto del certificado que se va a pegar en otro lugar.

a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.

b. Cargar el nombre del certificado de cliente (`.pem`).

   Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.

   - Seleccione **Descargar certificado** para guardar el archivo de certificado.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

c. Seleccione **Crear** para guardar el certificado en Grid Manager.

   El certificado actualizado se muestra en la ficha Cliente.

Generar certificado

Genere el texto del certificado para pegarlo en otro lugar.

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

   - **Tema** (opcional): X,509 Sujeto o nombre distinguido (DN) del titular del certificado.
   - **Días válidos**: El número de días que el certificado generado es válido, comenzando en el momento en que se genera.
   - **Agregar extensiones de uso de claves**: Si se selecciona (predeterminado y recomendado), el uso de claves y las extensiones de uso de claves extendidas se agregan al certificado generado.

     Estas extensiones definen el propósito de la clave contenida en el certificado.

     Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **generar**.

d. Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.

   No podrá ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copie o descargue la clave en una ubicación segura.

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en

otro lugar.

- Seleccione **Descargar certificado** para guardar el archivo de certificado.

  Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar clave privada** para copiar la clave privada del certificado para pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como archivo.

  Especifique el nombre del archivo de clave privada y la ubicación de descarga.

e. Seleccione **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha Cliente.

Descargar o copiar certificados de cliente

Puede descargar o copiar un certificado de cliente para utilizarlo en otro lugar.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione el certificado que desea copiar o descargar.
3. Descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el archivo de certificado `.pem`.

a. Seleccione **Descargar certificado**.
b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado

Copie el texto del certificado que se va a pegar en otro lugar.

a. Seleccione **Copiar certificado PEM**.
b. Pegue el certificado copiado en un editor de texto.
c. Guarde el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Quite certificados de cliente

Si ya no necesita un certificado de cliente de administrador, puede eliminarlo.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione el certificado que desea eliminar.
3. Seleccione **Eliminar** y, a continuación, confirme.

> Para eliminar hasta 10 certificados, seleccione cada certificado que desee eliminar en la ficha Cliente y, a continuación, seleccione **acciones** > **Eliminar**.

Una vez que se elimine un certificado, los clientes que lo hayan usado deben especificar un nuevo certificado de cliente para acceder a la base de datos Prometheus de StorageGRID.

Configurar los ajustes de seguridad

Gestione la política TLS y SSH

La política de TLS y SSH determina qué protocolos y cifrados se usan para establecer conexiones TLS seguras con aplicaciones de cliente y conexiones SSH seguras a servicios StorageGRID internos.

La directiva de seguridad controla cómo TLS y SSH cifran los datos en movimiento. En general, utilice la directiva de compatibilidad moderna (predeterminada), a menos que su sistema necesite cumplir con Common Criteria o que necesite utilizar otros cifrados.

> Algunos servicios de StorageGRID no se han actualizado para utilizar los cifrados en estas políticas.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".

Seleccione una política de seguridad

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Configuración de seguridad**.

   La pestaña **Políticas TLS y SSH** muestra las políticas disponibles. La política actualmente activa se indica mediante una marca de verificación verde en el mosaico de políticas.

2. Revise las pestañas para conocer las políticas disponibles.

Compatibilidad moderna (predeterminado)

Utilice la política predeterminada si necesita un cifrado fuerte y no tiene requisitos especiales. Esta política es compatible con la mayoría de los clientes TLS y SSH.

Compatibilidad con versiones anteriores

Utilice la política de compatibilidad heredada si necesita opciones de compatibilidad adicionales para clientes más antiguos. Las opciones adicionales en esta política podrían hacerla menos segura que la política de compatibilidad moderna.

Criterios comunes

Utilice la política de Criterios Comunes si necesita la certificación de Criterios Comunes.

Estricta con FIPS

Utilice la política estricta FIPS si necesita la certificación Common Criteria y usar el módulo de seguridad criptográfica de NetApp (NCSM) 3.0.8 o el módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 para conexiones de clientes externos a puntos finales del balanceador de carga, Tenant Manager y Grid Manager. El uso de esta política podría reducir el rendimiento.

El módulo NCSM 3.0.8 y NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 se utilizan en las siguientes operaciones:

- NCSM
  - Conexiones TLS entre los siguientes servicios: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw y cache-svc
  - Conexiones TLS entre clientes y el servicio nginx-gw (puntos finales del balanceador de carga)
  - Conexiones TLS entre clientes y el servicio LDR
  - Cifrado de contenido de objetos para SSE-S3, SSE-C y la configuración de cifrado de objetos almacenados
  - Conexiones SSH

  Para obtener más información, consulte el Programa de validación de algoritmos criptográficos del NIST."Certificado #4838" .

- Módulo API criptográfica del kernel StorageGRID de NetApp

  El módulo NetApp StorageGRID Kernel Crypto API está presente únicamente en plataformas de dispositivos VM y StorageGRID .

  - Colección de entropía
  - Cifrado de nodos

  Para obtener más información, consulte el Programa de validación de algoritmos criptográficos del NIST."Certificados #A6242 a #A6257" y"Certificado de entropía n.° E223" .

Nota: Después de seleccionar esta política,"realizar un reinicio continuo" para que todos los nodos activen el NCSM. Utilice **Mantenimiento** > **Reinicio progresivo** para iniciar y supervisar los reinicios.

Personalizado

Cree una política personalizada si necesita aplicar sus propios cifrados.

De manera opcional, si su StorageGRID tiene requisitos de criptografía FIPS 140, habilite la función de modo FIPS para usar el módulo NCSM 3.0.8 y NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64:

a. Establezca el `fipsMode` parámetro a `true` .
b. Cuando se le solicite,"realizar un reinicio continuo" para que todos los nodos activen los módulos de criptografía. Utilice **Mantenimiento** > **Reinicio progresivo** para iniciar y supervisar los reinicios.
c. Seleccione **Soporte** > **Diagnóstico** para ver las versiones activas del módulo FIPS.

3. Para ver detalles sobre los cifrados, protocolos y algoritmos de cada política, selecciona **Ver detalles**.
4. Para cambiar la política actual, seleccione **Usar política**.

   Aparece una marca de verificación verde junto a **Política actual** en el mosaico de políticas.

Cree una política de seguridad personalizada

Puede crear una política personalizada si necesita aplicar sus propios cifrados.

Pasos

1. Desde el mosaico de la política que es más similar a la política personalizada que desea crear, seleccione **Ver detalles**.
2. Selecciona **Copiar al portapapeles** y luego selecciona **Cancelar**.

3. En el mosaico **Política personalizada**, selecciona **Configurar y usar**.
4. Pegue el JSON que copió y realice los cambios necesarios.
5. Seleccione **Usar política**.

   Aparece una marca de verificación verde junto a **Política actual** en el mosaico Política personalizada.

6. Opcionalmente, seleccione **Editar configuración** para realizar más cambios en la nueva política personalizada.

Vuelva temporalmente a la política de seguridad predeterminada

Si ha configurado una política de seguridad personalizada, es posible que no pueda iniciar sesión en Grid Manager si la política TLS configurada es incompatible con "certificado de servidor configurado".

Puede revertir temporalmente a la política de seguridad predeterminada.

Pasos

1. Inicie sesión en un nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a raíz: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

   Al iniciar sesión como root, la petición de datos cambia de `$` a `#`.

2. Ejecute el siguiente comando:

   ```
   restore-default-cipher-configurations
   ```

3. Desde un explorador web, acceda a Grid Manager en el mismo nodo de administración.
4. Siga los pasos de Seleccione una política de seguridad para volver a configurar la política.

Configure la seguridad de la red y de los objetos

Puede configurar la seguridad de red y de objetos para cifrar objetos almacenados, para evitar determinadas solicitudes S3 o para permitir que las conexiones de cliente a los nodos de almacenamiento utilicen HTTP en lugar de HTTPS.

Cifrado de objetos almacenados

El cifrado de objetos almacenados permite el cifrado de todos los datos de objetos tal como se ingieren a través de S3. De forma predeterminada, los objetos almacenados no se cifran, pero puede optar por cifrar objetos mediante el algoritmo de cifrado AES-128 o AES-256. Cuando se activa la configuración, todos los objetos recién ingeridos se cifran pero no se realiza ningún cambio en los objetos almacenados existentes. Si deshabilita el cifrado, los objetos cifrados actualmente permanecen cifrados, pero los objetos recién procesados no se cifran.

La configuración de cifrado de objetos almacenados se aplica solo a objetos S3 que no han sido cifrados por el cifrado a nivel de cubo o de objeto.

Para obtener más información sobre los métodos de cifrado StorageGRID, consulte "Consulte los métodos de cifrado de StorageGRID".

Impida la modificación del cliente

Impedir la modificación del cliente es una configuración en todo el sistema. Cuando se selecciona la opción **Evitar modificación de cliente**, se rechazan las siguientes solicitudes.

API REST DE S3

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

Active HTTP para las conexiones del nodo de almacenamiento

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para cualquier conexión directa a los nodos de almacenamiento. Puede habilitar HTTP opcionalmente para estas conexiones, por ejemplo, al probar una cuadrícula que no sea de producción.

Utilice HTTP para las conexiones de nodo de almacenamiento solo si los clientes S3 necesitan realizar conexiones HTTP directamente a los nodos de almacenamiento. No es necesario utilizar esta opción para clientes que solo utilizan conexiones HTTPS o para clientes que se conectan al servicio de equilibrio de carga (porque puede "configure cada punto final del equilibrador de carga"usar HTTP o HTTPS).

Consulte "Resumen: Direcciones IP y puertos para conexiones cliente"para saber qué usan los clientes de S3 de los puertos al conectarse a nodos de almacenamiento mediante HTTP o HTTPS.

Seleccione las opciones

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tiene permiso de acceso raíz.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Configuración de seguridad**.
2. Seleccione la pestaña **Red y objetos**.
3. Para el cifrado de objetos almacenados, utilice la configuración **Ninguno** (predeterminada) si no desea que los objetos almacenados se cifren, o seleccione **AES-128** o **AES-256** para cifrar los objetos almacenados.
4. Opcionalmente, seleccione **Evitar modificación de cliente** si desea evitar que los clientes de S3 realicen solicitudes específicas.

   Si cambia este ajuste, el nuevo ajuste tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para el rendimiento y el escalado.

5. Opcionalmente, seleccione **Activar HTTP para conexiones de nodos de almacenamiento** si los clientes se conectan directamente a nodos de almacenamiento y desea utilizar conexiones HTTP.

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

6. Seleccione **Guardar**.

Cambie la configuración de seguridad de la interfaz

La configuración de seguridad de la interfaz le permite controlar si los usuarios están desconectados si están inactivos durante más de la cantidad de tiempo especificada y si se incluye un seguimiento de pila en las respuestas de error de la API.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "Permiso de acceso raíz".

Acerca de esta tarea

La página **Configuración de seguridad** incluye la configuración **Tiempo de espera de inactividad del navegador** y **Seguimiento de pila de API de administración**.

Tiempo de espera de inactividad del explorador

Indica cuánto tiempo puede permanecer inactivo el explorador de un usuario antes de que se cierre la sesión. El valor predeterminado es 15 minutos.

El tiempo de espera de inactividad del navegador también se controla mediante lo siguiente:

- Temporizador StorageGRID independiente no configurable, que se incluye para la seguridad del sistema. El token de autenticación de cada usuario caduca 16 horas después de que el usuario inicia sesión. Cuando caduca la autenticación de un usuario, ese usuario se cierra automáticamente, incluso si el tiempo de espera de inactividad del navegador está desactivado o no se ha alcanzado el valor del tiempo de espera del explorador. Para renovar el token, el usuario debe volver a iniciar sesión.
- Configuración de tiempo de espera para el proveedor de identidad, asumiendo que el inicio de sesión único (SSO) está activado para StorageGRID.

  Si SSO está habilitado y el navegador de un usuario expira, el usuario debe volver a ingresar sus credenciales de SSO para acceder a StorageGRID nuevamente. Ver "Cómo funciona el SSO" .

Seguimiento de la pila de API de gestión

Controla si se devuelve un seguimiento de pila en las respuestas de error de la API de Grid Manager y de Tenant Manager.

Esta opción está desactivada de forma predeterminada, pero es posible que desee activar esta funcionalidad para un entorno de prueba. En general, debe dejar el rastreo de pila desactivado en entornos de producción para evitar revelar detalles internos del software cuando se producen errores de API.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Configuración de seguridad**.
2. Seleccione la pestaña **Interfaz**.
3. Para cambiar la configuración del tiempo de espera de inactividad del navegador:
   a. Expande el acordeón.
   b. Para cambiar el período de tiempo de espera, especifique un valor entre 60 segundos y 7 días. El tiempo de espera predeterminado es de 15 minutos.
   c. Para desactivar esta función, desactive la casilla de verificación.
   d. Seleccione **Guardar**.

      La nueva configuración no afecta a los usuarios que están conectados actualmente. Los usuarios deben iniciar sesión de nuevo o actualizar sus exploradores para que la nueva configuración de tiempo de espera surta efecto.

4. Para cambiar la configuración del seguimiento de pila de API de administración:
   a. Expande el acordeón.

b. Active la casilla de verificación para devolver un seguimiento de pila en las respuestas de error de la API de Grid Manager y de Tenant Manager.

> Deje desactivado el rastreo de pila en entornos de producción para evitar revelar los detalles internos del software cuando se produzcan errores de API.

c. Seleccione **Guardar**.

Administrar el acceso SSH externo

Administre el acceso SSH para el tráfico entrante a la red bloqueando o permitiendo el acceso externo. La gestión del acceso externo SSH no tiene impacto en el tráfico entre nodos de la red.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "Permiso de acceso raíz".

Acerca de esta tarea

Para mejorar la seguridad del sistema, el acceso SSH externo está bloqueado de forma predeterminada. Si necesita realizar tareas que requieren acceso SSH entrante, como resolución de problemas, permita temporalmente el acceso externo. Cuando haya terminado la tarea, bloquee el acceso externo.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Configuración de seguridad**.
2. Seleccione la pestaña **Bloquear SSH**.
3. Utilice la opción **Bloquear acceso SSH entrante** para administrar el acceso SSH externo:
   a. Seleccione la casilla de verificación para bloquear el acceso (predeterminado).
   b. Desmarque la casilla de verificación para permitir el acceso.

> Requiere acceso al puerto 22 entre el portátil de servicio y todos los demás nodos de la red. Elimine el acceso al puerto 22 cuando complete la tarea de mantenimiento.

4. Seleccione **Guardar**.

Configuración de servidores de gestión de claves

¿Qué es un servidor de gestión de claves (KMS)?

Un servidor de gestión de claves (KMS) es un sistema externo de terceros que proporciona claves de cifrado a los nodos de los dispositivos StorageGRID en el sitio de StorageGRID asociado mediante el protocolo de interoperabilidad de gestión de claves (KMIP).

StorageGRID solo admite ciertos servidores de gestión de claves. Para obtener una lista de productos y versiones compatibles, utilice el "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

Puede utilizar uno o varios servidores de gestión de claves para administrar las claves de cifrado de nodos para los nodos de dispositivo StorageGRID que tengan activada la configuración * cifrado de nodos* durante

la instalación. El uso de servidores de gestión de claves con estos nodos de dispositivos le permite proteger los datos aunque se haya eliminado un dispositivo del centro de datos. Una vez que se han cifrado los volúmenes del dispositivo, no podrá acceder a ningún dato del dispositivo a menos que el nodo se pueda comunicar con el KMS.

> StorageGRID no crea ni gestiona las claves externas que se utilizan para cifrar y descifrar los nodos del dispositivo. Si planea usar un servidor de gestión de claves externo para proteger los datos StorageGRID, debe comprender cómo configurar ese servidor y debe comprender cómo gestionar las claves de cifrado. La realización de tareas de gestión de claves supera el alcance de estas instrucciones. Si necesita ayuda, consulte la documentación del servidor de gestión de claves o póngase en contacto con el soporte técnico.

KM y configuración del dispositivo

Antes de poder usar un servidor de gestión de claves (KMS) para proteger los datos de StorageGRID en los nodos de los dispositivos, debe completar dos tareas de configuración: Configurar uno o más servidores KMS y habilitar el cifrado de nodos de los nodos de los dispositivos. Cuando estas dos tareas de configuración se completan, el proceso de gestión de claves se realiza de forma automática.

El diagrama de flujo muestra los pasos de alto nivel para usar un KMS para proteger los datos de StorageGRID en los nodos de los dispositivos.

El diagrama de flujo muestra la configuración de KMS y la configuración de dispositivos que se producen en paralelo; sin embargo, puede configurar los servidores de gestión de claves antes o después de habilitar el cifrado de nodos para los nodos de la aplicación nuevos, en función de sus requisitos.

Configurar el servidor de gestión de claves (KMS)

La configuración de un servidor de gestión de claves incluye los siguientes pasos de alto nivel.

Paso	Consulte
Acceda al software KMS y añada un cliente para StorageGRID a cada clúster KMS o KMS.	"Configure StorageGRID como cliente en KMS"
Obtenga la información necesaria para el cliente StorageGRID en el KMS.	"Configure StorageGRID como cliente en KMS"
Agregue el KMS al Gestor de cuadrícula, asígnelo a un único sitio o a un grupo predeterminado de sitios, cargue los certificados necesarios y guarde la configuración de KMS.	"Añadir un servidor de gestión de claves (KMS)"

Configure el aparato

La configuración de un nodo de dispositivo para el uso de KMS incluye los siguientes pasos de alto nivel.

1. Durante la fase de configuración de hardware de la instalación del dispositivo, utilice el instalador del dispositivo StorageGRID para activar el ajuste **cifrado de nodos** del dispositivo.

No puede habilitar la configuración **Node Encryption** después de agregar un dispositivo a la cuadrícula, y no puede usar la administración de claves externa para dispositivos que no tienen el cifrado de nodos activado.

2. Ejecute el instalador del dispositivo StorageGRID. Durante la instalación, se asigna una clave de cifrado de datos aleatoria (DEK) a cada volumen de la cabina, como se indica a continuación:
   - Los depósitos se utilizan para cifrar los datos en cada volumen. Estas claves se generan mediante el cifrado de disco de Linux Unified Key Setup (LUKS) en el SO del dispositivo y no se pueden cambiar.
   - Cada DEK individual se cifra mediante una clave de cifrado de clave maestra (KEK). El KEK inicial es una clave temporal que cifra los depósitos hasta que el dispositivo pueda conectarse al KMS.
3. Añada el nodo del dispositivo a StorageGRID.

Consulte "Habilite el cifrado del nodo" para obtener más información.

Proceso de cifrado de gestión de claves (se produce automáticamente)

El cifrado de gestión de claves incluye los siguientes pasos de alto nivel que se realizan automáticamente.

1. Al instalar un dispositivo con el cifrado de nodos activado en la cuadrícula, StorageGRID determina si existe una configuración KMS para el sitio que contiene el nodo nuevo.
   - Si ya se ha configurado un KMS para el sitio, el dispositivo recibe la configuración de KMS.
   - Si aún no se ha configurado un KMS para el sitio, el KEK temporal continúa encriptado los datos del dispositivo hasta que configura un KMS para el sitio y el dispositivo recibe la configuración de KMS.
2. El dispositivo usa la configuración KMS para conectarse al KMS y solicitar una clave de cifrado.
3. El KMS envía una clave de cifrado al dispositivo. La nueva clave del KMS sustituye al KEK temporal y ahora se utiliza para cifrar y descifrar los depósitos de los volúmenes del dispositivo.

Los datos que existan antes de que el nodo del dispositivo cifrado se conecte al KMS configurado se cifran con una clave temporal. Sin embargo, los volúmenes de los dispositivos no se deben considerar protegidos de la eliminación del centro de datos hasta que la clave temporal se sustituya por la clave de cifrado KMS.

4. Si el dispositivo está encendido o reiniciado, se vuelve a conectar con el KMS para solicitar la clave. La clave, que se guarda en la memoria volátil, no puede sobrevivir a una pérdida de energía o un reinicio.

Consideraciones y requisitos para usar un servidor de gestión de claves

Antes de configurar un servidor de gestión de claves (KMS) externo, debe comprender las consideraciones y los requisitos.

¿Qué versión de KMIP es compatible?

StorageGRID admite la versión KMIP 1.4.

"Especificación del protocolo de interoperabilidad de gestión de claves versión 1.4"

¿Cuáles son las consideraciones de red?

La configuración del firewall de red debe permitir que cada nodo del dispositivo se comunique a través del puerto que se utiliza para las comunicaciones del protocolo de interoperabilidad de gestión de claves (KMIP).

El puerto KMIP predeterminado es 5696.

Debe asegurarse de que cada nodo de dispositivo que utilice cifrado de nodo tenga acceso de red al clúster KMS o KMS configurado para el sitio.

¿Qué versiones de TLS son compatibles?

Las comunicaciones entre los nodos del dispositivo y el KMS configurado utilizan conexiones TLS seguras. StorageGRID puede admitir el protocolo TLS 1,2 o TLS 1,3 cuando realiza conexiones KMIP a un clúster KMS o KMS, según lo que admite el KMS y que "Política de TLS y SSH"se esté utilizando.

StorageGRID negocia el protocolo y el cifrado (TLS 1.2) o el conjunto de cifrados (TLS 1.3) con el KMS cuando realiza la conexión. Para ver qué versiones de protocolo y cifrados/conjuntos de cifrados están disponibles, revise la `tlsOutbound` sección de la política TLS y SSH activa de la red (**Configuración** > **Seguridad Configuración de seguridad**).

¿Qué dispositivos son compatibles?

Puede usar un servidor de administración de claves (KMS) para administrar las claves de cifrado de cualquier dispositivo StorageGRID de la cuadrícula que tenga activada la configuración **cifrado de nodos**. Este ajuste solo se puede habilitar durante la fase de configuración de hardware de la instalación del dispositivo mediante el instalador de StorageGRID Appliance.

> No se puede habilitar el cifrado de nodo después de añadir un dispositivo al grid, y no se puede usar la gestión de claves externa para dispositivos que no tienen el cifrado de nodo habilitado.

Puede usar el KMS configurado para dispositivos StorageGRID y nodos de dispositivos.

No puede usar el KMS configurado para nodos basados en software (no en dispositivos), incluidos los siguientes:

- Nodos puestos en marcha como máquinas virtuales (VM)
- Nodos implementados en motores de contenedor en hosts Linux

Los nodos puestos en marcha en estas otras plataformas pueden utilizar el cifrado fuera de StorageGRID a nivel de almacén de datos o disco.

¿Cuándo se deben configurar los servidores de gestión de claves?

Para una instalación nueva, normalmente debe configurar uno o más servidores de gestión de claves en Grid Manager antes de crear inquilinos. Este orden garantiza que los nodos estén protegidos antes de que se almacenen datos de objeto en ellos.

Puede configurar los servidores de gestión de claves en Grid Manager antes o después de instalar los nodos de dispositivo.

¿Cuántos servidores de gestión de claves necesito?

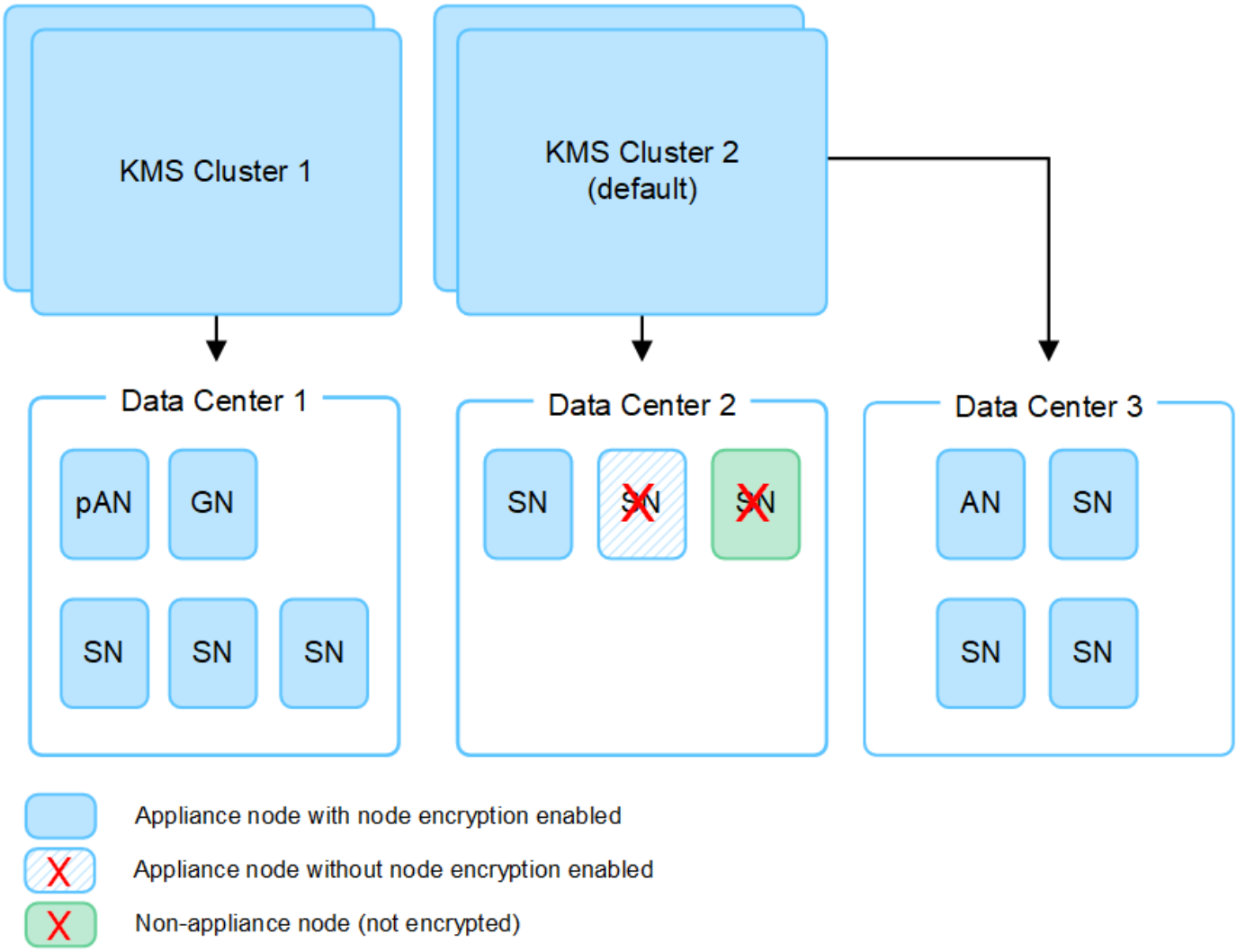
Puede configurar uno o varios servidores de gestión de claves externos para proporcionar claves de cifrado a los nodos de dispositivos en el sistema StorageGRID. Cada KMS proporciona una única clave de cifrado a los nodos de dispositivos StorageGRID en un único sitio o a un grupo de sitios.

StorageGRID admite el uso de clústeres KMS. Cada clúster de KMS contiene varios servidores de gestión de claves replicados que comparten configuraciones de configuración y claves de cifrado. Se recomienda usar

clústeres KMS para la gestión de claves porque mejora las funcionalidades de conmutación por error de una configuración de alta disponibilidad.

Por ejemplo, supongamos que el sistema StorageGRID tiene tres sitios de centro de datos. Podría configurar un clúster KMS para proporcionar una clave a todos los nodos de dispositivos en el centro de datos 1 y un segundo clúster KMS para proporcionar una clave a todos los nodos de dispositivos de los demás sitios. Al agregar el segundo clúster KMS, puede configurar un KMS predeterminado para el Centro de datos 2 y el Centro de datos 3.

Tenga en cuenta que no puede usar un KMS para nodos que no sean del dispositivo ni para ningún nodo del dispositivo que no tenga habilitada la configuración **Node Encryption** durante la instalación.



¿Qué ocurre cuando se gira una clave?

Como práctica recomendada de seguridad, debe utilizar periódicamente "gire la clave de cifrado"cada KMS configurado.

Cuando la nueva versión de clave esté disponible:

- Se distribuye automáticamente a los nodos de dispositivos cifrados del sitio o de los sitios asociados con el KMS. La distribución debe producirse dentro de una hora a partir de la cual se gira la clave.
- Si el nodo de dispositivo cifrado está sin conexión cuando se distribuye la nueva versión de clave, el nodo

recibirá la nueva clave en cuanto se reinicie.

- Si la nueva versión de clave no se puede utilizar para cifrar los volúmenes del dispositivo por cualquier motivo, se activa la alerta **KMS encryption key rotation failed** para el nodo del dispositivo. Es posible que deba ponerse en contacto con el soporte técnico para obtener ayuda para resolver esta alerta.

¿Puedo reutilizar un nodo de dispositivo después de cifrar?

Si necesita instalar un dispositivo cifrado en otro sistema StorageGRID, primero debe retirar el nodo grid para mover los datos del objeto a otro nodo. A continuación, puede utilizar el instalador de dispositivos de StorageGRID para "Borre la configuración de KMS". Al borrar la configuración KMS se deshabilita la configuración **cifrado de nodos** y se elimina la asociación entre el nodo del dispositivo y la configuración KMS del sitio StorageGRID.

> Sin acceso a la clave de cifrado KMS, no se puede acceder a los datos que queden en el dispositivo y queden bloqueados de forma permanente.

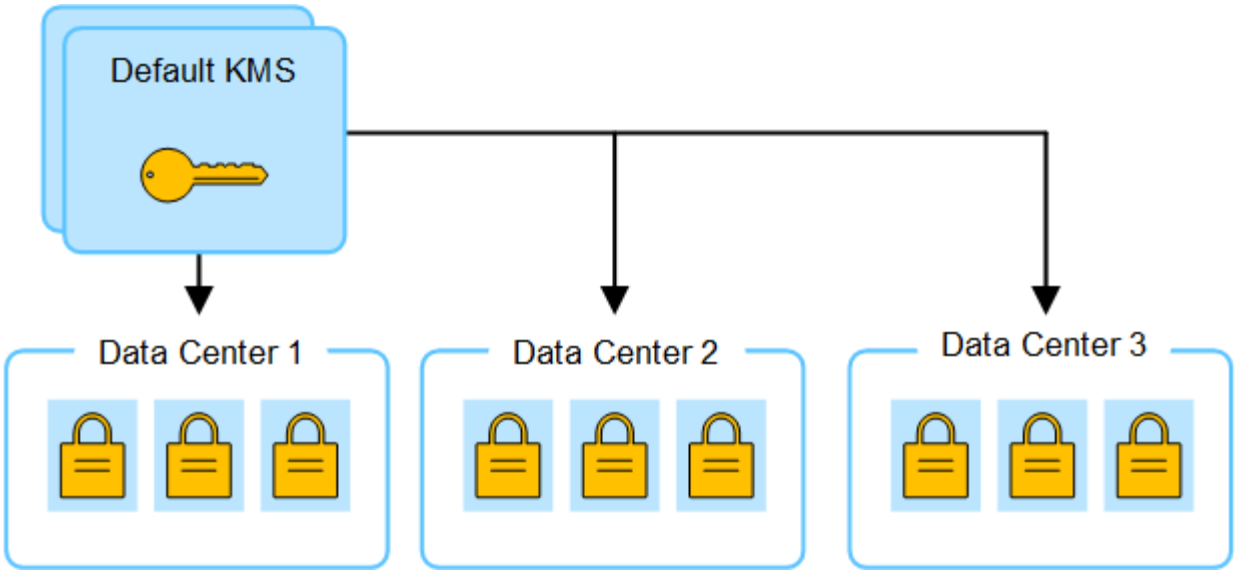
Consideraciones para cambiar el KMS de un sitio

Cada servidor de gestión de claves (KMS) o clúster KMS proporciona una clave de cifrado a todos los nodos de dispositivos en un único sitio o en un grupo de sitios. Si necesita cambiar qué KMS se utiliza para un sitio, es posible que necesite copiar la clave de cifrado de un KMS a otro.

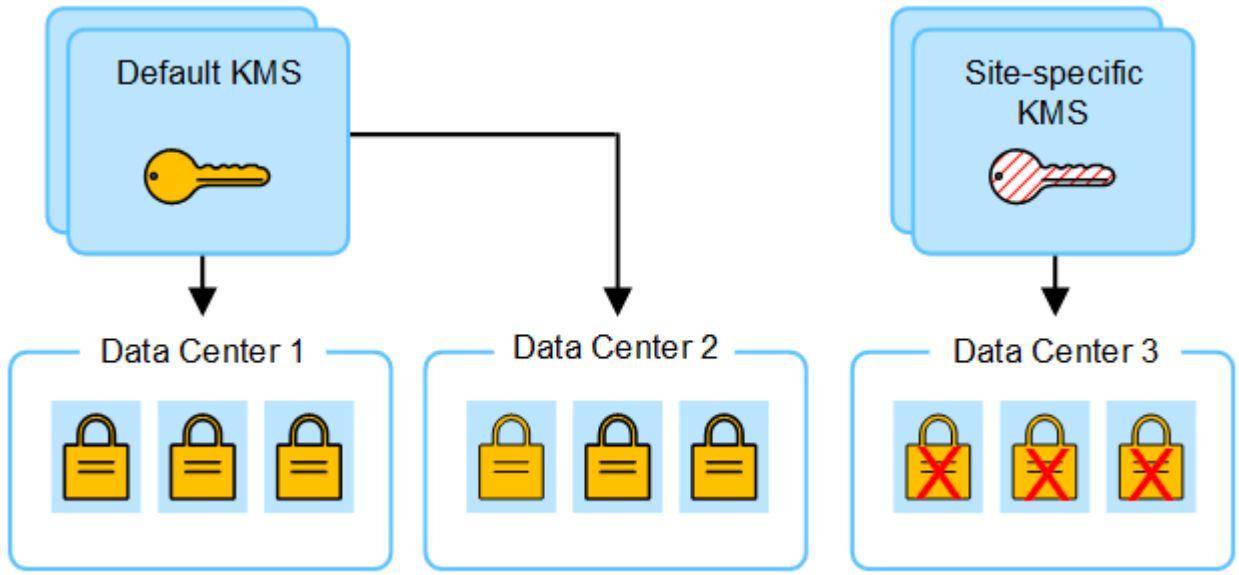
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo cifrados anteriormente en ese sitio se puedan descifrar utilizando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesite copiar la versión actual de la clave de cifrado del KMS original al KMS nuevo. Debe asegurarse de que el KMS tenga la clave correcta para descifrar los nodos del dispositivo cifrados en el sitio.

Por ejemplo:

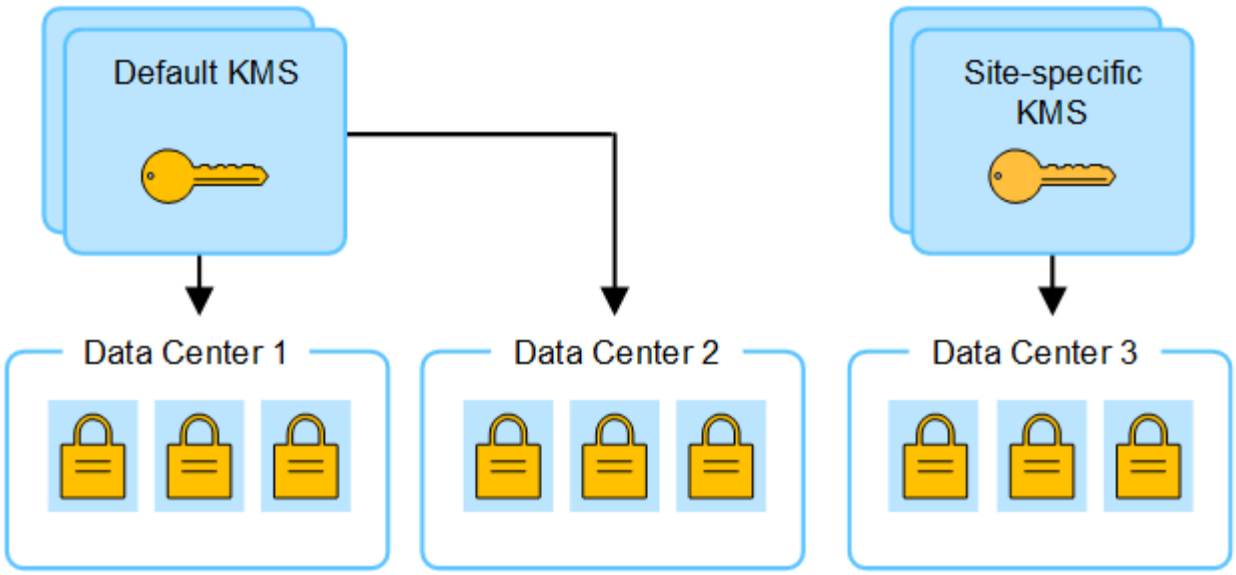
1. Inicialmente configuras un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos de dispositivo que tienen activada la configuración de **cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se usa para cifrar los nodos del dispositivo en todos los sitios. Esta misma clave también debe utilizarse para descifrar esos dispositivos.



3. Decide agregar un KMS específico de un sitio para un sitio (Data Center 3 en la figura). Sin embargo, como los nodos del dispositivo ya están cifrados, se produce un error de validación cuando se intenta guardar la configuración para el KMS específico del sitio. El error se produce porque el KMS específico del sitio no tiene la clave correcta para descifrar los nodos en ese sitio.



4. Para solucionar el problema, copia la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. (Técnicamente, copia la clave original en una nueva clave con el mismo alias. La clave original se convierte en una versión anterior de la nueva clave.) El KMS específico del sitio ahora tiene la clave correcta para descifrar los nodos del dispositivo en el centro de datos 3, por lo que se puede guardar en StorageGRID.



Utilice casos para cambiar qué KMS se utiliza para un sitio

La tabla resume los pasos necesarios para los casos más comunes para cambiar el KMS de un sitio.

Caso de uso para cambiar el KMS de un sitio	Pasos requeridos
Tiene una o más entradas KMS específicas del sitio y desea usar una de ellas como KMS predeterminado.	Edite el KMS específico del sitio. En el campo **administra claves para**, seleccione **Sitios no administrados por otro KMS (KMS predeterminado)**. El KMS específico del sitio se utilizará ahora como KMS predeterminado. Se aplicará a cualquier sitio que no tenga un KMS dedicado. "Editar un servidor de gestión de claves (KMS)"
Tiene un KMS predeterminado y agrega un sitio nuevo en una expansión. No desea utilizar el KMS predeterminado para el nuevo sitio.	1. Si los nodos del dispositivo en el sitio nuevo ya han sido cifrados por el KMS predeterminado, use el software KMS para copiar la versión actual de la clave de cifrado del KMS predeterminado a un KMS nuevo. 2. Con el Gestor de cuadrícula, agregue el nuevo KMS y seleccione el sitio. "Añadir un servidor de gestión de claves (KMS)"
Desea que el KMS para un sitio utilice un servidor diferente.	1. Si los nodos del dispositivo del sitio ya han sido cifrados por el KMS existente, use el software KMS para copiar la versión actual de la clave de cifrado del KMS existente al KMS nuevo. 2. Con el Administrador de cuadrícula, edite la configuración de KMS existente e introduzca el nuevo nombre de host o la dirección IP. "Añadir un servidor de gestión de claves (KMS)"

Configure StorageGRID como cliente en KMS

Debe configurar StorageGRID como cliente para cada servidor de gestión de claves externo o clúster de KMS antes de poder añadir el KMS a StorageGRID.

> Estas instrucciones se aplican a Thales CipherTrust Manager y Hashicorp Vault. Para obtener una lista de productos y versiones compatibles, utilice el "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

Pasos

1. Desde el software KMS, cree un cliente StorageGRID para cada clúster KMS o KMS que vaya a utilizar.

   Cada KMS gestiona una única clave de cifrado para los nodos de dispositivos StorageGRID en un único sitio o en un grupo de sitios.

2. Cree una clave utilizando uno de los dos métodos siguientes:
   - Utilice la página de gestión de claves de su producto KMS. Cree una clave de cifrado AES para cada clúster KMS o KMS.

     La clave de cifrado debe ser de 2.048 bits o más, y debe ser exportable.

   - Haga que StorageGRID cree la clave. Se le pedirá cuando pruebe y guarde después de "cargando certificados de cliente".
3. Registre la siguiente información de cada clúster KMS o KMS.

   Necesitará esta información cuando agregue el KMS a StorageGRID:

   - Nombre de host o dirección IP para cada servidor.
   - Puerto KMIP utilizado por el KMS.
   - Alias de clave para la clave de cifrado del KMS.
4. Para cada clúster de KMS o KMS, obtenga un certificado de servidor firmado por una entidad de certificación (CA) o un paquete de certificado que contiene cada uno de los archivos de certificado de CA codificados con PEM, concatenado en el orden de la cadena de certificados.

   El certificado de servidor permite que el KMS externo se autentique en StorageGRID.

   - El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.
   - El campo Nombre alternativo del asunto (SAN) de cada certificado de servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP a la que se conectará StorageGRID.

     > Al configurar el KMS en StorageGRID, debe introducir las mismas FQDN o direcciones IP en el campo **Nombre de host**.

   - El certificado de servidor debe coincidir con el certificado utilizado por la interfaz KMIP del KMS, que suele utilizar el puerto 5696.
5. Obtenga el certificado de cliente público emitido a StorageGRID por el KMS externo y la clave privada del certificado de cliente.

   El certificado de cliente permite que StorageGRID se autentique en el KMS.

Añadir un servidor de gestión de claves (KMS)

Utilice el asistente del servidor de gestión de claves de StorageGRID para agregar cada clúster KMS o KMS.

Antes de empezar

- Ha revisado el "consideraciones y requisitos para usar un servidor de gestión de claves".
- Tiene "Se ha configurado StorageGRID como cliente en el KMS", y tiene la información necesaria para cada cluster KMS o KMS.
- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".

Acerca de esta tarea

Si es posible, configure cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplica a todos los sitios no administrados por otro KMS. Si crea el KMS predeterminado primero, todos los dispositivos cifrados por nodo de la cuadrícula se cifrarán con el KMS predeterminado. Si desea crear más tarde un KMS específico del sitio, primero debe copiar la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. Consulte "Consideraciones para cambiar el KMS de un sitio" para obtener más información.

Paso 1: Detalles de KM

En el Paso 1 (detalles de KMS) del Asistente para agregar un servidor de gestión de claves, proporciona detalles sobre el clúster de KMS o KMS.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Servidor de administración de claves**.

   Aparece la página del servidor de gestión de claves con la pestaña Detalles de configuración seleccionada.

2. Seleccione **Crear**.

   Paso 1 (detalles de KMS) del asistente Add a Key Management Server.

3. Introduzca la siguiente información para el KMS y el cliente StorageGRID que configuró en ese KMS.

Campo	Descripción
Nombre de KM	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de clave	El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. **Nota**: Si no has creado una clave usando tu producto KMS, se te pedirá que StorageGRID cree la clave.

Campo	Descripción
Administra claves para	El sitio StorageGRID que se asociará a este KMS. Si es posible, debe configurar cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplica a todos los sitios no administrados por otro KMS. • Seleccione un sitio si este KMS gestionará las claves de cifrado de los nodos de los dispositivos en un sitio específico. • Seleccione **Sitios no gestionados por otro KMS (por defecto KMS)** para configurar un KMS predeterminado que se aplicará a cualquier sitio que no tenga un KMS dedicado y a cualquier sitio que agregue en expansiones posteriores. **Nota:** se producirá Un error de validación al guardar la configuración de KMS si selecciona un sitio que anteriormente estaba cifrado por el KMS predeterminado pero no proporciona la versión actual de la clave de cifrado original al nuevo KMS.
Puerto	El puerto que el servidor KMS utiliza para las comunicaciones mediante el protocolo de interoperabilidad de gestión de claves (KMIP). De forma predeterminada es 5696, que es el puerto estándar KMIP.
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. **Nota:** El campo Nombre Alternativo del Asunto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que introduzca aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **continuar**.

Paso 2: Cargar certificado de servidor

En el paso 2 (Cargar certificado de servidor) del asistente Agregar un servidor de gestión de claves, cargue el certificado de servidor (o paquete de certificados) para el KMS. El certificado de servidor permite que el KMS externo se autentique en StorageGRID.

Pasos

1. Desde **Paso 2 (Cargar certificado de servidor)**, busque la ubicación del certificado de servidor guardado o el paquete de certificados.
2. Cargue el archivo de certificado.

   Se muestran los metadatos del certificado del servidor.

   Si cargó un paquete de certificados, los metadatos de cada certificado aparecen en la pestaña correspondiente.

3. Seleccione **continuar**.

Paso 3: Cargar certificados de cliente

En el paso 3 (Cargar certificados de cliente) del asistente para agregar un servidor de gestión de claves, cargue el certificado de cliente y la clave privada de certificado de cliente. El certificado de cliente permite que StorageGRID se autentique en el KMS.

Pasos

1. Desde **Paso 3 (Cargar certificados de cliente)**, busque la ubicación del certificado de cliente.
2. Cargue el archivo de certificado de cliente.

   Aparecen los metadatos del certificado de cliente.

3. Busque la ubicación de la clave privada del certificado de cliente.
4. Cargue el archivo de clave privada.
5. Selecciona **Probar y guardar**.

   Si no existe una clave, se le pedirá que StorageGRID cree una.

   Se prueban las conexiones entre el servidor de gestión de claves y los nodos del dispositivo. Si todas las conexiones son válidas y se encuentra la clave correcta en el KMS, el servidor de gestión de claves nuevo se añade a la tabla de la página del servidor de gestión de claves.

   > Inmediatamente después de añadir un KMS, el estado del certificado en la página servidor de gestión de claves aparece como Desconocido. StorageGRID puede tardar hasta 30 minutos en obtener el estado real de cada certificado. Debe actualizar el navegador web para ver el estado actual.

6. Si aparece un mensaje de error al seleccionar **Probar y guardar**, revise los detalles del mensaje y luego seleccione **Aceptar**.

   Por ejemplo, puede recibir un error 422: Entidad no procesable si se produjo un error en una prueba de conexión.

7. Si necesita guardar la configuración actual sin probar la conexión externa, seleccione **Forzar guardar**.

   > Al seleccionar **Force save** se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos de los dispositivos que tienen habilitado el cifrado de nodos en el sitio afectado. Es posible que pierda acceso a los datos hasta que se resuelvan los problemas.

8. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.

   La configuración de KMS se guarda pero la conexión con el KMS no se prueba.

Administrar un KMS

La gestión de un servidor de gestión de claves (KMS) implica ver y editar detalles,

gestionar certificados, ver nodos cifrados y eliminar un KMS cuando ya no es necesario.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "permiso de acceso necesario".

Ver detalles de KMS

Es posible ver información sobre cada servidor de gestión de claves (KMS) en el sistema StorageGRID, incluidos los detalles de claves y el estado actual de los certificados de servidor y de cliente.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Servidor de administración de claves**.

   Aparecerá la página Servidor de gestión de claves con la siguiente información:

   - En la pestaña Detalles de configuración, se enumeran los servidores de gestión de claves configurados.
   - El separador Nodos Cifrados muestra todos los nodos que tienen el cifrado de nodos activado.

2. Para ver los detalles de un KMS específico y realizar operaciones en ese KMS, seleccione el nombre del KMS. La página de detalles del KMS muestra la siguiente información:

Campo	Descripción
Administra claves para	El sitio StorageGRID asociado con el KMS. Este campo muestra el nombre de un sitio StorageGRID específico o **Sitios no administrados por otro KMS (KMS predeterminado).**
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. Si existe un clúster de dos servidores de gestión de claves, se muestran el nombre de dominio completo o la dirección IP de ambos servidores. Si hay más de dos servidores de gestión de claves en un clúster, el nombre de dominio completo o la dirección IP del primer KMS se enumeran junto con la cantidad de servidores de gestión de claves adicionales en el clúster. Por ejemplo `10.10.10.10 and 10.10.10.11`: O `10.10.10.10 and 2 others`. Para ver todos los nombres de host de un clúster, seleccione un KMS y seleccione **Editar** o **Acciones** > **Editar**.

3. Seleccione una pestaña en la página de detalles de KMS para ver la siguiente información:

Pestaña	Campo	Descripción
Detalles clave	Nombre de clave	El alias clave del cliente StorageGRID en el KMS.

Pestaña	Campo	Descripción
UID de clave	Identificador único de la última versión de la clave.	Última modificación
La fecha y la hora de la última versión de la clave.	Certificado de servidor	Metadatos
Los metadatos del certificado, como el número de serie, la fecha y la hora de caducidad y el certificado PEM.	Certificado PEM	El contenido del archivo PEM (correo de privacidad mejorada) para el certificado.
Certificado de cliente	Metadatos	Los metadatos del certificado, como el número de serie, la fecha y la hora de caducidad y el certificado PEM.

4. Con la frecuencia requerida por las prácticas de seguridad de su organización, seleccione **Rotar clave** o utilice el software KMS para crear una nueva versión de la clave.

   Cuando la rotación de claves es correcta, se actualizan los campos UID Clave y Última Modificación.

> Si gira la clave de cifrado con el software KMS, gírela de la última versión utilizada de la clave a una nueva versión de la misma clave. No gire a una clave completamente diferente.
>
> Nunca intente girar una clave cambiando el nombre de clave (alias) del KMS. StorageGRID requiere que se pueda acceder a todas las versiones de claves usadas anteriormente (así como a las futuras) desde el KMS con el mismo alias de clave. Si cambia el alias de clave para un KMS configurado, es posible que StorageGRID no pueda descifrar los datos.

Gestionar certificados

Resuelva con prontitud cualquier problema de servidor o certificado de cliente. Si es posible, sustituya los certificados antes de que caduquen.

> Debe solucionar cualquier problema con los certificados Lo antes posible. para mantener el acceso a los datos.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Servidor de administración de claves**.
2. En la tabla, observe el valor de Caducidad de certificado para cada KMS.
3. Si se desconoce la caducidad del certificado para cualquier KMS, espere hasta 30 minutos y, a continuación, actualice el explorador web.
4. Si la columna Caducidad del certificado indica que un certificado ha caducado o está a punto de caducar, seleccione el KMS para ir a la página de detalles del KMS.
   a. Seleccione **Certificado de servidor** y verifique el valor del campo “Expires on”.

b. Para reemplazar el certificado, seleccione **Editar certificado** para cargar un nuevo certificado.

c. Repita estos subpasos y seleccione **Certificado de cliente** en lugar de Certificado de servidor.

5. Cuando se activan las alertas **KMS CA CERTIFICATION**, **KMS client certificate expiration** y **KMS server certificate expiration**, anote la descripción de cada alerta y realice las acciones recomendadas.

   StorageGRID puede tardar hasta 30 minutos en obtener actualizaciones para la expiración del certificado. Actualice el explorador web para ver los valores actuales.

> Si obtiene un estado de **El estado del certificado del servidor es desconocido**, asegúrese de que su KMS permite obtener un certificado de servidor sin necesidad de un certificado de cliente.

Vea los nodos cifrados

Puede ver información acerca de los nodos del dispositivo en el sistema StorageGRID que tienen activada la configuración * cifrado de nodos*.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Servidor de administración de claves**.

   Se muestra la página servidor de gestión de claves. En la pestaña Configuration Details, se muestra todos los servidores de gestión de claves que se configuraron.

2. En la parte superior de la página, seleccione la pestaña **Nodos encriptados**.

   La pestaña Nodos cifrados muestra los nodos del dispositivo en su sistema StorageGRID que tienen habilitada la configuración **Encriptación de nodos**.

3. Revise la información de la tabla de cada nodo del dispositivo.

Columna	Descripción
Nombre del nodo	El nombre del nodo del dispositivo.
Tipo de nodo	El tipo de nodo: Almacenamiento, administrador o puerta de enlace.
Sitio	El nombre del sitio StorageGRID donde se instala el nodo.
Nombre de KM	Nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS, seleccione la pestaña Detalles de configuración para agregar un KMS. "Añadir un servidor de gestión de claves (KMS)"
UID de clave	El ID único de la clave de cifrado utilizada para cifrar y descifrar datos en el nodo del dispositivo. Para ver un UID de clave completo, seleccione el texto. Un guión (--) indica que el UID de la clave es desconocido, posiblemente debido a un problema de conexión entre el nodo del dispositivo y el KMS.

Columna	Descripción
Estado	El estado de la conexión entre el KMS y el nodo del dispositivo. Si el nodo está conectado, la Marca de tiempo se actualiza cada 30 minutos. El estado de la conexión puede tardar varios minutos en actualizarse después de que cambie la configuración de KMS. **Nota:** Actualiza tu navegador web para ver los nuevos valores.

4. Si la columna Estado indica un problema de KMS, resuelva el problema inmediatamente.

   Durante las operaciones normales de KMS, el estado será **conectado a KMS**. Si un nodo está desconectado de la cuadrícula, se muestra el estado de conexión del nodo (administrativamente abajo o Desconocido).

   Otros mensajes de estado corresponden a las alertas StorageGRID con los mismos nombres:

   - No se ha podido cargar la configuración DE KMS
   - Error de conectividad DE KMS
   - No se ha encontrado el nombre de la clave de cifrado DE KMS
   - Error en la rotación de la clave de cifrado DE KMS
   - LA clave KMS no pudo descifrar el volumen de un dispositivo
   - KMS no está configurado

   Realice las acciones recomendadas para estas alertas.

> Debe solucionar cualquier problema inmediatamente para garantizar que los datos están totalmente protegidos.

Editar un KMS

Es posible que deba editar la configuración de un servidor de gestión de claves, por ejemplo, si un certificado está a punto de expirar.

Antes de empezar

- Si tiene previsto actualizar el sitio seleccionado para un KMS, ha revisado el "Consideraciones para cambiar el KMS de un sitio".
- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Servidor de administración de claves**.

   Se muestra la página Servidor de gestión de claves donde se muestran todos los servidores de gestión de claves que se configuraron.

2. Selecciona el KMS que deseas editar y selecciona **Acciones** > **Editar**.

   También puede editar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Editar** en la página de detalles del KMS.

3. Opcionalmente, actualice los detalles en **Paso 1 (detalles de KMS)** del asistente Editar un servidor de administración de claves.

Campo	Descripción
Nombre de KM	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de clave	El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Solo es necesario editar el nombre de la clave en casos excepcionales. Por ejemplo, debe editar el nombre de clave si se cambia el nombre del alias en el KMS o si se han copiado todas las versiones de la clave anterior al historial de versiones del nuevo alias.
Administra claves para	Si está editando un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione opcionalmente **Sitios no gestionados por otro KMS (KMS predeterminado)**. Esta selección convierte un KMS específico del sitio al KMS predeterminado, que se aplicará a todos los sitios que no tienen un KMS dedicado y a cualquier sitio agregado en una expansión. **Nota:** Si está editando un KMS específico del sitio, no puede seleccionar otro sitio. Si está editando el KMS predeterminado, no puede seleccionar un sitio específico.
Puerto	El puerto que el servidor KMS utiliza para las comunicaciones mediante el protocolo de interoperabilidad de gestión de claves (KMIP). De forma predeterminada es 5696, que es el puerto estándar KMIP.
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. **Nota:** El campo Nombre Alternativo del Asunto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que introduzca aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **continuar**.

   Paso 2 (Cargar certificado de servidor) del asistente Editar un servidor de gestión de claves.

6. Si necesita sustituir el certificado del servidor, seleccione **examinar** y cargue el nuevo archivo.
7. Seleccione **continuar**.

   El paso 3 (Cargar certificados de cliente) del asistente Editar un servidor de gestión de claves aparece.

8. Si necesita sustituir el certificado de cliente y la clave privada del certificado de cliente, seleccione **examinar** y cargue los nuevos archivos.
9. Selecciona **Probar y guardar**.

Se prueban las conexiones entre el servidor de gestión de claves y todos los nodos de dispositivos cifrados por nodo en los sitios afectados. Si todas las conexiones de nodos son válidas y se encuentra la clave correcta en el KMS, el servidor de gestión de claves se agrega a la tabla de la página servidor de gestión de claves.

10. Si aparece un mensaje de error, revise los detalles del mensaje y seleccione **Aceptar**.

    Por ejemplo, puede recibir un error 422: Entidad no procesable si el sitio seleccionado para este KMS ya está administrado por otro KMS o si se produjo un error en una prueba de conexión.

11. Si necesita guardar la configuración actual antes de resolver los errores de conexión, seleccione **Forzar guardar**.

    > Al seleccionar **Force save** se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos de los dispositivos que tienen habilitado el cifrado de nodos en el sitio afectado. Es posible que pierda acceso a los datos hasta que se resuelvan los problemas.

    Se guarda la configuración de KMS.

12. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.

    La configuración del KMS se guarda, pero la conexión al KMS no se prueba.

Quitar un servidor de gestión de claves (KMS)

En algunos casos, es posible quitar un servidor de gestión de claves. Por ejemplo, puede que desee quitar un KMS específico de un sitio si ha retirado del servicio el sitio.

Antes de empezar

- Ha revisado el "consideraciones y requisitos para usar un servidor de gestión de claves".
- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".

Acerca de esta tarea

Puede eliminar un KMS en los siguientes casos:

- Puede eliminar un KMS específico de un sitio si se ha dado de baja o si el sitio incluye ningún nodo de dispositivo con cifrado de nodo activado.
- Puede eliminar el KMS predeterminado si ya existe un KMS específico del sitio para cada sitio que tiene nodos de dispositivo con cifrado de nodo activado.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Servidor de administración de claves**.

   Se muestra la página Servidor de gestión de claves donde se muestran todos los servidores de gestión de claves que se configuraron.

2. Selecciona el KMS que deseas eliminar y selecciona **Acciones** > **Eliminar**.

También puede eliminar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Eliminar** en la página de detalles del KMS.

3. Confirme que lo siguiente es verdadero:
   - Está eliminando un KMS específico del sitio para un sitio que no tiene ningún nodo de dispositivo con cifrado de nodo activado.
   - Está eliminando el KMS predeterminado, pero ya existe un KMS específico para cada sitio con cifrado de nodo.
4. Seleccione **Sí**.

   La configuración de KMS se elimina.

Administrar la configuración de proxy

Configurar 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.

> La configuración de proxy de almacenamiento configurada no se aplica a los extremos de servicios de plataforma Kafka.

Antes de empezar

- Tienes "permisos de acceso específicos".
- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".

Acerca de esta tarea

Puede configurar los ajustes para un solo proxy de almacenamiento.

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Configuración de proxy**.
2. En la pestaña **Almacenamiento**, selecciona la casilla de verificación **Habilitar proxy de almacenamiento**.
3. Seleccione el protocolo para el proxy de almacenamiento.
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.

   Deje este campo en blanco para utilizar el puerto predeterminado para el protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Seleccione **Guardar**.

   Después de guardar el proxy de almacenamiento, se pueden configurar y probar nuevos puntos finales para los servicios de plataforma o los pools de Cloud Storage.

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.
8. Si necesita deshabilitar un proxy de almacenamiento, desactive la casilla de verificación y seleccione **Guardar**.

Configurar valores de proxy de administración

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

Para obtener más información sobre AutoSupport, consulte "Configure AutoSupport".

Antes de empezar

- Tienes "permisos de acceso específicos".
- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".

Acerca de esta tarea

Puede configurar los ajustes para un solo proxy de administración.

Pasos

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

   Aparecerá la página Configuración de Proxy. De forma predeterminada, se selecciona Almacenamiento en el menú de pestañas.

2. Seleccione la pestaña **Admin**.
3. Seleccione la casilla de verificación **Enable Admin Proxy**.
4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Introduzca el puerto utilizado para conectarse al servidor proxy.
6. Opcionalmente, introduzca un nombre de usuario y una contraseña para el servidor proxy.

   Deje estos campos en blanco si el servidor proxy no requiere un nombre de usuario ni una contraseña.

7. Seleccione una de las siguientes opciones:

   - Si desea proteger la conexión al proxy de administración, seleccione **Verificar certificado de proxy**. Cargue un paquete de CA para verificar la autenticidad de los certificados SSL que presenta el servidor proxy de administrador.

     AutoSupport On Demand, E-Series AutoSupport a través de StorageGRID y Update Path Determination en la página de actualización de StorageGRID no funcionarán si se verifica un certificado proxy.

     Después de cargar el paquete de CA, aparecen sus metadatos.

   - Si no desea validar los certificados al comunicarse con el servidor proxy de administración, seleccione **No verificar el certificado de proxy**.

8. Seleccione **Guardar**.

   Una vez que se guarda 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 deshabilitar el proxy de administración, desactive la casilla de verificación **Habilitar proxy de administración** y, a continuación, seleccione **Guardar**.

Controle los firewalls

Controle el acceso a un firewall externo

Puede abrir o cerrar puertos específicos en el firewall externo.

Puede controlar el acceso a las interfaces de usuario y las API de los nodos de administrador de StorageGRID. Para ello, abra y cierre puertos específicos en el firewall externo. Por ejemplo, es posible que desee evitar que los inquilinos puedan conectarse a Grid Manager en el firewall, además de utilizar otros métodos para controlar el acceso al sistema.

Si desea configurar el firewall interno de StorageGRID, consulte "Configure el firewall interno".

Puerto	Descripción	Si el puerto está abierto…
443	Puerto HTTPS predeterminado para nodos de administración	Los exploradores web y los clientes de la API de gestión pueden acceder a Grid Manager, a la API de gestión de grid, al administrador de inquilinos y a la API de gestión de inquilinos. **Nota:** el puerto 443 también se utiliza para tráfico interno.
8443	Puerto de Grid Manager restringido en nodos de administración	• Los exploradores web y los clientes de la API de gestión pueden acceder a Grid Manager y a la API de gestión de grid mediante HTTPS. • Los exploradores web y los clientes de API de gestión no pueden acceder al administrador de inquilinos ni a la API de gestión de inquilinos. • Se rechazarán las solicitudes de contenido interno.

Puerto	Descripción	Si el puerto está abierto…
9443	Puerto de administrador de inquilinos restringido en los nodos de administrador	• Los exploradores web y los clientes de API de gestión pueden acceder al administrador de inquilinos y a la API de gestión de inquilinos mediante HTTPS. • Los exploradores web y los clientes de API de gestión no pueden acceder a Grid Manager ni a la API de administración de grid. • Se rechazarán las solicitudes de contenido interno.

El inicio de sesión único (SSO) no está disponible en los puertos de administrador de grid restringido o de administrador de inquilinos. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único.

Información relacionada

- "Inicie sesión en Grid Manager"
- "Cree una cuenta de inquilino"
- "Comunicaciones externas"

Gestionar los controles internos del firewall

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad del grid al permitirle controlar el acceso de red al nodo. Utilice el firewall para evitar el acceso a la red en todos los puertos, excepto los necesarios para su implementación de grid específica. Los cambios de configuración que realice en la página de control del firewall se despliegan en cada nodo.

Utilice las tres pestañas de la página de control de Firewall para personalizar el acceso que necesita para su grid.

- **Lista de direcciones privilegiadas**: Utilice esta pestaña para permitir el acceso seleccionado a los puertos cerrados. Puede agregar direcciones IP o subredes en la notación CIDR que pueden acceder a los puertos cerrados mediante la pestaña Administrar acceso externo.
- **Administrar acceso externo**: Utilice esta pestaña para cerrar los puertos que están abiertos por defecto, o reabrir los puertos previamente cerrados.
- **Red de cliente no confiable**: Utilice esta pestaña para especificar si un nodo confía en el tráfico entrante de la red cliente.

  La configuración de esta ficha sustituye a la configuración de la ficha Administrar acceso externo.

  - Un nodo con una red de cliente que no sea de confianza aceptará solo conexiones en los puertos de punto final del equilibrador de carga configurados en ese nodo (puntos finales enlazados de tipo de nodo, interfaz de nodo y global).
  - Los puertos de punto final del equilibrador de carga *son los únicos puertos abiertos* en redes de cliente que no son de confianza, independientemente de la configuración de la pestaña Administrar redes externas.

- Cuando se confía, se puede acceder a todos los puertos abiertos en la pestaña Administrar acceso externo, así como a cualquier punto final del equilibrador de carga abierto en la red cliente.

> La configuración que realice en una pestaña puede afectar a los cambios de acceso que realice en otra pestaña. Asegúrese de comprobar la configuración en todas las pestañas para asegurarse de que su red se comporta de la forma que espera.

Para configurar los controles internos del firewall, consulte "Configurar los controles del firewall".

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulte "Controle el acceso a un firewall externo".

Lista de direcciones con privilegios y pestañas Gestionar acceso externo

El separador Lista de Direcciones con Privilegios permite registrar una o más direcciones IP a las que se les concede acceso a los puertos de grid que están cerrados. La pestaña Administrar acceso externo permite cerrar el acceso externo a los puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son puertos a los que pueden acceder los nodos que no son de cuadrícula de forma predeterminada). Estas dos pestañas a menudo se pueden utilizar juntas para personalizar el acceso exacto a la red que necesita para su grid.

> Las direcciones IP con privilegios no tienen acceso de puerto de grid interno por defecto.

Ejemplo 1: Utilice un host de salto para tareas de mantenimiento

Supongamos que desea utilizar un host de salto (un host reforzado con seguridad) para la administración de la red. Puede utilizar estos pasos generales:

1. Utilice el separador Lista de Direcciones con Privilegios para agregar la dirección IP del host de salto.
2. Utilice la pestaña Gestionar acceso externo para bloquear todos los puertos.

> Agregue la dirección IP con privilegios antes de bloquear los puertos 443 y 8443. Cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios.

Después de guardar la configuración, todos los puertos externos en el nodo de administración de la cuadrícula se bloquearán para todos los hosts excepto el host de salto. A continuación, puede utilizar el host de salto para realizar tareas de mantenimiento en la red de forma más segura.

Ejemplo 2: Bloquear puertos sensibles

Supongamos que desea bloquear puertos sensibles y el servicio en ese puerto. Podrías utilizar los siguientes pasos generales:

1. Utilice el separador Lista de Direcciones con Privilegios para otorgar acceso sólo a los hosts que necesitan acceso al servicio.
2. Utilice la pestaña Gestionar acceso externo para bloquear todos los puertos.

Agregue la dirección IP con privilegios antes de bloquear el acceso a los puertos asignados para acceder a Grid Manager y al gestor de inquilinos (los puertos predefinidos son 443 y 8443). Cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios.

Después de guardar su configuración, el puerto sensible y el servicio en ese puerto estarán disponibles para los hosts en la lista de direcciones privilegiadas. A todos los demás hosts se les niega el acceso al servicio sin importar de qué interfaz provenga la solicitud.

Ejemplo 3: Desactivar el acceso a los servicios no utilizados

A nivel de red, puede desactivar algunos servicios que no desea utilizar. Por ejemplo, para bloquear el tráfico de cliente HTTP S3, debe utilizar el conmutador de la pestaña Gestionar acceso externo para bloquear el puerto 18084.

Pestaña Redes de cliente 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, por defecto, StorageGRID confía en las conexiones entrantes a cada nodo de grid en All "puertos externos disponibles".

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. Consulte "Configurar puntos finales del equilibrador de carga" y "Configurar los controles del firewall".

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. Desde "Puntos finales del equilibrador de carga"la página, configure un extremo de balanceador de carga para S3 over HTTPS en el puerto 443.
2. En la página de control de firewall, seleccione Sin confianza para especificar que la red 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

Suponga que desea habilitar el tráfico de servicios de la plataforma S3 saliente desde un nodo de almacenamiento, pero desea evitar las conexiones entrantes a ese nodo de almacenamiento en la red de clientes. Debe realizar este paso general:

- En la pestaña Redes de cliente sin confianza de la página de control de firewall, indique que la red de cliente en el 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 las solicitudes salientes a los destinos de servicios de plataforma configurados.

Ejemplo 3: Limitar el acceso a Grid Manager a una subred

Supongamos que desea permitir el acceso de Grid Manager solo en una subred específica. Debe realizar los siguientes pasos:

1. Conecte la red cliente de sus nodos de administración a la subred.
2. Utilice la pestaña Red de cliente sin confianza para configurar la red cliente como no confiable.
3. Cuando cree un extremo del balanceador de carga de la interfaz de gestión, introduzca el puerto y seleccione la interfaz de gestión a la que accederá el puerto.
4. Seleccione **Sí** para Red cliente no confiable.
5. Utilice el separador Gestionar acceso externo para bloquear todos los puertos externos (con o sin direcciones IP con privilegios definidas para hosts fuera de esa subred).

Después de guardar la configuración, solo los hosts de la subred especificada pueden acceder a Grid Manager. Todos los demás hosts están bloqueados.

Configure el firewall interno

Puede configurar el firewall de StorageGRID para controlar el acceso a la red a puertos específicos de los nodos de StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Ha revisado la información en "Gestionar los controles del firewall" y "Directrices sobre redes".
- 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.

> Al cambiar la configuración de la red cliente, las conexiones de cliente existentes pueden fallar si no se han configurado los puntos finales del equilibrador de carga.

Acerca de esta tarea

StorageGRID incluye un firewall interno en cada nodo que le permite abrir o cerrar algunos de los puertos en los nodos del grid. Puede utilizar las pestañas de control del firewall para abrir o cerrar los puertos que están abiertos de forma predeterminada en la red de grid, la red de administración y la red de cliente. También puede crear una lista de direcciones IP con privilegios que pueden acceder a los puertos de cuadrícula que están cerrados. Si utiliza una red cliente, puede especificar si un nodo confía en el tráfico entrante de la red cliente y puede configurar el acceso de puertos específicos en la red cliente.

Limitar el número de puertos abiertos a direcciones IP fuera de su red a solo aquellos que son absolutamente necesarios mejora la seguridad de su red. Utilice la configuración en cada una de las tres pestañas de control de Firewall para asegurarse de que solo los puertos necesarios estén abiertos.

Para obtener más información sobre el uso de controles de firewall, incluidos ejemplos, consulte "Gestionar los controles del firewall".

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulte "Controle el acceso a un firewall externo".

Acceda a los controles del cortafuegos

Pasos

1. Seleccione **Configuración** > **Seguridad** > **Control de firewall**.

   Las tres pestañas de esta página se describen en "Gestionar los controles del firewall".

2. Seleccione cualquier pestaña para configurar los controles del firewall.

   Puede utilizar estas pestañas en cualquier orden. Las configuraciones establecidas en una pestaña no limitan lo que puede hacer en las otras pestañas; sin embargo, los cambios de configuración que realice en una pestaña pueden cambiar el comportamiento de los puertos configurados en otras pestañas.

Lista de direcciones con privilegios

Utilice el separador Lista de Direcciones con Privilegios para otorgar a los hosts acceso a los puertos que están cerrados por defecto o cerrados por valores en el separador Gestionar Acceso Externo.

Las direcciones IP y subredes con privilegios no tienen acceso interno a la cuadrícula por defecto. Además, los puntos finales del equilibrador de carga y los puertos adicionales abiertos en la pestaña de lista de direcciones con privilegios son accesibles incluso si están bloqueados en la pestaña Gestionar acceso externo.

> La configuración de la pestaña Lista de direcciones con privilegios no puede sustituir la configuración de la pestaña Red de clientes sin confianza.

Pasos

1. En la pestaña Lista de direcciones con privilegios, introduzca la dirección o subred IP que desea otorgar acceso a los puertos cerrados.
2. Opcionalmente, seleccione **Agregar otra dirección IP o subred en notación CIDR** para agregar clientes con privilegios adicionales.

   > Agregue el menor número posible de direcciones a la lista de privilegios.

3. Opcionalmente, seleccione **Permitir direcciones IP privilegiadas para acceder a los puertos internos de StorageGRID**. Consulte "Puertos internos StorageGRID".

   > Esta opción elimina algunas protecciones para los servicios internos. Déjelo desactivado si es posible.

4. Seleccione **Guardar**.

Gestione el acceso externo

Cuando se cierra un puerto en la pestaña Administrar acceso externo, ninguna dirección IP que no sea de grid puede acceder al puerto a menos que agregue la dirección IP a la lista de direcciones con privilegios. Solo puede cerrar los puertos que están abiertos de forma predeterminada y sólo puede abrir los puertos que haya cerrado.

La configuración de la pestaña Administrar acceso externo no puede sustituir la configuración de la pestaña Red de cliente no confiable. Por ejemplo, si un nodo no es de confianza, el puerto SSH/22 se bloquea en la red cliente incluso si está abierto en la pestaña Gestionar acceso externo. La configuración de la pestaña Red de cliente no confiable anula los puertos cerrados (como 443, 8443, 9443) en la red cliente.

Pasos

1. Selecciona **Administrar acceso externo**. El separador muestra una tabla con todos los puertos externos (puertos a los que pueden acceder los nodos que no son de cuadrícula por defecto) para los nodos de la cuadrícula.
2. Configure los puertos que desea abrir y cerrar mediante las siguientes opciones:
   - Utilice la palanca situada junto a cada puerto para abrir o cerrar el puerto seleccionado.
   - Seleccione **Abrir todos los puertos mostrados** para abrir todos los puertos enumerados en la tabla.
   - Seleccione **Cerrar todos los puertos mostrados** para cerrar todos los puertos enumerados en la tabla.

     Si cierra los puertos 443 o 8443 de Grid Manager, cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios.

   Utilice la barra de desplazamiento situada a la derecha de la tabla para asegurarse de que ha visto todos los puertos disponibles. Utilice el campo de búsqueda para buscar la configuración de cualquier puerto externo introduciendo un número de puerto. Puede introducir un número de puerto parcial. Por ejemplo, si introduce un **2**, se mostrarán todos los puertos que tengan la cadena “2” como parte de su nombre.
3. Seleccione **Guardar**

Red cliente no confiable

Si la red cliente de un nodo no es de confianza, el nodo solo acepta el tráfico entrante en los puertos configurados como puntos finales de equilibrio de carga y, opcionalmente, los puertos adicionales que seleccione en esta pestaña. También puede usar esta pestaña para especificar la configuración predeterminada para los nuevos nodos agregados en una expansión.

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

Los cambios de configuración que realice en la pestaña **Red de clientes sin confianza** anulan la configuración de la pestaña **Administrar acceso externo**.

Pasos

1. Seleccione **Red cliente no confiable**.
2. En la sección Definir Nuevo Nodo por Defecto, especifique cuál debe ser el valor por defecto cuando se agregan nuevos nodos a la cuadrícula en un procedimiento de expansión.
   - **De confianza** (por defecto): Cuando se agrega un nodo en una expansión, su red 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 pestaña para cambiar la configuración de un nuevo nodo específico.

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

3. Utilice las siguientes opciones para seleccionar los nodos que deben permitir conexiones de cliente solo en puntos finales del equilibrador de carga configurados explícitamente o puertos seleccionados adicionales:
   - Seleccione **Untrust on Visualized Nodes** para agregar todos los nodos mostrados en la tabla a la lista Untrusted Client Network.
   - Seleccione **Confiar en los nodos mostrados** para eliminar todos los nodos mostrados en la tabla de la lista Red de clientes sin confianza.
   - Utilice el conmutador situado junto a cada nodo para establecer la red cliente como de confianza o no de confianza para el nodo seleccionado.

     Por ejemplo, puede seleccionar **Untrust on displayed nodes** para agregar todos los nodos a la lista Untrusted Client Network y, a continuación, usar el conmutador junto a un nodo individual para agregar ese nodo a la lista Trusted Client Network.

     Use la barra de desplazamiento en la parte derecha de la tabla para asegurarse de que ha visto todos los nodos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier nodo introduciendo el nombre del nodo. Puede introducir un nombre parcial. Por ejemplo, si introduce un **GW**, se mostrarán todos los nodos que tengan la cadena “GW” como parte de su nombre.

4. Seleccione **Guardar**.

   La nueva configuración del firewall se aplica y aplica inmediatamente. Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Gestione inquilinos

¿Qué son las cuentas de inquilinos?

Una cuenta de inquilino permite usar la API DE REST DE Simple Storage Service (S3) para almacenar y recuperar objetos en un sistema StorageGRID.

Se han eliminado los detalles de Swift de esta versión del sitio del documento. Consulte "StorageGRID 11,8: Gestión de inquilinos".

Como administrador de grid, crea y gestiona las cuentas de tenant que los clientes S3 utilizan para almacenar y recuperar objetos.

Cada cuenta de inquilino tiene grupos locales o federados, usuarios, bloques de S3 y objetos.

Las cuentas de arrendatario se pueden utilizar para segregar objetos almacenados por diferentes entidades. Por ejemplo, pueden utilizarse varias cuentas de inquilino en cualquiera de estos casos de uso:

- **Caso de uso empresarial:** Si administra un sistema StorageGRID en una aplicación empresarial, es posible que desee segregar el almacenamiento de objetos de la red por los diferentes departamentos de

la organización. En este caso, podría crear cuentas de inquilino para el departamento de marketing, el departamento de soporte al cliente, el departamento de recursos humanos, etc.

> Si utiliza el protocolo de cliente S3, puede usar depósitos S3 y políticas de depósitos para segregar objetos entre los departamentos de una empresa. No es necesario utilizar cuentas de inquilino. Consulte las instrucciones para la implementación"Bloques de S3 y políticas de bloques" Para más información.

- **Caso de uso del proveedor de servicios:** Si administra un sistema StorageGRID como proveedor de servicios, puede segregar el almacenamiento de objetos de la red por las diferentes entidades que alquile el almacenamiento en la red. En este caso, creará cuentas de inquilino para la empresa A, la empresa B, la empresa C, etc.

Para obtener más información, consulte "Usar una cuenta de inquilino".

¿Cómo se crea una cuenta de inquilino?

Utilice Grid Manager para crear una cuenta de inquilino. Al crear una cuenta de inquilino, especifique la siguiente información:

- Información básica, como el nombre del inquilino, el tipo de cliente (S3) y la cuota de almacenamiento opcional.
- Permisos para la cuenta de inquilino, como si la cuenta de inquilino puede usar los servicios de la plataforma S3, configurar su propio origen de identidad, usar S3 Select o usar una conexión de federación de grid.
- Acceso raíz inicial para el inquilino, basado en si el sistema StorageGRID utiliza usuarios y grupos locales, federación de identidades o inicio de sesión único (SSO).

Además, puede habilitar la configuración Bloqueo de objetos S3 para el sistema StorageGRID si las cuentas de arrendatario S3 necesitan cumplir con los requisitos normativos. Cuando se habilita el bloqueo de objetos S3, todas las cuentas de inquilinos S3 pueden crear y gestionar bloques conforme a la normativa.

¿Para qué se utiliza el gestor de inquilinos?

Después de crear la cuenta de inquilino, los usuarios de inquilino pueden iniciar sesión en el Administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidad se comparta con la cuadrícula)
- Gestionar grupos y usuarios
- Utilice la federación de grid para la clonación de cuentas y la replicación entre grid
- Gestión de claves de acceso de S3
- Cree y gestione bloques de S3
- Utilice los servicios de la plataforma S3
- Utilice S3 Select
- Supervise el uso del almacenamiento

Mientras que los usuarios inquilinos de S3 pueden crear y gestionar la clave de acceso y los depósitos S3 con el administrador de inquilinos, deben usar una aplicación cliente S3 para ingerir y gestionar objetos. Consulte "USE LA API DE REST DE S3" para obtener más información.

Cree una cuenta de inquilino

Debe crear al menos una cuenta de inquilino para controlar el acceso al almacenamiento en su sistema de StorageGRID.

Los pasos para crear una cuenta de inquilino varían según si"federación de identidades" y"inicio de sesión único" están configurados y si la cuenta de Grid Manager que utiliza para crear la cuenta de inquilino pertenece a un grupo de administradores con permiso de acceso raíz.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Acceso raíz o cuentas de inquilino".
- Si la cuenta de arrendatario utilizará el origen de identidad configurado para el Administrador de grid y desea otorgar permiso de acceso raíz para la cuenta de arrendatario a un grupo federado, ha importado ese grupo federado en el Gestor de grid. No es necesario asignar ningún permiso de Grid Manager a este grupo de administración. Consulte "Gestione los grupos de administradores".
- Si desea permitir que un inquilino de S3 clone los datos de su cuenta y replique objetos de bucket en otro grid mediante una conexión de federación de grid:
  - Tienes "se ha configurado la conexión de federación de grid".
  - El estado de la conexión es **Conectado**.
  - Tiene permiso de acceso raíz.
  - Ha revisado las consideraciones para "gestionar los inquilinos permitidos para la federación de grid".
  - Si la cuenta de arrendatario utilizará el origen de identidad configurado para Grid Manager, ha importado el mismo grupo federado en Grid Manager en ambas cuadrículas.

    Al crear el inquilino, seleccionará este grupo para que tenga el permiso inicial de acceso raíz para las cuentas de inquilino de origen y de destino.

Si este grupo de administración no existe en ambas cuadrículas antes de crear el arrendatario, el arrendatario no se replica en el destino.

Acceda al asistente

Pasos

1. Seleccione **Inquilinos**.
2. Seleccione **Crear**.

Introduzca los detalles

Pasos

1. Introduzca los detalles del arrendatario.

Campo	Descripción
Nombre	Un nombre para la cuenta de inquilino. Los nombres de inquilinos no necesitan ser únicos. Cuando se crea la cuenta de inquilino, recibe un ID de cuenta único de 20 dígitos.
Descripción (opcional)	Descripción para ayudar a identificar al inquilino. Si va a crear un inquilino que utilizará una conexión de federación de grid, opcionalmente, utilice este campo para ayudar a identificar cuál es el inquilino de origen y cuál es el inquilino de destino. Por ejemplo, esta descripción para un inquilino creado en Grid 1 también aparecerá para el inquilino replicado en Grid 2: «Este inquilino se creó en Grid 1».
Tipo de cliente	Debe ser **S3**.
Cuota de almacenamiento (opcional)	Si desea que este inquilino tenga una cuota de almacenamiento, un valor numérico para la cuota y las unidades.

2. Seleccione **continuar**.

Seleccione permisos

Pasos

1. Opcionalmente, seleccione los permisos básicos que desea que tenga este arrendatario.

> Algunos de estos permisos tienen requisitos adicionales. Para obtener más información, seleccione el icono de ayuda de cada permiso.

Permiso	Si se ha seleccionado…
Permitir los servicios de plataforma	El inquilino puede usar servicios de plataforma S3 como CloudMirror. Consulte "Gestione servicios de plataformas para cuentas de inquilinos de S3".
Usar origen de identidad propio	El inquilino puede configurar y administrar su propia fuente de identidad para grupos y usuarios federados. Esta opción está deshabilitada si tiene"SSO configurado" para su sistema StorageGRID .
Permitir selección S3	El inquilino puede emitir solicitudes de API S3 SelectObjectContent para filtrar y recuperar datos de objetos. Consulte "Gestione S3 Select para cuentas de inquilinos". **Importante**: Las solicitudes de SelectObjectContent pueden disminuir el rendimiento del equilibrador de carga para todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

2. Opcionalmente, seleccione los permisos avanzados que desea que tenga este arrendatario.

Permiso	Si se ha seleccionado…
Conexión de federación de grid	El inquilino puede usar una conexión de federación de grid, que: • Hace que este arrendatario y todos los grupos de arrendatarios y usuarios agregados a la cuenta se clonen desde esta cuadrícula (la cuadrícula *source*) a la otra cuadrícula de la conexión seleccionada (la cuadrícula *destination*). • Permite a este inquilino configurar la replicación entre grid entre bloques correspondientes en cada grid. Consulte "Gestione los inquilinos permitidos para la federación de grid".
Bloqueo de objetos de S3	Permitir que el inquilino utilice características específicas de S3 Object Lock: • **Establecer el período máximo de retención** define cuánto tiempo se deben retener los nuevos objetos agregados a este cubo, a partir del momento en que se ingieren. • **Permitir el modo de cumplimiento** evita que los usuarios sobrescriban o eliminen versiones de objetos protegidos durante el período de retención.

3. Seleccione **continuar**.

Defina el acceso raíz y cree un inquilino

Pasos

1. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza la federación de identidades, el inicio de sesión único (SSO) o ambos.

Opción	Haga esto
Si la federación de identidades no está activada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidades está activada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si se activan tanto la federación de identidades como el inicio de sesión único (SSO)	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

2. Seleccione **Crear arrendatario**.

   Aparece un mensaje Correcto y el nuevo arrendatario aparece en la página Inquilinos. Para obtener información sobre cómo ver los detalles del inquilino y supervisar la actividad del inquilino, consulte "Supervise la actividad de los inquilinos".

La aplicación de la configuración de inquilino a través del grid puede tardar 15 minutos o más en función de la conectividad de red, el estado del nodo y las operaciones de Cassandra.

3. Si seleccionó el permiso **Usar conexión de federación de grid** para el inquilino:
   a. Confirme que se ha replicado un inquilino idéntico en la otra cuadrícula de la conexión. Los inquilinos de ambas cuadrículas tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos.

      Si ve el mensaje de error “Inquilino creado sin un clon”, consulte las instrucciones en "Solucionar errores de federación de grid".

   b. Si proporcionó una contraseña de usuario raíz local al definir el acceso raíz, "cambie la contraseña del usuario raíz local" para el inquilino replicado.

      Un usuario raíz local no puede iniciar sesión en el gestor de inquilinos en la cuadrícula de destino hasta que se cambie la contraseña.

Iniciar sesión en el inquilino (opcional)

Según sea necesario, puede iniciar sesión en el nuevo inquilino ahora para completar la configuración, o puede iniciar sesión en el inquilino más adelante. Los pasos de inicio de sesión dependen de si ha iniciado sesión en Grid Manager mediante el puerto predeterminado (443) o un puerto restringido. Consulte "Controle el acceso a un firewall externo".

Inicie sesión ahora

Si está usando…	Realice lo siguiente…
Puerto 443 y se establece una contraseña para el usuario raíz local	1. Seleccione **Iniciar sesión como root**. Al iniciar sesión, aparecen enlaces para configurar buckets, federación de identidades, grupos y usuarios. 2. Seleccione los vínculos para configurar la cuenta de arrendatario. Cada enlace abre la página correspondiente en el Administrador de arrendatarios. Para completar la página, consulte la "instrucciones para el uso de cuentas de inquilino".
Puerto 443 y no ha establecido una contraseña para el usuario raíz local	Seleccione **Iniciar sesión** e introduzca las credenciales de un usuario en el grupo federado de acceso raíz.

Si está usando…	Realice lo siguiente…
Un puerto restringido	1. Selecciona **Finalizar** 2. Seleccione **Restringido** en la tabla de arrendatarios para obtener más información sobre el acceso a esta cuenta de arrendatario. La dirección URL del administrador de inquilinos tiene el siguiente formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* Es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ *port* es el puerto de sólo inquilino ◦ *20-digit-account-id* Es el ID de cuenta único del inquilino

Inicie sesión más tarde

Si está usando…	Realice una de estas…
Puerto 443	• Desde el Administrador de red, seleccione **Inquilinos** y seleccione * Sign in* a la derecha del nombre del inquilino. • Introduzca la URL del inquilino en un navegador web: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* Es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ *20-digit-account-id* Es el ID de cuenta único del inquilino
Un puerto restringido	• Desde el Administrador de red, seleccione **Inquilinos** y seleccione **Restringido**. • Introduzca la URL del inquilino en un navegador web: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* Es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ *port* es el puerto restringido solo para el inquilino ◦ *20-digit-account-id* Es el ID de cuenta único del inquilino

Configure el inquilino

Siga las instrucciones descritas en "Usar una cuenta de inquilino" para gestionar usuarios y grupos de inquilinos, claves de acceso de S3, buckets, servicios de plataforma y replicación entre grid y clonación de

cuentas.

Edite la cuenta de inquilino

Una cuenta de inquilino se puede editar para cambiar el nombre para mostrar, la cuota de almacenamiento o los permisos de inquilino.

Si un inquilino tiene el permiso **Usar conexión de federación de grid**, puede editar los detalles del inquilino desde cualquier cuadrícula en la conexión. Sin embargo, los cambios que realice en una cuadrícula de la conexión no se copiarán en la otra cuadrícula. Si desea mantener los detalles del arrendatario exactamente sincronizados entre las cuadrículas, realice las mismas modificaciones en ambas cuadrículas. Consulte "Gestione los inquilinos permitidos para la conexión de federación de grid".

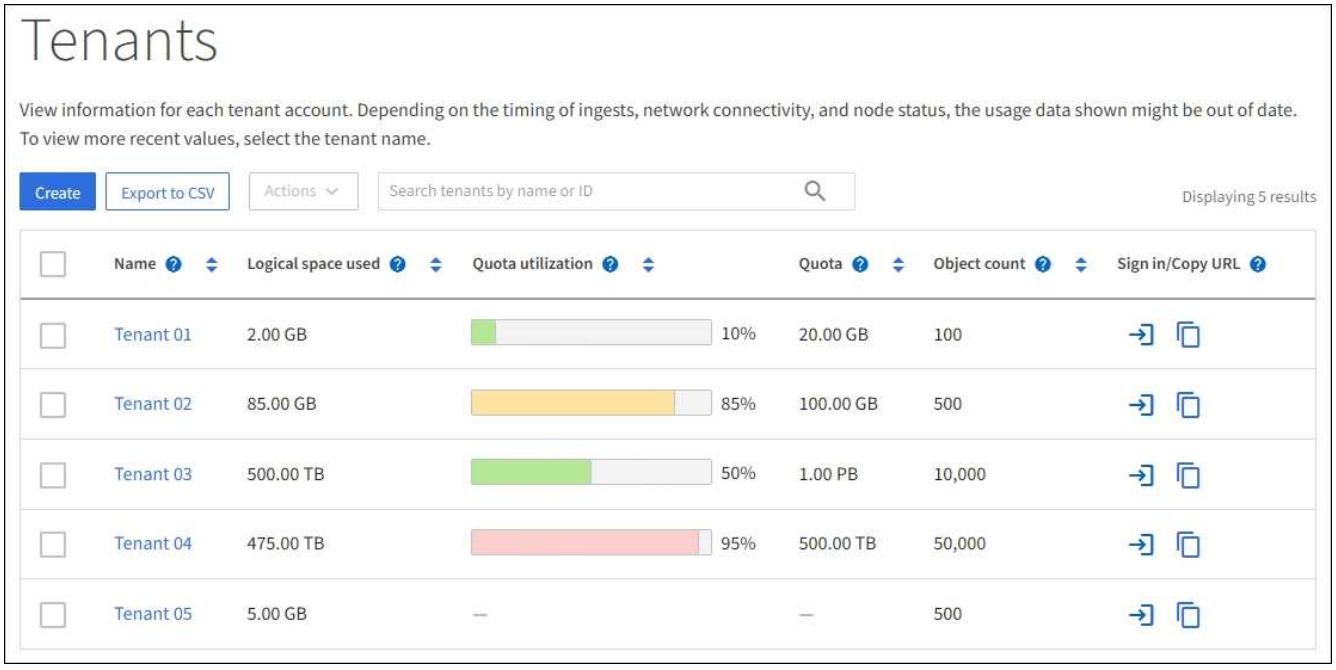
Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Acceso raíz o cuentas de inquilino".

La aplicación de la configuración de inquilino a través del grid puede tardar 15 minutos o más en función de la conectividad de red, el estado del nodo y las operaciones de Cassandra.

Pasos

1. Seleccione **Inquilinos**.



2. Localice la cuenta de inquilino que desea editar.

   Utilice el cuadro de búsqueda para buscar un inquilino por nombre o ID de inquilino.

3. Seleccione el inquilino. Puede realizar una de las siguientes acciones:
   - Selecciona la casilla de verificación para el inquilino y selecciona **Acciones** > **Editar**.
   - Seleccione el nombre del inquilino para mostrar la página de detalles y seleccione **Editar**.

4. Si lo desea, cambie los valores de estos campos:
   - **Nombre**
   - **Descripción**
   - **Cuota de almacenamiento**
5. Seleccione **continuar**.
6. Seleccione o borre los permisos para la cuenta de inquilino.
   - Si deshabilita **Servicios de plataforma** para un arrendatario que ya los está utilizando, los servicios que han configurado para sus cubos S3 dejarán de funcionar. No se envía ningún mensaje de error al inquilino. Por ejemplo, si el inquilino ha configurado la replicación de CloudMirror para un bloque de S3, podrán seguir almacenando objetos en el bloque, pero las copias de esos objetos ya no se realizarán en el bloque S3 externo que se hayan configurado como extremo. Consulte "Gestione servicios de plataformas para cuentas de inquilinos de S3".
   - Cambie la configuración de **Use own identity source** para determinar si la cuenta de inquilino utilizará su propia fuente de identidad o la fuente de identidad que se configuró para Grid Manager.

     Si **Usar la propia fuente de identidad** es:

     - Desactivado y seleccionado, el arrendatario ya ha activado su propio origen de identidad. Un arrendatario debe desactivar su origen de identidad antes de poder utilizar el origen de identidad configurado para el Gestor de cuadrícula.
     - Desactivado y no seleccionado, SSO está activado para el sistema StorageGRID. El inquilino debe utilizar el origen de identidad configurado para el administrador de grid.
   - Seleccione o desactive el permiso **Permitir S3 Select** según sea necesario. Consulte "Gestione S3 Select para cuentas de inquilinos".
   - Para eliminar el permiso **Use grid federation connection**:
     i. Seleccione la pestaña **Grid federation**.
     ii. Selecciona **Eliminar permiso**.
   - Para agregar el permiso **Use grid federation connection**:
     i. Seleccione la pestaña **Grid federation**.
     ii. Seleccione la casilla de verificación **Usar conexión de federación de cuadrícula**.
     iii. Opcionalmente, seleccione **Clonar usuarios y grupos locales existentes** para clonarlos a la cuadrícula remota. Si desea, puede detener la clonado en curso o volver a intentar la clonado si no se pudieron clonar algunos usuarios o grupos locales después de completar la última operación de clonado.
   - Para establecer un período de retención máximo o permitir el modo de cumplimiento:

     > S3 El bloqueo de objetos debe estar activado en la cuadrícula antes de poder utilizar estos ajustes.

     i. Seleccione la pestaña **S3 Object Lock**.
     ii. Para **Establecer período de retención máximo**, ingrese un valor y seleccione el período de tiempo en el menú desplegable.
     iii. Para **Permitir el modo de cumplimiento**, selecciona la casilla de verificación.

Cambiar la contraseña del usuario raíz local del inquilino

Puede que necesite cambiar la contraseña del usuario raíz local de un inquilino si el usuario raíz está bloqueado en la cuenta.

Antes de empezar

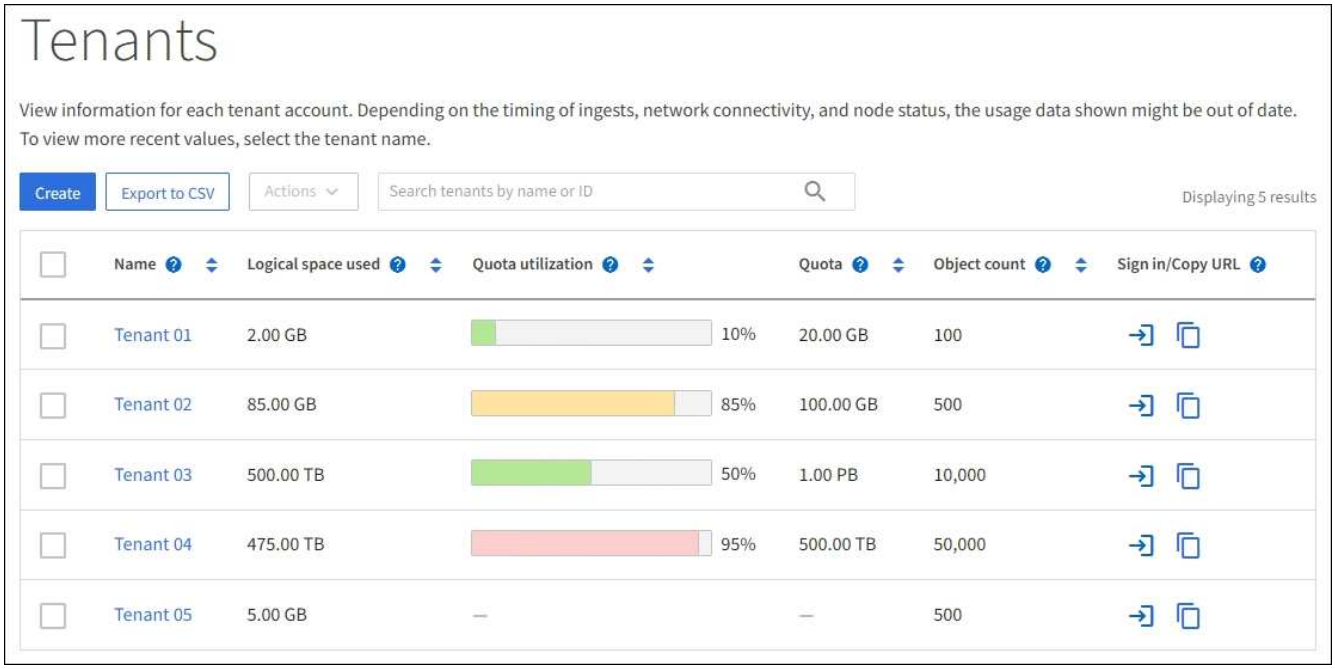
- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "permisos de acceso específicos".

Acerca de esta tarea

Si está habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, el usuario raíz local no puede iniciar sesión en la cuenta de inquilino. Para realizar tareas de usuario raíz, los usuarios deben pertenecer a un grupo federado que tenga el permiso acceso raíz para el arrendatario.

Pasos

1. Seleccione **Inquilinos**.



2. Seleccione la cuenta de inquilino. Puede realizar una de las siguientes acciones:
   - Selecciona la casilla de verificación para el inquilino y selecciona **Acciones** > **Cambiar contraseña raíz**.
   - Seleccione el nombre del inquilino para mostrar la página de detalles y seleccione **Acciones** > **Cambiar contraseña raíz**.
3. Introduzca la nueva contraseña de la cuenta de inquilino.
4. Seleccione **Guardar**.

Eliminar cuenta de inquilino

Puede eliminar una cuenta de inquilino si desea eliminar de forma permanente el acceso del inquilino al sistema.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Ha eliminado los S3 buckets y los objetos asociados con la cuenta de inquilino.
- Si el inquilino puede utilizar una conexión de federación de grid, ha revisado las consideraciones para "Eliminación de un inquilino con el permiso de conexión Usar federación de grid".

Pasos

1. Seleccione **Inquilinos**.
2. Localice la cuenta de inquilino o las cuentas que desea eliminar.

   Utilice el cuadro de búsqueda para buscar un inquilino por nombre o ID de inquilino.

3. Para eliminar varios inquilinos, selecciona las casillas de verificación y selecciona **Acciones** > **Eliminar**.
4. Para suprimir un solo inquilino, realice una de las siguientes acciones:
   - Selecciona la casilla de verificación y selecciona **Acciones** > **Eliminar**.
   - Seleccione el nombre del inquilino para mostrar la página de detalles y, a continuación, seleccione * Acciones * > * Eliminar *.
5. Seleccione **Sí**.

Gestione los servicios de la plataforma

¿Qué son los servicios de plataforma?

Los servicios de plataforma incluyen la replicación de CloudMirror, las notificaciones de eventos y el servicio de integración de búsqueda.

Si habilita los servicios de plataforma para cuentas de inquilino de S3, debe configurar su grid para que los inquilinos puedan acceder a los recursos externos necesarios para usar estos servicios.

Los servicios de plataforma no son compatibles con"cubos de ramas" .

Replicación de CloudMirror

El servicio de replicación de CloudMirror de StorageGRID se usa para reflejar objetos concretos desde un bloque de StorageGRID en un destino externo especificado.

Por ejemplo, podría usar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y, a continuación, aprovechar los servicios de AWS para realizar análisis de los datos.

La replicación de CloudMirror tiene algunas similitudes y diferencias importantes con la función de replicación entre redes. Para obtener más información, consulte "Compare la replicación entre grid y la replicación de CloudMirror".

> La replicación de CloudMirror no es compatible si el depósito de origen tiene habilitado el bloqueo de objetos S3.

Notificaciones

Las notificaciones de eventos por bucket se utilizan para enviar notificaciones sobre acciones específicas realizadas en objetos a un clúster de Kafka externo especificado, un punto final de webhook o un Amazon Simple Notification Service.

Por ejemplo, podría configurar que se envíen alertas a administradores acerca de cada objeto agregado a un bloque, donde los objetos representan los archivos de registro asociados a un evento crítico del sistema.

> Aunque la notificación de eventos se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluido el estado retener hasta fecha y retención legal) de los objetos no se incluirán en los mensajes de notificación.

Servicio de integración de búsqueda

El servicio de integración de búsqueda se utiliza para enviar metadatos de objetos S3 a un índice de Elasticsearch especificado en el que se pueden buscar o analizar los metadatos mediante el servicio externo.

Por ejemplo, podría configurar sus bloques para que envíen metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, podría usar Elasticsearch para realizar búsquedas en los bloques y ejecutar análisis sofisticados de los patrones presentes en los metadatos de objetos.

> Aunque la integración de Elasticsearch se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos de S3 (incluidos los Estados Retain Until Date and Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

Los servicios de plataforma ofrecen a los inquilinos la capacidad de usar recursos de almacenamiento externo, servicios de notificación y servicios de búsqueda o análisis con sus datos. Puesto que la ubicación objetivo para los servicios de plataforma suele ser externa a la implementación de StorageGRID, debe decidir si desea permitir a los inquilinos utilizar estos servicios. Si lo hace, debe habilitar el uso de servicios de plataforma al crear o editar cuentas de inquilino. También debe configurar la red de modo que los mensajes de servicios de plataforma que generan los inquilinos puedan llegar a sus destinos.

Recomendaciones para el uso de servicios de plataformas

Antes de utilizar los servicios de plataforma, tenga en cuenta las siguientes recomendaciones:

- Si un bloque de S3 del sistema StorageGRID tiene habilitadas las versiones y la replicación de CloudMirror, también debe habilitar el control de versiones de bloques de S3 para el extremo de destino. Esto permite que la replicación de CloudMirror genere versiones de objetos similares en el extremo.
- No debe usar más de 100 inquilinos activos con solicitudes S3 que requieran la replicación, las notificaciones y la integración de búsqueda de CloudMirror. Tener más de 100 inquilinos activos puede dar como resultado un rendimiento del cliente S3 más lento.
- Las solicitudes a un punto final que no se puedan completar se pondrán en cola a un máximo de 500.000 solicitudes. Este límite se comparte por igual entre los inquilinos activos. Los nuevos inquilinos pueden exceder temporalmente este límite de 500.000 para que los nuevos inquilinos no sean penalizados injustamente.

Información relacionada

- "Gestione los servicios de la plataforma"
- "Configure las opciones de proxy de almacenamiento"
- "Supervisar StorageGRID"

Red y puertos para servicios de plataforma

Si permite que un inquilino de S3 utilice los servicios de plataforma, debe configurar las redes para el grid para garantizar que los mensajes de servicios de plataforma se puedan entregar a sus destinos.

Puede habilitar los servicios de plataforma para una cuenta de inquilino de S3 al crear o actualizar la cuenta de inquilino. Si se habilitan los servicios de plataforma, el inquilino puede crear extremos que sirvan como destino para la replicación de CloudMirror, notificaciones de eventos o mensajes de integración de búsqueda desde sus bloques de S3. Estos mensajes de servicios de plataforma se envían desde los nodos de almacenamiento que ejecutan el servicio ADC a los extremos de destino.

Por ejemplo, los inquilinos pueden configurar los siguientes tipos de extremos de destino:

- Un clúster de Elasticsearch alojado localmente
- Una aplicación local que admite la recepción de mensajes de Amazon Simple Notification Service
- Un clúster Kafka alojado localmente
- Un punto final de webhook externo o alojado localmente que admite solicitudes de notificación HTTP POST.

  Este punto final se puede alojar en varios servidores web, marcos o herramientas de procesamiento de datos como Fluentd.

- Un bloque de S3 alojado localmente en la misma instancia de StorageGRID u otra
- Un extremo externo, como un extremo en Amazon Web Services.

Para garantizar que los mensajes de servicios de plataforma se puedan entregar, debe configurar la red o las redes que contienen los nodos de almacenamiento ADC. Debe asegurarse de que se pueden utilizar los siguientes puertos para enviar mensajes de servicios de plataforma a los extremos de destino.

De forma predeterminada, los mensajes de servicios de plataforma se envían a los siguientes puertos:

- **80**: Para URI de punto final que comienzan con http (la mayoría de los puntos finales)
- **443**: Para URI de punto final que comienzan con https (la mayoría de los puntos finales)
- **9092**: Para URI de punto final que comienzan con http o https (solo puntos finales Kafka)

Los inquilinos pueden especificar un puerto diferente cuando crean o editan un extremo.

> Si se usa una puesta en marcha de StorageGRID como destino de la replicación de CloudMirror, podrían recibirse mensajes de replicación en un puerto distinto de 80 o 443. Compruebe que el puerto que se utiliza para S3 en la implementación de StorageGRID de destino se especifique en el extremo.

Si utiliza un servidor proxy no transparente, también debe "configure las opciones del proxy de almacenamiento"permitir que los mensajes se envíen a puntos finales externos, como un punto final en Internet.

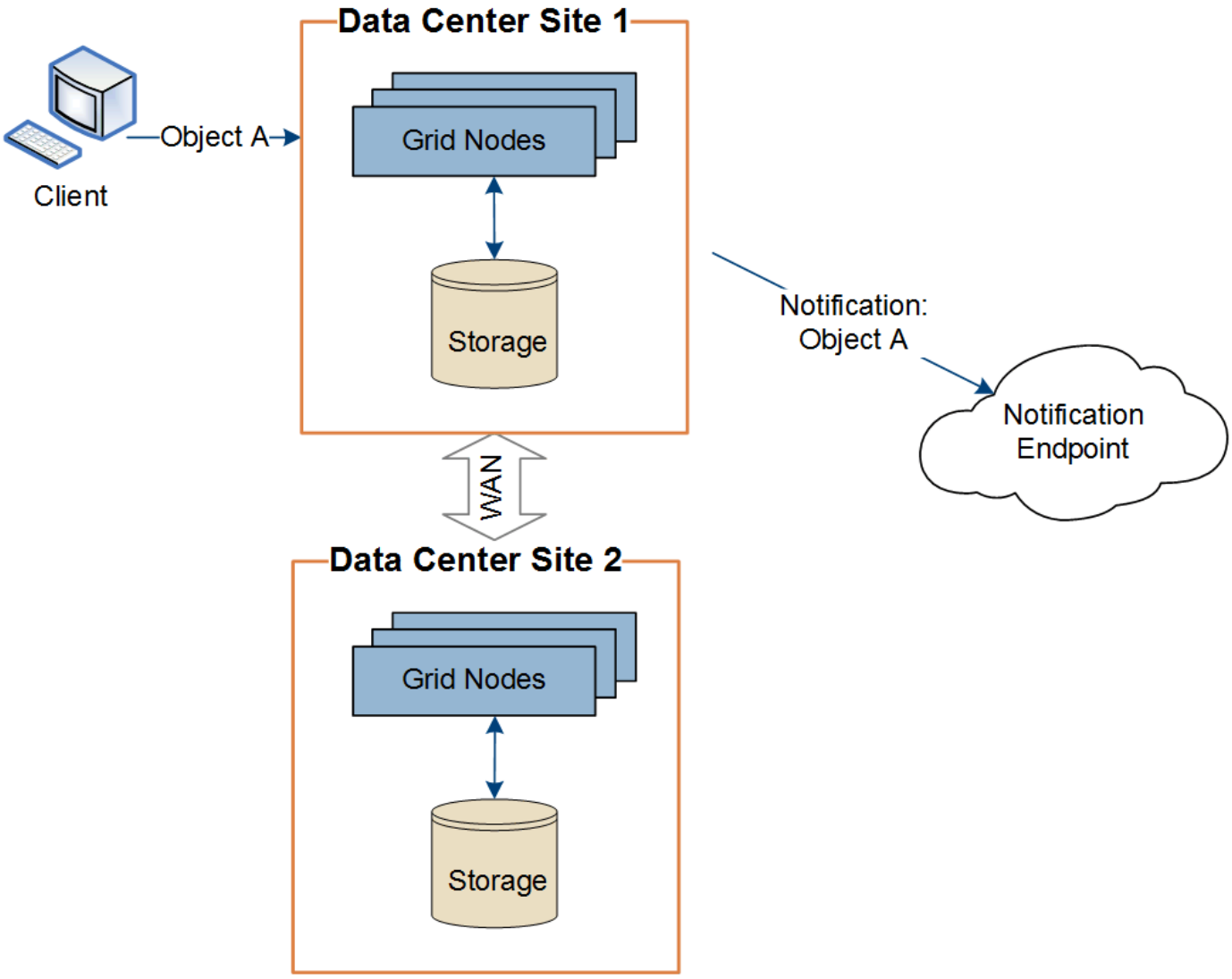
Información relacionada

"Usar una cuenta de inquilino"

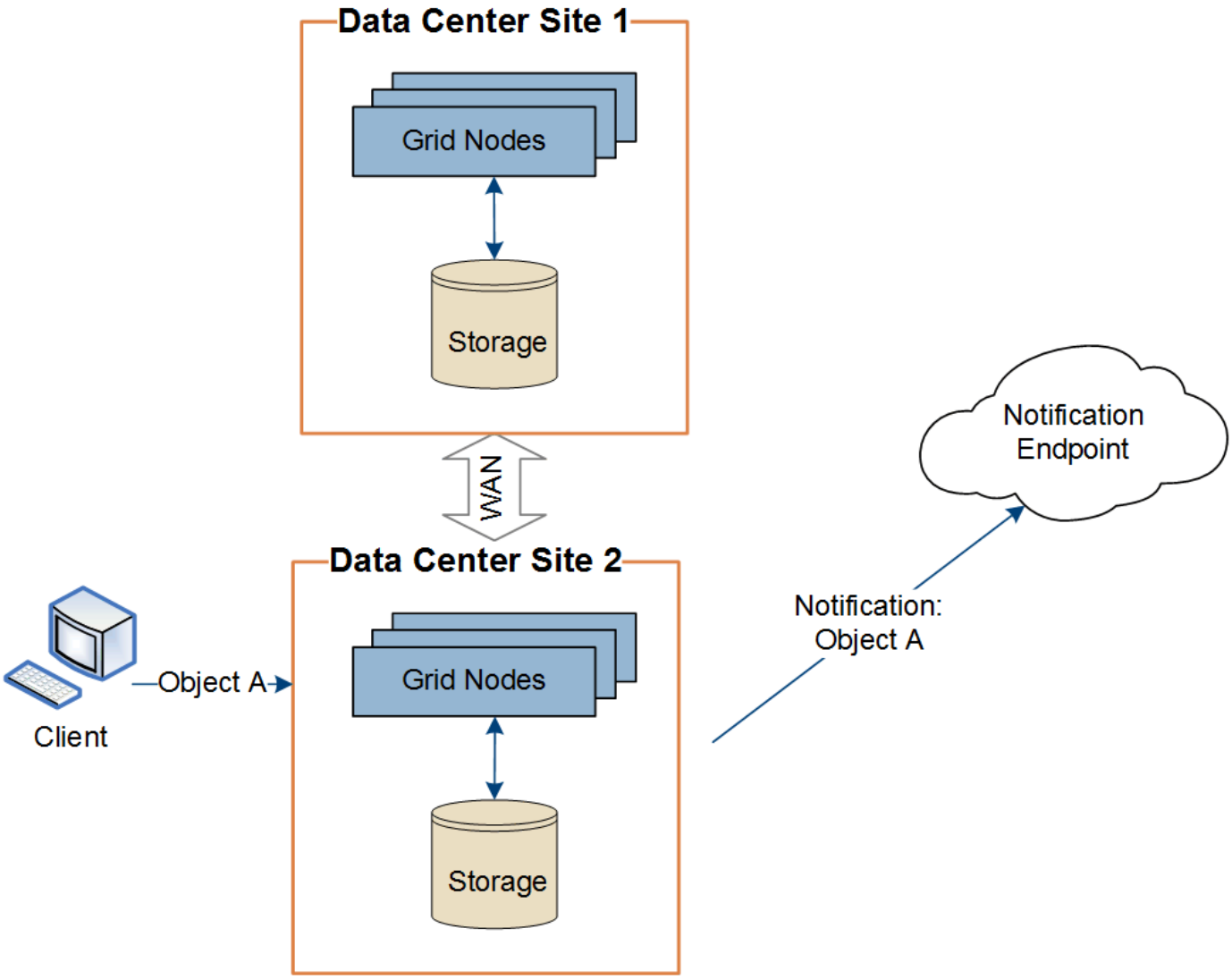
Entrega de mensajes de servicios de plataforma por sitio

Todas las operaciones de servicios de plataforma se realizan in situ.

Es decir, si un inquilino utiliza un cliente para realizar una operación S3 API Create en un objeto conectando a un nodo de puerta de enlace en el sitio 1 del centro de datos, se activa y envía la notificación acerca de esa acción desde el sitio 1 del centro de datos.



Si el cliente realiza posteriormente una operación de eliminación de API de S3 en ese mismo objeto desde el centro de datos Sitio 2, se activa y envía la notificación sobre la acción de eliminación desde el centro de datos Sitio 2.



Asegúrese de que la red de cada sitio esté configurada de modo que los mensajes de servicios de la plataforma se puedan entregar a sus destinos.

Solucione problemas de servicios de plataforma

Los extremos utilizados en los servicios de plataforma los crean y mantienen los usuarios de arrendatarios en el Administrador de arrendatarios; sin embargo, si un arrendatario tiene problemas al configurar o utilizar servicios de plataforma, puede utilizar el Administrador de grid para ayudar a resolver el problema.

Problemas con nuevos extremos

Para que un inquilino pueda utilizar los servicios de plataforma, deben crear uno o varios extremos mediante el administrador de inquilinos. Cada extremo representa un destino externo para un servicio de plataforma, como un bucket de StorageGRID S3, un bucket de Amazon Web Services, un tema del servicio de notificación simple de Amazon, un tema de Kafka o un clúster de Elasticsearch alojado localmente o en AWS. Cada extremo incluye la ubicación del recurso externo y las credenciales que se necesitan para acceder a ese recurso.

Cuando un inquilino crea un extremo, el sistema StorageGRID valida que existe el extremo y que se puede acceder a él utilizando las credenciales que se han especificado. La conexión con el extremo se valida desde

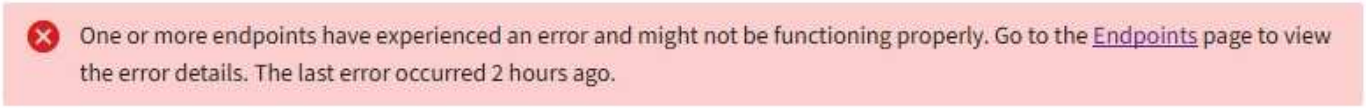
un nodo en cada sitio.

Si falla la validación del punto final, un mensaje de error explica por qué falló la validación del punto final. El usuario inquilino debe resolver el problema y, a continuación, intentar crear el extremo de nuevo.

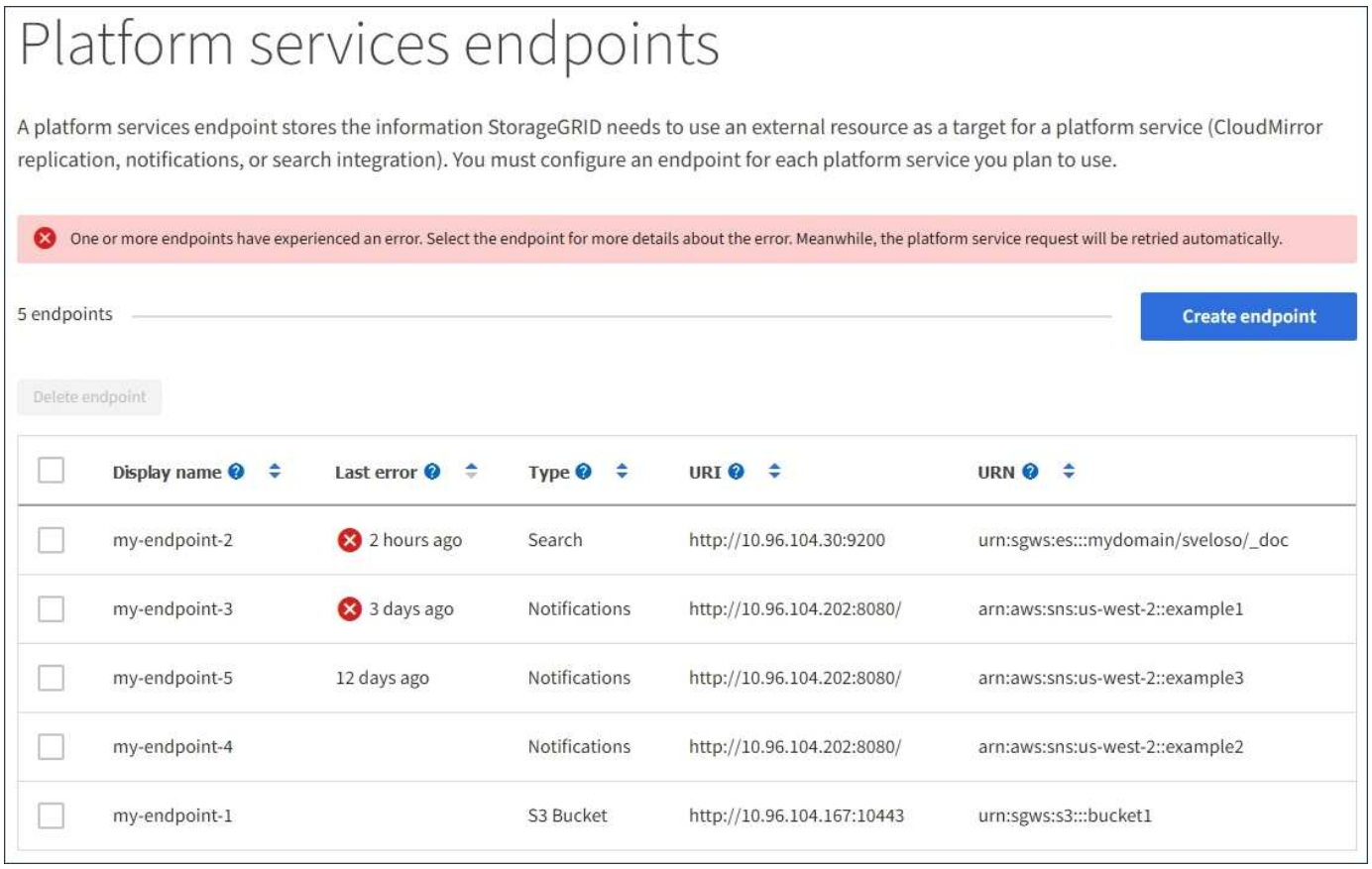
La creación de punto final fallará si los servicios de plataforma no están activados para la cuenta de inquilino.

Problemas con los extremos existentes

Si se produce un error cuando StorageGRID intenta llegar a un punto final existente, se muestra un mensaje en el panel de control del gestor de inquilinos.



Los usuarios de arrendatarios pueden ir a la página endpoints para revisar el mensaje de error más reciente de cada extremo y determinar cuánto tiempo ha ocurrido el error. La columna **último error** muestra el mensaje de error más reciente para cada extremo e indica cuánto tiempo se produjo el error. Los errores que incluyen el icono se han producido en los últimos 7 días.



Algunos mensajes de error en la columna **último error** pueden incluir un identificador de registro entre paréntesis. Un administrador de grid o soporte técnico puede usar este ID para encontrar información más detallada sobre el error en bycast.log.

Problemas relacionados con los servidores proxy

Si ha configurado un"proxy de almacenamiento" entre los nodos de almacenamiento y los puntos finales del servicio de la plataforma, pueden ocurrir errores si su servicio proxy no permite mensajes de StorageGRID. Para resolver estos problemas, verifique la configuración de su servidor proxy para asegurarse de que los mensajes relacionados con el servicio de la plataforma no estén bloqueados.

Determine si se ha producido un error

Si se ha producido algún error de punto final en los últimos 7 días, el panel de control del gestor de inquilinos muestra un mensaje de alerta. Puede ir a la página endpoints para ver más detalles sobre el error.

Error en las operaciones del cliente

Algunos problemas de los servicios de plataforma pueden provocar errores en las operaciones del cliente en el bloque de S3. Por ejemplo, las operaciones del cliente S3 fallarán si se detiene el servicio interno Replicated State Machine (RSM) o si hay demasiados mensajes de servicios de plataforma en cola para su entrega.

Para comprobar el estado de los servicios:

1. Seleccione **Nodos** > ***sitio*** > ***Nodo de almacenamiento*** > **Descripción general**.
2. Compruebe si hay alertas activas en la tabla Alertas.
3. Resuelva cualquier alerta activa. Según sea necesario, comuníquese con el soporte técnico.

Errores de punto final recuperables e irrecuperables

Una vez creados los extremos, los errores de solicitud de servicio de la plataforma pueden producirse por varios motivos. Algunos errores se pueden recuperar con la intervención del usuario. Por ejemplo, pueden producirse errores recuperables por los siguientes motivos:

- Las credenciales del usuario se han eliminado o han caducado.
- El depósito de destino no existe.
- No se puede entregar la notificación.

Si StorageGRID encuentra un error recuperable, la solicitud de servicio de la plataforma se reintentará hasta que se complete correctamente.

Otros errores son irrecuperables. Por ejemplo, podrían producirse errores irrecuperables por las siguientes razones:

- Se elimina el punto final.
- Un destino de punto final de webhook responde a una solicitud de notificación con un `400 Bad Request` error.

Si StorageGRID encuentra un error de punto final irrecuperable:

- En Grid Manager, vaya a **Soporte** > **Herramientas** > **Métricas** > **Grafana** > **Descripción general de los servicios de la plataforma** para ver los detalles del error.
- En el gestor de inquilinos, vaya a **STORAGE (S3)** > **Platform Services Endpoints** para ver los detalles del error.
- Consulte la `/var/local/log/bycast-err.log` para ver los errores relacionados. Los nodos de

almacenamiento que tienen el servicio ADC contienen este archivo de registro.

Los mensajes de servicios de plataforma no se pueden entregar

Si el destino encuentra un problema que le impide aceptar mensajes de servicios de plataforma, la operación del cliente en el depósito se realiza correctamente, pero el mensaje de servicios de plataforma no se entrega. Por ejemplo, este error podría ocurrir si las credenciales se actualizan en el destino de tal manera que StorageGRID ya no puede autenticarse en el servicio de destino.

Compruebe si hay alertas relacionadas.

Rendimiento más lento para las solicitudes de servicio de la plataforma

El software StorageGRID puede reducir las solicitudes entrantes de S3 para un bloque si la velocidad a la que se envían las solicitudes supera la velocidad a la que el extremo de destino puede recibir las solicitudes. La limitación sólo se produce cuando hay una acumulación de solicitudes que están a la espera de ser enviadas al extremo de destino.

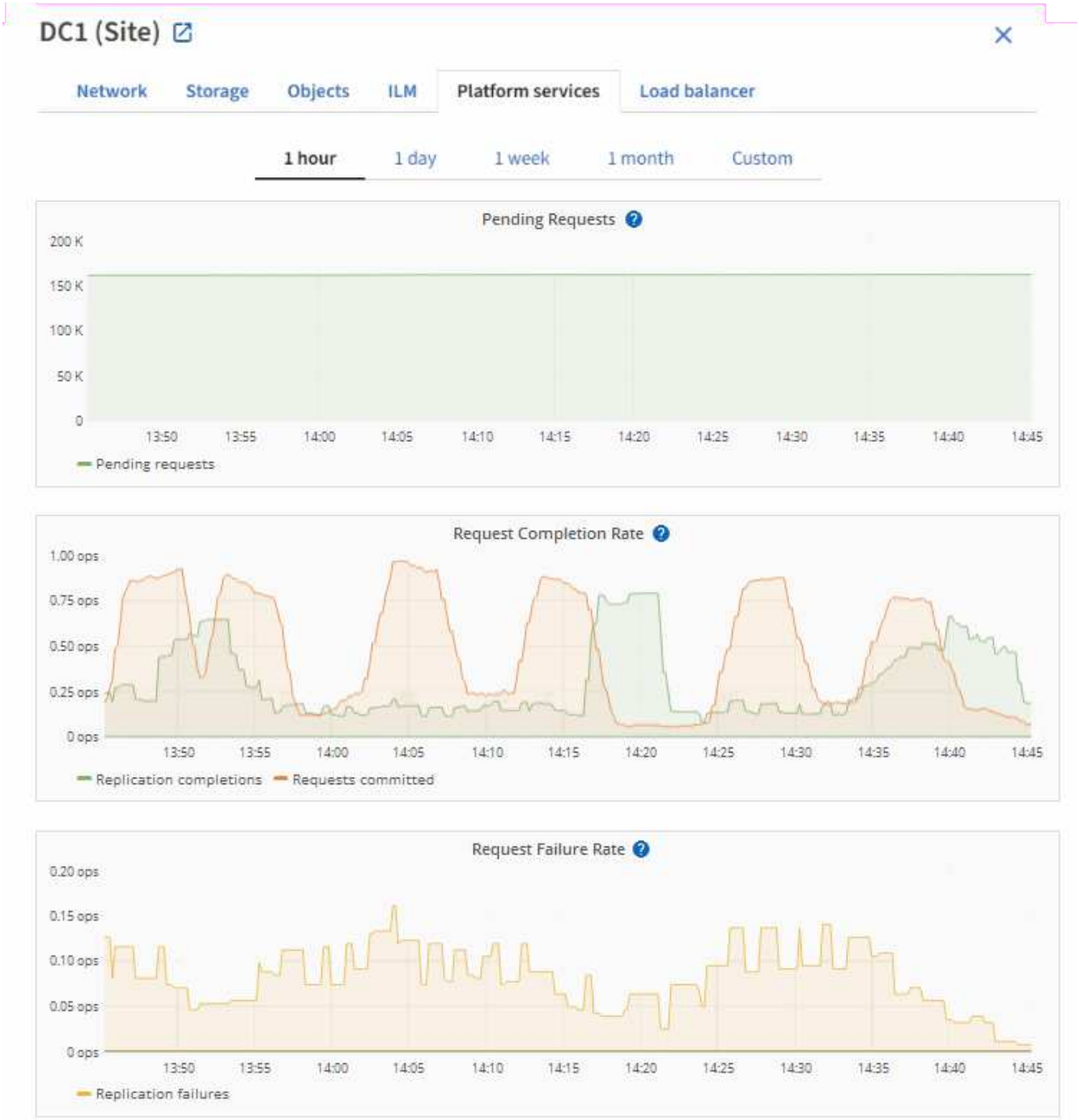
El único efecto visible es que las solicitudes entrantes de S3 tardarán más en ejecutarse. Si empieza a detectar un rendimiento significativamente más lento, debe reducir la tasa de procesamiento o utilizar un extremo con mayor capacidad. Si la acumulación de solicitudes sigue creciendo, las operaciones de S3 del cliente (como SOLICITUDES PUT) fallarán en el futuro.

Las solicitudes de CloudMirror tienen más probabilidades de que se vean afectadas por el rendimiento del extremo de destino, ya que estas solicitudes suelen requerir más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.

Las solicitudes de servicio de la plataforma fallan

Para ver la tasa de fallos de solicitud para servicios de plataforma:

1. Seleccionar **Nodos**.
2. Seleccione ***site*** > **Servicios de plataforma**.
3. Vea el gráfico de tasa de errores de solicitud.



Alerta de servicios de plataforma no disponibles

La alerta **Servicios de plataforma no disponibles** indica que no se pueden realizar operaciones de servicio de plataforma en un sitio porque hay demasiados nodos de almacenamiento con el servicio RSM en ejecución o disponibles.

El servicio RSM garantiza que las solicitudes de servicio de la plataforma se envíen a sus respectivos extremos.

Para resolver esta alerta, determine qué nodos de almacenamiento del sitio incluyen el servicio RSM. (El servicio RSM está presente en los nodos de almacenamiento que también incluyen el servicio ADC). A continuación, asegúrese de que la mayoría sencilla de estos nodos de almacenamiento están en ejecución y disponible.

Si se produce un error en más de un nodo de almacenamiento que contiene el servicio RSM de un sitio, perderá las solicitudes de servicio de plataforma pendientes para ese sitio.

Orientación adicional para la solución de problemas para extremos de servicios de la plataforma

Para obtener más información, consulte **Use una cuenta de inquilino › Solucionar problemas de los extremos de servicios de la plataforma**.

Información relacionada

"Solucionar los problemas del sistema StorageGRID"

Gestione S3 Select para cuentas de inquilinos

Puede permitir que determinados inquilinos S3 usen S3 Select para emitir solicitudes SelectObjectContent en objetos individuales.

S3 Select proporciona una forma eficiente de buscar en grandes cantidades de datos sin tener que implementar una base de datos y recursos asociados para permitir las búsquedas. También reduce el coste y la latencia de la recuperación de datos.

¿Qué es S3 Select?

S3 Select permite que los clientes S3 utilicen solicitudes SelectObjectContent para filtrar y recuperar solo los datos necesarios de un objeto. La implementación de StorageGRID de S3 Select incluye un subconjunto de comandos y funciones de S3 Select.

Consideraciones y requisitos para usar S3 Select

Requisitos de administración de grid

El administrador de grid debe conceder a los inquilinos la Capacidad Select S3. Seleccione **Permitir S3 Seleccionar** Cuando "crear un inquilino" o "edición de un arrendatario".

Requisitos de formato de objeto

El objeto que desea consultar debe tener uno de los siguientes formatos:

- **CSV**. Se puede utilizar tal cual o comprimir en archivos GZIP o bzip2.
- **Parquet**. Requisitos adicionales para objetos de parquet:
  - S3 Select solo admite la compresión en columnas usando GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos de parquet.
  - S3 La selección no es compatible con la salida de parquet. Debe especificar el formato de salida como CSV o JSON.
  - El tamaño máximo del grupo de filas sin comprimir es de 512 MB.
  - Debe utilizar los tipos de dato especificados en el esquema del objeto.
  - No puede utilizar los tipos lógicos INTERVAL, JSON, LIST, TIME o UUID.

Requisitos de los extremos

La solicitud SelectObjectContent debe enviarse a un "Extremo del equilibrador de carga de StorageGRID".

Los nodos de administración y puerta de enlace utilizados por el punto final deben ser uno de los siguientes:

- Un nodo de dispositivo de servicios
- Nodo de software basado en VMware
- Nodo bare metal que ejecuta un kernel con cgroup v2 habilitado

Consideraciones generales

Las consultas no pueden enviarse directamente a los nodos de almacenamiento.

> Las solicitudes SelectObjectContent pueden reducir el rendimiento de equilibrio de carga de todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

Consulte la "Instrucciones para usar S3 Select".

Para ver"Gráficos Grafana" Para seleccionar operaciones a lo largo del tiempo, seleccione **Soporte** > **Herramientas** > **Métricas** en el Administrador de cuadrícula.

Configurar conexiones de cliente

Configure las conexiones de cliente S3

Como administrador de grid, usted administra las opciones de configuración que controlan cómo las aplicaciones cliente S3 se conectan al sistema StorageGRID para almacenar y recuperar datos.

> Se han eliminado los detalles de Swift de esta versión del sitio del documento. Consulte "StorageGRID 11,8: Configure las conexiones de clientes S3 y Swift".

Tareas de configuración

1. Realice tareas de requisitos previos en StorageGRID, según cómo se conectará la aplicación cliente a StorageGRID.

Tareas requeridas

Debe obtener:

- Direcciones IP
- Nombres de dominio
- Certificado SSL

Tareas opcionales

Opcionalmente, configure:

- federación de identidades
- SSO

1. Utilice StorageGRID para obtener los valores que la aplicación necesita para conectarse a la cuadrícula. Puede utilizar el asistente de configuración de S3 o configurar cada entidad de StorageGRID manualmente.

Utilice el asistente de configuración de S3

Siga los pasos del asistente de configuración de S3.

Configura manualmente

1. Cree un grupo de alta disponibilidad
2. Crear punto final de equilibrador de carga
3. Cree una cuenta de inquilino
4. Crear bloque y claves de acceso
5. Configurar la regla y la política de ILM

1. Utilice la aplicación S3 para completar la conexión a StorageGRID. Cree entradas DNS para asociar direcciones IP a cualquier nombre de dominio que desee utilizar.

   Si es necesario, realice una configuración de aplicación adicional.

2. Realice tareas continuas en la aplicación y en StorageGRID para gestionar y supervisar el almacenamiento de objetos a lo largo del tiempo.

Información necesaria para asociar StorageGRID a una aplicación cliente

Para poder asociar StorageGRID a una aplicación cliente S3, debe realizar pasos de configuración en StorageGRID y obtener cierto valor.

¿Qué valores necesito?

La siguiente tabla muestra los valores que debe configurar en StorageGRID y dónde los utilizan la aplicación S3 y el servidor DNS.

Valor	Donde se configura el valor	Donde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto final del equilibrador de carga	Aplicación cliente
Certificado SSL	StorageGRID > Punto final del equilibrador de carga	Aplicación cliente
Nombre del servidor (FQDN)	StorageGRID > Punto final del equilibrador de carga	• Aplicación cliente • Entrada DNS
S3 ID de clave de acceso y clave de acceso secreta	StorageGRID > inquilino y bloque	Aplicación cliente

Valor	Donde se configura el valor	Donde se utiliza el valor
Nombre de cubo/contenedor	StorageGRID > inquilino y bloque	Aplicación cliente

¿Cómo obtengo estos valores?

Dependiendo de sus requisitos, puede hacer cualquiera de los siguientes pasos para obtener la información que necesita:

- **Utilice el "S3 Asistente de configuración"**. El asistente de configuración de S3 le ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera uno o dos archivos que puede utilizar al configurar la aplicación S3. El asistente le guiará por los pasos necesarios y le ayudará a garantizar que la configuración cumple las prácticas recomendadas de StorageGRID.

  > Si está configurando una aplicación S3, se recomienda utilizar el asistente de configuración de S3 a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

- **Utilice el "Asistente de configuración de FabricPool"**. De forma similar al asistente de configuración de S3, el asistente de configuración de FabricPool ayuda a configurar rápidamente los valores necesarios y genera un archivo que se puede usar al configurar un nivel de cloud de FabricPool en ONTAP.

  > Si va a utilizar StorageGRID como sistema de almacenamiento de objetos para un nivel cloud de FabricPool, se recomienda utilizar el asistente de configuración de FabricPool, a menos que sepa que tiene requisitos especiales o que su implementación requerirá una gran personalización.

- **Configurar artículos manualmente**. Si se conecta a una aplicación S3 y prefiere no utilizar el asistente de configuración de S3, puede obtener los valores necesarios realizando la configuración manualmente. Siga estos pasos:
  a. Configure el grupo de alta disponibilidad (HA) que desee utilizar para la aplicación S3. Consulte "Configuración de grupos de alta disponibilidad".
  b. Cree el punto final de equilibrio de carga que utilizará la aplicación S3. Consulte "Configurar puntos finales del equilibrador de carga".
  c. Cree la cuenta de inquilino que utilizará la aplicación S3. Consulte "Cree una cuenta de inquilino".
  d. Para un inquilino de S3, inicie sesión en la cuenta de inquilino y genere un ID de clave de acceso y una clave de acceso secreta para cada usuario que acceda a la aplicación. Consulte "Cree sus propias claves de acceso".
  e. Cree uno o varios bloques de S3 dentro de la cuenta de inquilino. Para S3, consulte "Crear bloque de S3".
  f. Para agregar instrucciones de ubicación específicas para los objetos que pertenecen al inquilino o bloque/contenedor nuevo, cree una regla de ILM nueva y active una nueva política de ILM para utilizar esa regla. Consulte "Cree la regla de ILM" y "Cree una política de ILM".

Seguridad para clientes S3

Las cuentas de inquilino de StorageGRID usan aplicaciones cliente S3 para guardar datos de objetos en StorageGRID. Debe revisar las medidas de seguridad implementadas para las aplicaciones cliente.

Resumen

En la lista siguiente se resume cómo se implementa la seguridad para la API de REST DE S3:

Seguridad de la conexión

TLS

Autenticación del servidor

Certificado de servidor X.509 firmado por CA del sistema o certificado de servidor personalizado suministrado por el administrador

Autentificación de clientes

S3 ID de clave de acceso de cuenta y clave de acceso secreta

Autorización de cliente

Propiedad de buckets y todas las políticas de control de acceso aplicables

Cómo ofrece StorageGRID seguridad a las aplicaciones cliente

Las aplicaciones cliente S3 pueden conectarse al servicio de equilibrio de carga en los nodos de la puerta de enlace o los nodos de administración, o bien directamente a los nodos de almacenamiento.

- Los clientes que se conectan al servicio Load Balancer pueden usar HTTPS o HTTP, según su forma"configure el punto final del equilibrador de carga".

  HTTPS proporciona una comunicación segura cifrada con TLS y se recomienda. Debe adjuntar un certificado de seguridad al punto final.

  HTTP proporciona una comunicación menos segura y sin cifrar y solo debe utilizarse para redes que no sean de producción o de prueba.

- Los clientes que se conectan a los nodos de almacenamiento también pueden usar HTTPS o HTTP.

  HTTPS es el valor predeterminado y se recomienda.

  HTTP proporciona una comunicación menos segura y sin cifrar, pero puede ser opcionalmente "activado" para redes que no sean de producción o de prueba.

- Las comunicaciones entre StorageGRID y el cliente se cifran mediante TLS.
- Las comunicaciones entre el servicio Load Balancer y los nodos de almacenamiento de la cuadrícula están cifradas si el extremo de equilibrio de carga está configurado para aceptar conexiones HTTP o HTTPS.
- Los clientes deben suministrar "Cabeceras de autenticación HTTP" a StorageGRID para realizar operaciones de API DE REST.

Certificados de seguridad y aplicaciones cliente

En todos los casos, las aplicaciones cliente pueden realizar conexiones TLS mediante un certificado de servidor personalizado cargado por el administrador de grid o un certificado generado por el sistema StorageGRID:

- Cuando las aplicaciones cliente se conectan al servicio Load Balancer, utilizan el certificado configurado para el punto final del equilibrio de carga. Cada punto final del equilibrador de carga tiene su propio certificado— un certificado de servidor personalizado cargado por el administrador de grid o un certificado

que el administrador de grid generó en StorageGRID al configurar el punto final.

Consulte "Consideraciones que tener en cuenta al equilibrio de carga".

- Cuando las aplicaciones cliente se conectan directamente a un nodo de almacenamiento, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (que están firmados por la entidad de certificación del sistema), o bien, un único certificado de servidor personalizado proporcionado para la cuadrícula por un administrador de grid. Consulte "Agregue un certificado API S3 personalizado".

Los clientes deben configurarse para que confíen en la entidad emisora de certificados que firmó el certificado que utilicen para establecer conexiones TLS.

Algoritmos de cifrado y hash compatibles para bibliotecas TLS

El sistema StorageGRID admite un conjunto de conjuntos de cifrado que las aplicaciones cliente pueden usar al establecer una sesión TLS. Para configurar cifrados, vaya a **Configuración** > **Seguridad** > **Configuración de seguridad** y seleccione **Políticas TLS y SSH**.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3.

SSLv3 y TLS 1.1 (o versiones anteriores) ya no son compatibles.

Utilice el asistente de configuración de S3

Utilice el asistente de configuración de S3: Consideraciones y requisitos

Puede usar el asistente de configuración de S3 para configurar StorageGRID como el sistema de almacenamiento de objetos de una aplicación S3.

Cuándo utilizar el asistente de configuración de S3

El asistente de configuración de S3 le guiará en cada paso de la configuración de StorageGRID para su uso con una aplicación S3. Como parte de completar el asistente, descargará archivos que puede utilizar para introducir valores en la aplicación S3. Utilice el asistente para configurar su sistema con mayor rapidez y asegurarse de que su configuración cumple las prácticas recomendadas de StorageGRID.

Si dispone de "Permiso de acceso raíz", puede completar el asistente de configuración de S3 cuando comience a utilizar el Administrador de grid de StorageGRID, o bien puede acceder y completar el asistente en cualquier momento posterior. En función de los requisitos, también puede configurar algunos o todos los elementos necesarios manualmente y, a continuación, utilizar el asistente para ensamblar los valores que necesita una aplicación S3.

Antes de utilizar el asistente

Antes de utilizar el asistente, confirme que ha completado estos requisitos previos.

Obtenga direcciones IP y configure interfaces VLAN

Si va a configurar un grupo de alta disponibilidad (HA), sabrá a qué nodos se conectará la aplicación S3 y a qué red StorageGRID se utilizará. También sabe qué valores introducir para la subred CIDR, la dirección IP de la puerta de enlace y las direcciones IP virtuales (VIP).

Si planea utilizar una LAN virtual para segregar el tráfico de la aplicación S3, ya ha configurado la interfaz VLAN. Consulte "Configure las interfaces VLAN".

Configurar la federación de identidades y SSO

Si planea utilizar la federación de identidad o el inicio de sesión único (SSO) para su sistema StorageGRID , debe habilitar estas funciones. También sabe qué grupo federado debe tener acceso raíz para la cuenta de inquilino que utilizará la aplicación S3. Ver"Usar la federación de identidades" y"Configurar el inicio de sesión único" .

Obtener y configurar nombres de dominio

Sabe qué nombre de dominio completo (FQDN) debe utilizar para StorageGRID. Las entradas del servidor de nombres de dominio (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad que cree con el asistente.

Si planea utilizar S3 solicitudes virtuales de estilo hospedado, debe tener "Nombres de dominio de punto final S3 configurados". Se recomienda utilizar solicitudes virtuales de estilo alojado.

Revisión de los requisitos del equilibrio de carga y del certificado de seguridad

Si tiene pensado utilizar el equilibrador de carga de StorageGRID, ha revisado las consideraciones generales sobre el equilibrio de carga. Tiene los certificados que cargará o los valores necesarios para generar un certificado.

Si planea utilizar un punto final de equilibrio de carga externo (de terceros), tiene el nombre de dominio completo (FQDN), el puerto y el certificado para ese equilibrador de carga.

Configure cualquier conexión de federación de grid

Si desea permitir que el inquilino S3 clone los datos de la cuenta y replique objetos del bloque en otra cuadrícula mediante una conexión de federación de grid, antes de iniciar el asistente confirme lo siguiente:

- Tienes "se ha configurado la conexión de federación de grid".
- El estado de la conexión es **Conectado**.
- Tiene permiso de acceso raíz.

Acceda al asistente de configuración de S3 y complete este

Puede utilizar el asistente de configuración de S3 para configurar StorageGRID para su uso con una aplicación S3. El asistente de configuración proporciona los valores que la aplicación necesita para acceder a un bucket de StorageGRID y guardar objetos.

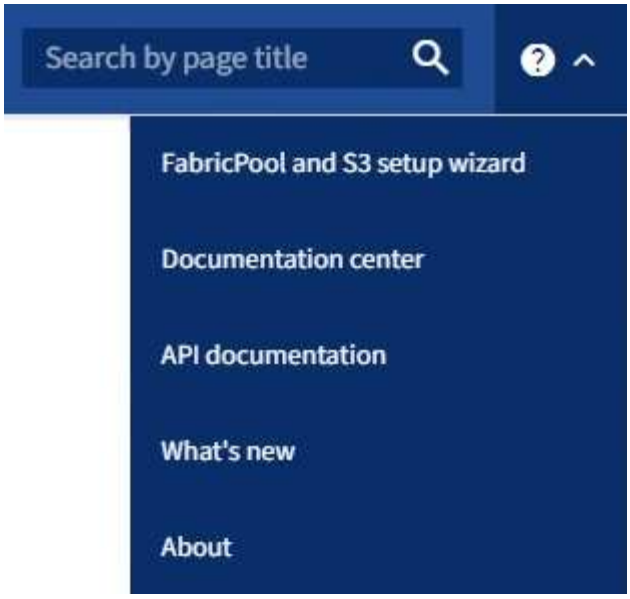
Antes de empezar

- Usted tiene el "Permiso de acceso raíz".
- Ha revisado el "consideraciones y requisitos" para utilizar el asistente.

Acceda al asistente

Pasos

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Si el banner del asistente de configuración **FabricPool y S3** aparece en el panel de control, seleccione el enlace en el banner. Si el banner ya no aparece, seleccione el icono de ayuda en la barra de encabezado del Administrador de cuadrículas y seleccione **FabricPool y el asistente de configuración S3**.



3. En la sección de aplicación S3 de la página del asistente de configuración de FabricPool y S3, seleccione **Configurar ahora**.

Paso 1 de 6: Configurar el grupo de alta disponibilidad

Un grupo de alta disponibilidad es una colección de nodos que contiene cada uno de ellos el servicio de equilibrador de carga de StorageGRID. Un grupo de alta disponibilidad puede contener nodos de pasarela, nodos de administración o ambos.

Puede usar un grupo de alta disponibilidad para ayudar a mantener las conexiones de datos de S3 GbE disponibles. Si falla la interfaz activa del grupo HA, una interfaz de backup puede gestionar la carga de trabajo con poco impacto en las operaciones de S3.

Para obtener detalles sobre esta tarea, consulte "Gestión de grupos de alta disponibilidad".

Pasos

1. Si va a utilizar un equilibrador de carga externo, no es necesario crear un grupo de alta disponibilidad. Seleccione **Omitir este paso** y vaya a Paso 2 de 6: Configurar punto final de equilibrio de carga.
2. Para usar el equilibrador de carga de StorageGRID, es posible crear un grupo de alta disponibilidad nuevo o usar un grupo de alta disponibilidad existente.

Crear grupo de alta disponibilidad

a. Para crear un nuevo grupo HA, selecciona **Crear grupo HA**.

b. Para el paso **Enter details**, complete los siguientes campos.

Campo	Descripción
Nombre del GRUPO HA	Un nombre mostrado exclusivo para este grupo HA.
Descripción (opcional)	La descripción de este grupo de alta disponibilidad.

c. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo HA.

Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.

Puede seleccionar uno o varios nodos, pero solo puede seleccionar una interfaz para cada nodo.

d. Para el paso **Priorize interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo HA.

Arrastre las filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.

Si el grupo de alta disponibilidad incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de respaldo, etc. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

e. Para el paso **Introducir direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en la notación CIDR — una dirección IPv4 seguida de una barra diagonal y la longitud de subred (0-32). La dirección de red no debe tener ningún bit de host configurado. Por ejemplo, `192.16.0.0/22`.
Dirección IP de la puerta de enlace (opcional)	Si las direcciones IP de S3 utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID, introduzca la dirección IP de la puerta de enlace local VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	Introduzca al menos una y como máximo diez direcciones VIP para la interfaz activa en el grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

f. Seleccione **Crear grupo HA** y luego seleccione **Finalizar** para volver al asistente de configuración S3.

g. Seleccione **Continuar** para ir al paso del equilibrador de carga.

Use el grupo de alta disponibilidad existente

a. Para usar un grupo HA existente, seleccione el nombre del grupo HA en el **Seleccione un grupo HA**.

b. Seleccione **Continuar** para ir al paso del equilibrador de carga.

Paso 2 de 6: Configurar punto final de equilibrio de carga

StorageGRID utiliza un balanceador de carga para gestionar la carga de trabajo desde aplicaciones cliente. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en varios nodos de almacenamiento.

Puede usar el servicio de equilibrador de carga de StorageGRID, que existe en todos los nodos de administración y puerta de enlace, o puede conectarse a un equilibrador de carga externo (de terceros). Se recomienda utilizar el equilibrador de carga de StorageGRID.

Para obtener detalles sobre esta tarea, consulte "Consideraciones que tener en cuenta al equilibrio de carga".

Para usar el servicio de Equilibrador de Carga de StorageGRID, seleccione la pestaña **Equilibrador de Carga de StorageGRID** y, a continuación, cree o seleccione el punto final del equilibrador de carga que desea utilizar. Para usar un equilibrador de carga externo, selecciona la pestaña **Equilibrador de carga externo** y proporciona detalles sobre el sistema que ya has configurado.

Crear punto final

Pasos

1. Para crear un punto final de equilibrio de carga, selecciona **Crear punto final**.
2. Para el paso **Introducir detalles de punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Nombre descriptivo para el punto final.
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. Este campo se establece por defecto en 10433 para el primer punto final que cree, pero puede introducir cualquier puerto externo no utilizado. Si introduce 80 o 443, el punto final se configura sólo en los nodos de Gateway, ya que estos puertos están reservados en los nodos de Admin. **Nota:** No se permiten los puertos utilizados por otros servicios de red. Ver "Puertos internos StorageGRID" .
Tipo de cliente	Debe ser **S3**.
Protocolo de red	Seleccione **HTTPS**. **Nota**: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

3. Para el paso **Select Binding mode**, especifique el modo de encuadernación. El modo de enlace controla cómo se accede al punto final mediante cualquier dirección IP o mediante direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final mediante la dirección IP de cualquier nodo de gateway o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice el ajuste **Global** (predeterminado) a menos que necesite restringir la accesibilidad de este extremo.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad para acceder a este extremo. Los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que seleccione para los puntos finales no se superpongan.

Modo	Descripción
Interfaces de nodos	Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo	En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este extremo.

4. Para el paso de acceso de arrendatario, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir todos los inquilinos (predeterminado)	Todas las cuentas de inquilino pueden usar este extremo para acceder a sus bloques.
Permitir arrendatarios seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este extremo para acceder a sus bloques.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este punto final para acceder a sus bloques. Todos los demás inquilinos pueden usar este extremo.

5. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Cargar certificado (recomendado)	Use esta opción para cargar un certificado de servidor firmado por CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Use esta opción para generar un certificado autofirmado. Consulte "Configurar puntos finales del equilibrador de carga" para obtener más información sobre los elementos que se deben introducir.
Utilice el certificado StorageGRID S3	Utilice esta opción solo si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID. Consulte "Configure los certificados de API S3" para obtener más información.

6. Seleccione **Finalizar** para volver al asistente de configuración de S3.
7. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utilizar punto final de equilibrio de carga existente

Pasos

1. Para usar un punto final existente, seleccione su nombre en el **Seleccione un punto final de equilibrio de carga**.
2. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Utilizar equilibrador de carga externo

Pasos

1. Para utilizar un equilibrador de carga externo, complete los siguientes campos.

Campo	Descripción
FQDN	Nombre de dominio completo (FQDN) del equilibrador de carga externo.
Puerto	Número de puerto que utilizará la aplicación S3 para conectarse al equilibrador de carga externo.
Certificado	Copie el certificado del servidor para el equilibrador de carga externo y péguelo en este campo.

2. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Paso 3 de 6: Crear inquilino y bloque

Un inquilino es una entidad que puede utilizar aplicaciones S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, bloques, objetos y un conjunto específico de funcionalidades.

Un bucket es un contenedor que se usa para almacenar los objetos y los metadatos de objetos de un inquilino. Aunque puede que los inquilinos tengan muchos buckets, el asistente le ayuda a crear un inquilino y un bloque de la forma más rápida y sencilla. Si necesita agregar cubos o establecer opciones más tarde, puede utilizar el Gestor de inquilinos.

Para obtener detalles sobre esta tarea, consulte "Cree una cuenta de inquilino" y "Crear bloque de S3".

Pasos

1. Escriba un nombre para la cuenta de inquilino.

   Los nombres de inquilinos no necesitan ser únicos. Cuando se crea la cuenta de arrendatario, recibe un ID de cuenta numérico único.

2. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza"federación de identidades" ,"Inicio de sesión único (SSO)" , o ambos.

Opción	Haga esto
Si la federación de identidades no está activada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.

Opción	Haga esto
Si la federación de identidades está activada	a. Seleccione un grupo federado existente para "Permiso de acceso raíz"el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si se activan tanto la federación de identidades como el inicio de sesión único (SSO)	Seleccione un grupo federado existente para "Permiso de acceso raíz"el inquilino. Ningún usuario local puede iniciar sesión.

3. Si desea que el asistente cree el ID de clave de acceso y la clave de acceso secreta para el usuario root, seleccione **Crear clave de acceso S3 de usuario root automáticamente**.

   Seleccione esta opción si el único usuario para el arrendatario será el usuario root. Si otros usuarios usarán este inquilino, "Utilizar el gestor de inquilinos" para configurar claves y permisos.

4. Si desea crear un depósito para este inquilino ahora, seleccione **Crear depósito para este inquilino**.

   Si S3 Object Lock está habilitado para la cuadrícula, el depósito creado en este paso no tiene S3 Object Lock habilitado. Si necesita usar un depósito de bloqueo de objetos S3 para esta aplicación S3, no seleccione crear un depósito ahora. En su lugar, utilice Tenant Manager "cree el cucharón"para más adelante.

   a. Introduzca el nombre del depósito que utilizará la aplicación S3. Por ejemplo, `s3-bucket`.

      No puede cambiar el nombre del bloque después de crear el bloque.

   b. Seleccione la **Región** para este cubo.

      Utilice la región por defecto (`us-east-1`) a menos que espere utilizar ILM en el futuro para filtrar objetos según la región del bloque.

5. Selecciona **Crear y continuar**.

Paso 4 de 6: Descargar datos

En el paso de descarga de datos, puede descargar uno o dos archivos para guardar los detalles de lo que acaba de configurar.

Pasos

1. Si seleccionó **Crear clave de acceso S3 de usuario root automáticamente**, realice una o ambas de las siguientes acciones:
   - Seleccione **Descargar claves de acceso** para descargar un `.csv` archivo que contenga el nombre de la cuenta de inquilino, el ID de clave de acceso y la clave de acceso secreta.
   - Seleccione el icono de copia ( ) para copiar el ID de clave de acceso y la clave de acceso secreta en el portapapeles.
2. Seleccione **Descargar valores de configuración** para descargar un `.txt` archivo que contenga la configuración para el punto final del equilibrador de carga, el inquilino, el depósito y el usuario raíz.
3. Guarde esta información en una ubicación segura.

No cierre esta página hasta que haya copiado ambas claves de acceso. Las teclas no estarán disponibles después de cerrar esta página. Asegúrese de guardar esta información en una ubicación segura, ya que se puede utilizar para obtener datos de su sistema StorageGRID.

4. Si se le solicita, seleccione la casilla de verificación para confirmar que ha descargado o copiado las claves.
5. Seleccione **Continuar** para ir a la regla de ILM y paso de política.

Paso 5 de 6: Revise la regla de ILM y la política de ILM para S3

Las reglas de gestión de la vida útil de la información controlan la ubicación, la duración y el comportamiento de procesamiento de todos los objetos del sistema StorageGRID. La política de ILM incluida con StorageGRID hace dos copias replicadas de todos los objetos. Esta política está en vigor hasta que active al menos una nueva política.

Pasos

1. Revise la información proporcionada en la página.
2. Si desea agregar instrucciones específicas para los objetos que pertenecen al nuevo arrendatario o depósito, cree una nueva regla y una nueva política. Consulte "Cree la regla de ILM" y "Use políticas de ILM".
3. Seleccione **He revisado estos pasos y entiendo lo que tengo que hacer**.
4. Seleccione la casilla de verificación para indicar que comprende qué hacer a continuación.
5. Selecciona **Continuar** para ir a **Resumen**.

Paso 6 de 6: Resumen de la revisión

Pasos

1. Revise el resumen.
2. Anote los detalles en los siguientes pasos, que describen la configuración adicional que puede ser necesaria antes de conectarse al cliente S3. Por ejemplo, si selecciona **Iniciar sesión como root**, accederá al gestor de inquilinos, donde podrá agregar usuarios de inquilinos, crear depósitos adicionales y actualizar la configuración del depósito.
3. Seleccione **Finalizar**.
4. Configure la aplicación mediante el archivo descargado de StorageGRID o los valores obtenidos manualmente.

Gestionar grupos de alta disponibilidad

¿Cuáles son los grupos de alta disponibilidad?

Los grupos de alta disponibilidad proporcionan conexiones de datos de alta disponibilidad para los clientes S3 y conexiones de alta disponibilidad a Grid Manager y al Gestor de inquilinos.

Puede agrupar las interfaces de red de varios nodos de administrador y puerta de enlace en un grupo de alta disponibilidad (ha). Si la interfaz activa del grupo de alta disponibilidad falla, una interfaz de backup puede administrar la carga de trabajo.

Cada grupo de alta disponibilidad proporciona acceso a los servicios compartidos en los nodos seleccionados.

- Los grupos de ALTA disponibilidad que incluyen nodos de puerta de enlace, nodos de administración o ambos proporcionan conexiones de datos de alta disponibilidad para clientes S3.
- Los grupos DE ALTA DISPONIBILIDAD que incluyen solo los nodos de administrador proporcionan conexiones de alta disponibilidad con el administrador de grid y el administrador de inquilinos.
- Un grupo de alta disponibilidad que incluya solo dispositivos de servicios y nodos de software basados en VMware puede proporcionar conexiones altamente disponibles para "Inquilinos de S3 que usan S3 Select". Se recomienda a los grupos de ALTA DISPONIBILIDAD cuando se usa S3 Select, pero no es obligatorio.

¿Cómo se crea un grupo de alta disponibilidad?

1. Debe seleccionar una interfaz de red para uno o más nodos de administrador o nodos de puerta de enlace. Puede usar una interfaz de red de cuadrícula (eth0), una interfaz de red de cliente (eth2), una interfaz VLAN o una interfaz de acceso que haya agregado al nodo.

   > ⓘ No puede agregar una interfaz a un grupo de alta disponibilidad si tiene una dirección IP asignada por DHCP.

2. Se especifica una interfaz para ser la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.
3. El orden de prioridad de las interfaces de copia de seguridad se determina.
4. Asigne una a 10 direcciones IP virtuales (VIP) al grupo. Las aplicaciones cliente pueden utilizar cualquiera de estas direcciones VIP para conectarse a StorageGRID.

Para obtener instrucciones, consulte "Configuración de grupos de alta disponibilidad".

¿Cuál es la interfaz activa?

Durante el funcionamiento normal, todas las direcciones VIP del grupo ha se añaden a la interfaz principal, que es la primera interfaz en el orden de prioridad. Siempre que la interfaz principal siga estando disponible, se utiliza cuando los clientes se conectan a cualquier dirección VIP del grupo. Es decir, durante el funcionamiento normal, la interfaz principal es la interfaz activa del grupo.

Del mismo modo, durante el funcionamiento normal, las interfaces de menor prioridad del grupo de alta disponibilidad actúan como interfaces de backup. Estas interfaces de copia de seguridad no se utilizan a menos que la interfaz primaria (actualmente activa) deje de estar disponible.

Ver el estado actual del grupo de alta disponibilidad de un nodo

Para ver si un nodo está asignado a un grupo de alta disponibilidad y determinar su estado actual, seleccione **Nodos** > ***nodo***.

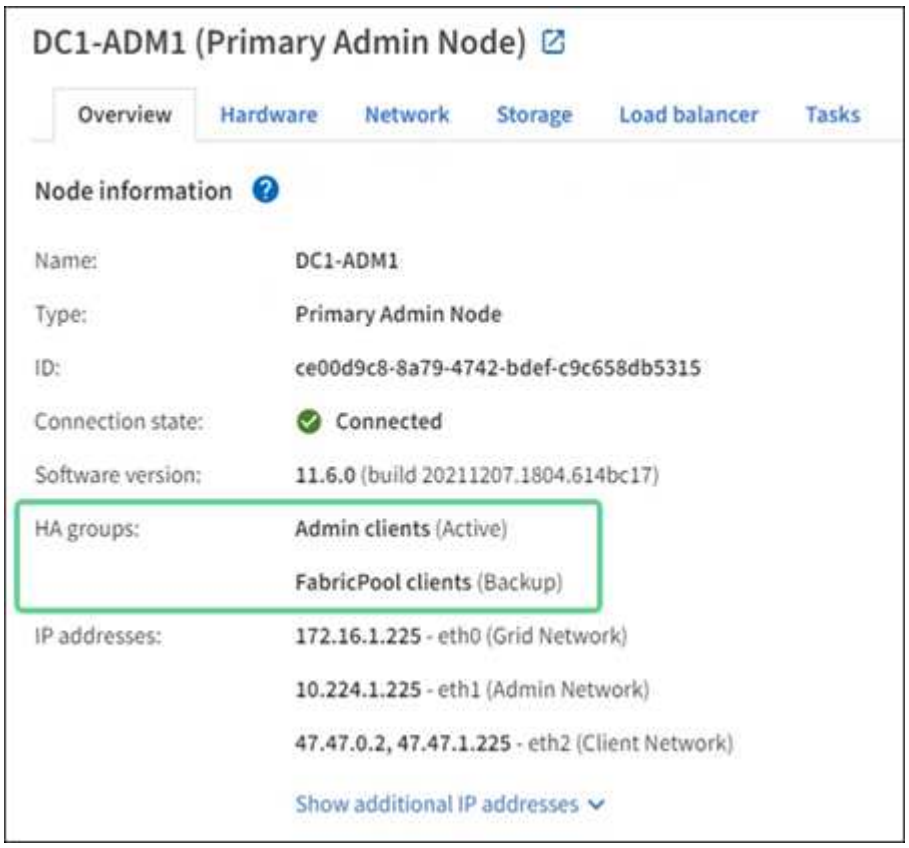
Si la ficha **Descripción general** incluye una entrada para **grupos ha**, el nodo se asigna a los grupos ha enumerados. El valor después de que el nombre del grupo sea el estado actual del nodo del grupo de alta disponibilidad:

- **Activo**: El grupo ha se está alojando actualmente en este nodo.
- **Copia de seguridad**: El grupo ha no está utilizando actualmente este nodo; se trata de una interfaz de copia de seguridad.
- **Detenido**: El grupo HA no se puede alojar en este nodo porque el servicio High Availability (Keepalived)

se ha detenido manualmente.

- **Fallo**: El grupo HA no se puede alojar en este nodo debido a uno o más de los siguientes:
  - El servicio Load Balancer (nginx-gw) no se está ejecutando en el nodo.
  - La interfaz eth0 o VIP del nodo está inactiva.
  - El nodo está inactivo.

En este ejemplo, el nodo de administración principal se ha añadido a dos grupos de alta disponibilidad. Este nodo es actualmente la interfaz activa del grupo de clientes de administración y una interfaz de respaldo del grupo de clientes de FabricPool.



¿Qué ocurre cuando falla la interfaz activa?

La interfaz que aloja actualmente las direcciones VIP es la interfaz activa. Si el grupo ha incluye más de una interfaz y la interfaz activa falla, las direcciones VIP se mueven a la primera interfaz de respaldo disponible en el orden de prioridad. Si falla esa interfaz, las direcciones VIP se mueven a la siguiente interfaz de respaldo disponible, etc.

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, los servicios para Grid Manager o el Gestor de inquilinos no activan la conmutación por error.

Por lo general, el proceso de recuperación tras fallos sólo 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.

Cuando se resuelve un fallo y hay una interfaz de mayor prioridad disponible de nuevo, las direcciones VIP se mueven automáticamente a la interfaz de mayor prioridad disponible.

¿Cómo se utilizan los grupos de alta disponibilidad?

Puede usar grupos de alta disponibilidad para proporcionar conexiones de alta disponibilidad a StorageGRID para datos de objetos y para uso administrativo.

- 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 a los clientes S3.
- 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 Gateway*: Incluye el servicio de Equilibrador de Carga.

Objetivo del grupo de alta disponibilidad	Añada nodos de este tipo al grupo de alta disponibilidad
Acceso a Grid Manager	• Nodo de administración principal (**primario**) • Nodos de administrador no primario **Nota:** el nodo de administración principal debe ser la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.
Acceso solo al administrador de inquilinos	• Nodos de administrador primario o no primario
Acceso de cliente S3 - Servicio Load Balancer	• Nodos de administración • Nodos de puerta de enlace

Objetivo del grupo de alta disponibilidad	Añada nodos de este tipo al grupo de alta disponibilidad
Acceso de clientes S3 para "S3 Select"	• Dispositivos de servicios • Nodos de software basados en VMware **Nota**: Se recomiendan los grupos DE HA cuando se usa S3 Select, pero no es necesario.

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

Si falla un servicio de Grid Manager o de arrendatario Manager, no se activa la conmutación por error del grupo de alta disponibilidad.

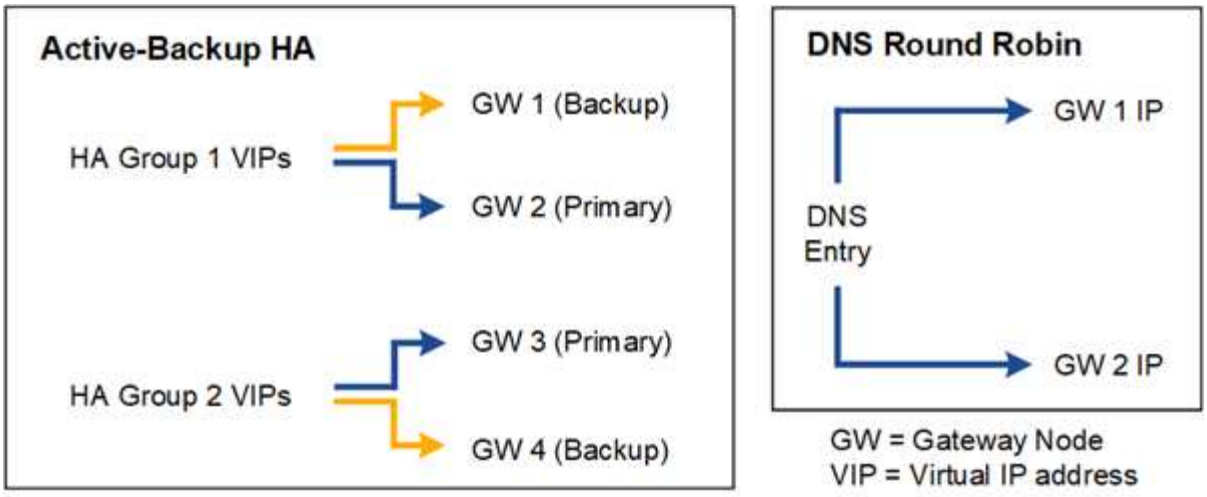
Si ha iniciado sesión en Grid Manager o en el arrendatario Manager cuando se produce la conmutación por error, ha cerrado sesión y debe volver a iniciar sesión para reanudar la tarea.

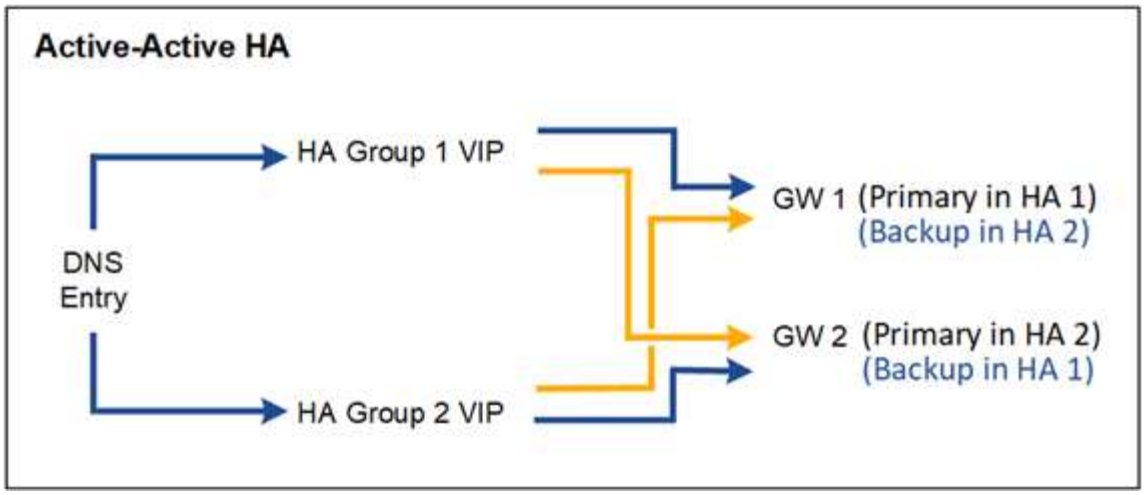
Algunos procedimientos de mantenimiento no se pueden realizar cuando el nodo de administración principal no está disponible. Durante la conmutación por error, puede utilizar Grid Manager para supervisar el sistema StorageGRID.

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.

En los diagramas, el azul indica la interfaz primaria del grupo de alta disponibilidad y el amarillo indica la interfaz de backup del grupo de alta disponibilidad.





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	• Gestionada por StorageGRID sin dependencias externas. • Rápida recuperación tras fallos.	• Solo un nodo de un grupo de alta disponibilidad está activo. Al menos un nodo por grupo de alta disponibilidad estará inactivo.
Operación por turnos DNS	• Mayor rendimiento total. • Sin hosts inactivos.	• 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.

Configuración	Ventajas	Desventajas
Alta disponibilidad activo-activo	• 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.	• Más complejo de configurar. • Requiere la configuración del hardware fuera de StorageGRID. • Necesita una comprobación del estado implementada por el cliente.

Configuración de grupos de alta disponibilidad

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

Un sistema StorageGRID puede tener un máximo de 255 grupos HA.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".
- Si piensa utilizar una interfaz VLAN en un grupo de alta disponibilidad, ha creado la interfaz VLAN. Consulte "Configure las interfaces VLAN".
- Si planea utilizar una interfaz de acceso para un nodo en un grupo de alta disponibilidad, ha creado la interfaz:
  - **Linux (antes de instalar el nodo)**:"Crear archivos de configuración del nodo"
  - **Linux (después de instalar el nodo)**:"Agregar interfaces troncales o de acceso a un nodo"
  - **VMware (después de instalar el nodo)**:"Agregar interfaces troncales o de acceso a un nodo"

"Linux" se refiere a una implementación de RHEL, Ubuntu o Debian. Para obtener una lista de las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp (IMT)" .

Crear un grupo de alta disponibilidad

Cuando crea un grupo de alta disponibilidad, selecciona una o varias interfaces y las organiza por orden de prioridad. A continuación, debe asignar una o varias direcciones VIP al grupo.

Una interfaz debe ser para que un nodo de puerta de enlace o un nodo de administrador se incluyan en un grupo de alta disponibilidad. Un grupo de alta disponibilidad solo puede usar una interfaz para cualquier nodo concreto; sin embargo, se pueden usar otras interfaces para el mismo nodo en otros grupos de alta disponibilidad.

Acceda al asistente

Pasos

1. Seleccione **Configuración** > **Red** > **Grupos de alta disponibilidad**.
2. Seleccione **Crear**.

Introduzca los detalles del grupo de alta disponibilidad

Pasos

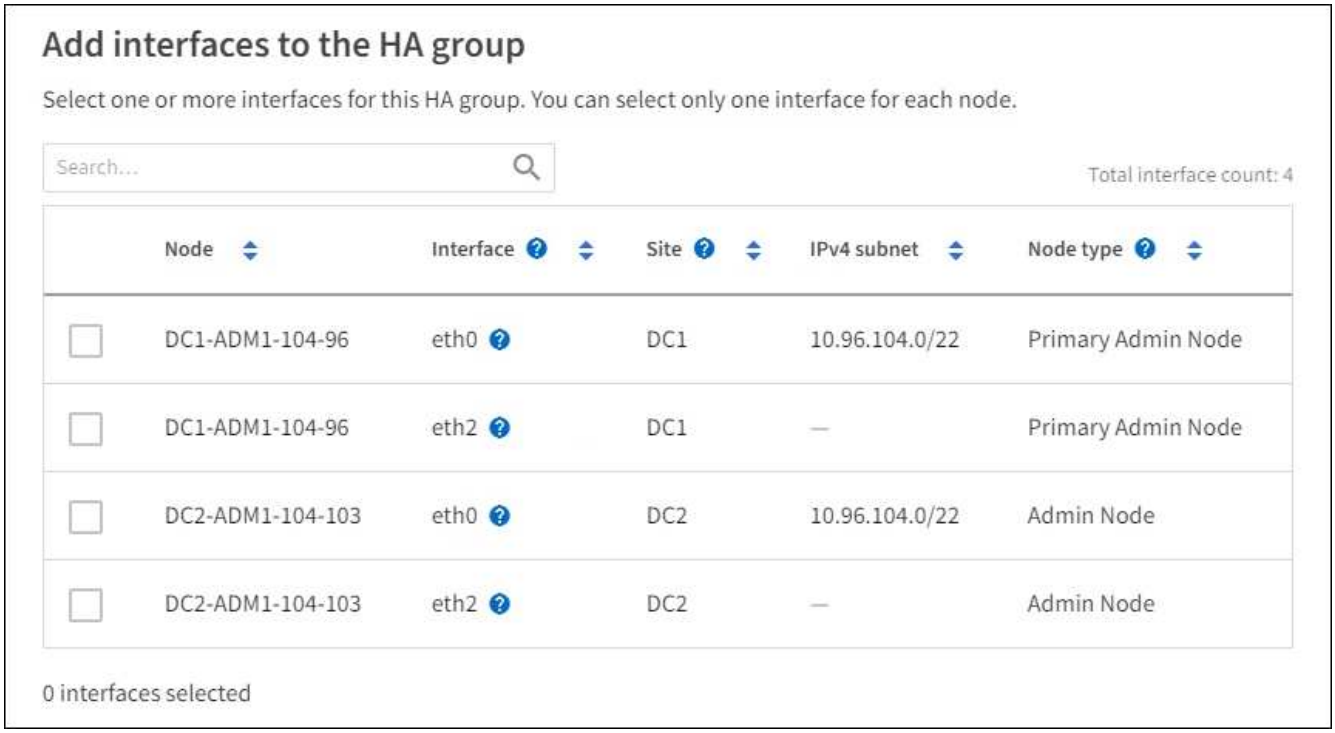
1. Proporcione un nombre único para el grupo de alta disponibilidad.
2. De forma opcional, puede introducir una descripción para el grupo de alta disponibilidad.
3. Seleccione **continuar**.

Añada interfaces al grupo de alta disponibilidad

Pasos

1. Seleccione una o varias interfaces para añadirlas a este grupo de alta disponibilidad.

   Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.



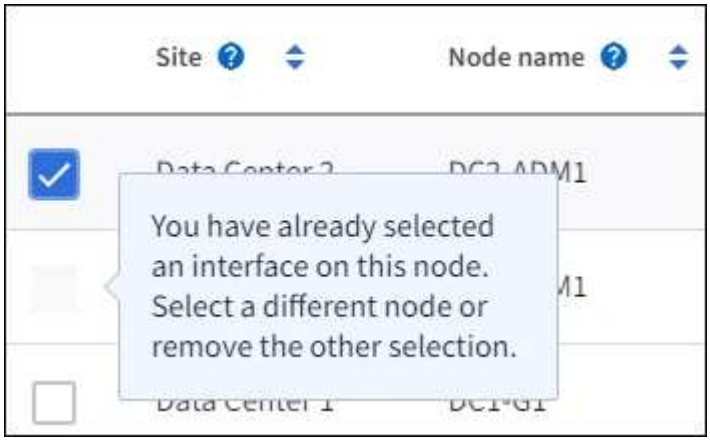
   Después de crear una interfaz VLAN, espere hasta 5 minutos para que la nueva interfaz aparezca en la tabla.

Directrices para seleccionar interfaces

- Debe seleccionar al menos una interfaz.
- Solo puede seleccionar una interfaz para un nodo.
- Si el grupo ha es para la protección de alta disponibilidad de los servicios Admin Node, que incluyen Grid Manager y el inquilino Manager, seleccione interfaces sólo en nodos de administrador.
- Si el grupo de alta disponibilidad está destinado a la protección de alta disponibilidad del tráfico de cliente S3, seleccione interfaces en los nodos de administración, nodos de puerta de enlace o ambos.
- Si selecciona interfaces en diferentes tipos de nodos, aparece una nota informativa. Se le recuerda que si se produce una conmutación al respaldo, los servicios que proporciona el nodo que antes estaba activo podrían no estar disponibles en el nodo recién activo. Por ejemplo, un nodo de puerta de enlace de backup no puede ofrecer una protección de alta disponibilidad de los servicios de nodo de

administración. Del mismo modo, un nodo de administración de copia de seguridad no puede realizar todos los procedimientos de mantenimiento que puede proporcionar el nodo de administración primario.

- Si no puede seleccionar una interfaz, su casilla de verificación está desactivada. La sugerencia de herramienta proporciona más información.



- No puede seleccionar una interfaz si su valor de subred o puerta de enlace entra en conflicto con otra interfaz seleccionada.
- No puede seleccionar una interfaz configurada si no tiene una dirección IP estática.

2. Seleccione **continuar**.

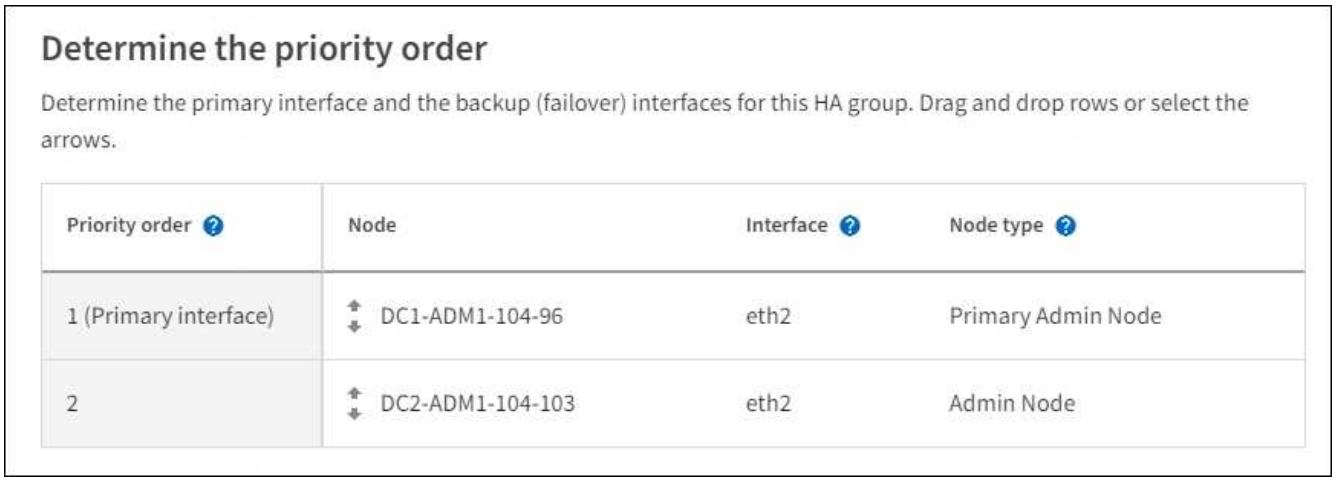
Determinar el orden de prioridad

Si el grupo HA incluye más de una interfaz, puede determinar cuál es la interfaz principal y cuáles son las interfaces de backup (failover). Si la interfaz principal falla, las direcciones VIP se mueven a la interfaz de mayor prioridad que está disponible. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de mayor prioridad que esté disponible, etc.

Pasos

1. Arrastre filas en la columna **Orden de prioridad** para determinar la interfaz principal y cualquier interfaz de respaldo.

   La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.



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

2. Seleccione **continuar**.

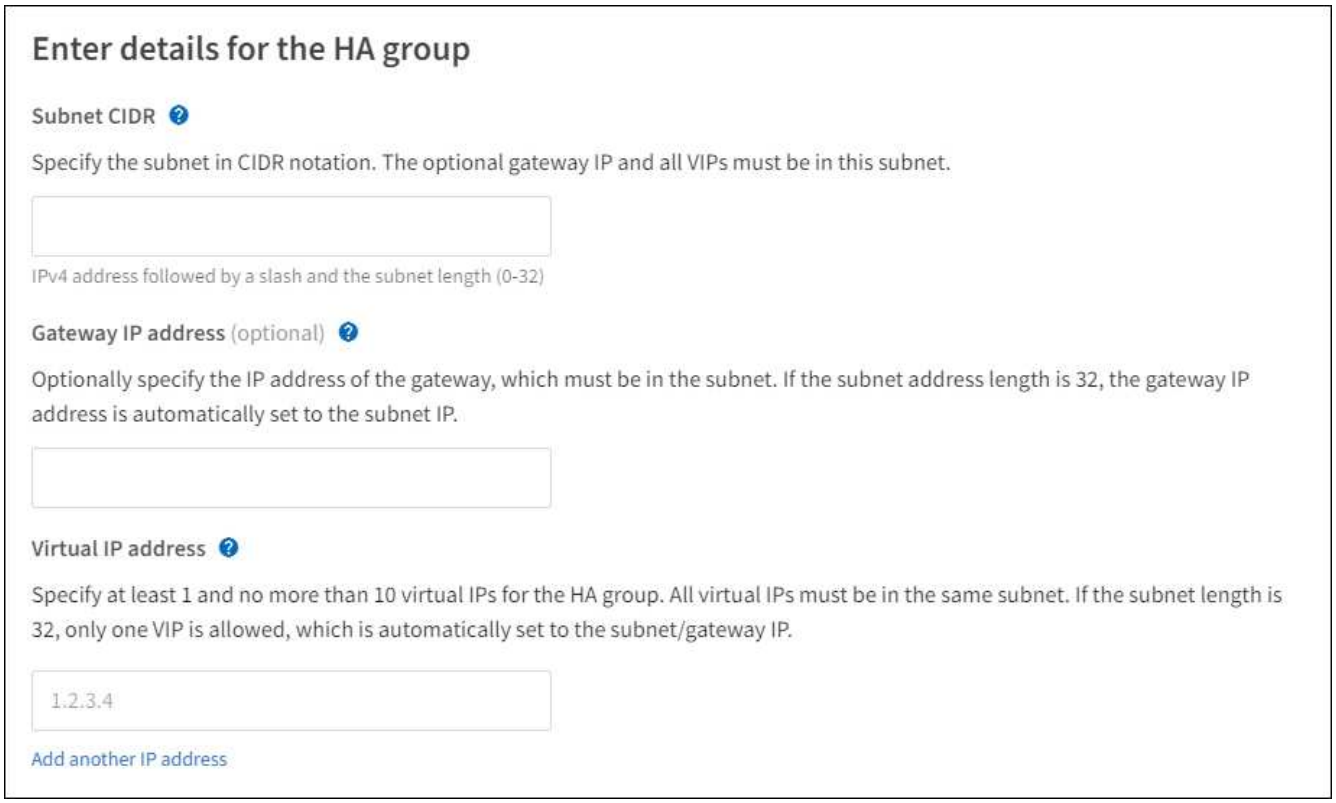
Introduzca las direcciones IP

Pasos

1. En el campo **CIDR de subred**, especifique la subred VIP en notación CIDR --una dirección IPv4 seguida de una barra y la longitud de subred (0-32).

   La dirección de red no debe tener ningún bit de host configurado. Por ejemplo, `192.16.0.0/22`.

   Si utiliza un prefijo de 32 bits, la dirección de red VIP también funciona como dirección de puerta de enlace y dirección VIP.



2. Opcionalmente, si cualquier cliente administrativo o inquilino de S3 accederá a estas direcciones VIP desde una subred diferente, introduzca la dirección IP de la puerta de enlace *. La dirección de la puerta de enlace debe estar en la subred VIP.

   Los usuarios de cliente y administrador utilizarán esta puerta de enlace para acceder a las direcciones IP virtuales.

3. Introduzca al menos una y como máximo diez direcciones VIP para la interfaz activa en el grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa.

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

IPv4 e IPv6 adicionales.

4. Seleccione **Crear grupo ha** y seleccione **Finalizar**.

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

Siguientes pasos

Si utilizará este grupo de ha para el equilibrio de carga, cree un extremo de equilibrio de carga para determinar el puerto y el protocolo de red y para conectar los certificados necesarios. Consulte "Configurar puntos finales del equilibrador de carga".

Editar un grupo de alta disponibilidad

Puede editar un grupo de alta disponibilidad para cambiar su nombre y descripción, agregar o quitar interfaces, cambiar el orden de prioridad o agregar o actualizar direcciones IP virtuales.

Por ejemplo, es posible que deba editar un grupo de alta disponibilidad si desea quitar el nodo asociado a una interfaz seleccionada en un procedimiento de retirada del sitio o nodo.

Pasos

1. Seleccione **Configuración** > **Red** > **Grupos de alta disponibilidad**.

   La página grupos de alta disponibilidad muestra todos los grupos de alta disponibilidad existentes.

2. Seleccione la casilla de comprobación del grupo de alta disponibilidad que desea editar.
3. Realice una de las siguientes acciones, según lo que desee actualizar:
   - Seleccione **acciones** > **Editar dirección IP virtual** para agregar o eliminar direcciones VIP.
   - Seleccione **acciones** > **Editar grupo ha** para actualizar el nombre o la descripción del grupo, agregar o quitar interfaces, cambiar el orden de prioridad o agregar o quitar direcciones VIP.
4. Si ha seleccionado **Editar dirección IP virtual**:
   a. Actualice las direcciones IP virtuales del grupo de alta disponibilidad.
   b. Seleccione **Guardar**.
   c. Seleccione **Finalizar**.
5. Si ha seleccionado **Editar grupo ha**:
   a. Si lo desea, actualice el nombre o la descripción del grupo.
   b. Opcionalmente, seleccione o desactive las casillas de verificación para agregar o eliminar interfaces.

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

   c. Opcionalmente, arrastre Filas para cambiar el orden de prioridad de la interfaz principal y cualquier interfaz de backup de este grupo de alta disponibilidad.
   d. De manera opcional, actualice las direcciones IP virtuales.
   e. Seleccione **Guardar** y, a continuación, seleccione **Finalizar**.

Eliminar un grupo de alta disponibilidad

Puede eliminar uno o varios grupos de alta disponibilidad al mismo tiempo.

> No puede eliminar un grupo de alta disponibilidad si está vinculado a un extremo de equilibrador de carga. Para eliminar un grupo de alta disponibilidad, debe eliminarlo de los extremos de equilibrio de carga que lo utilicen.

Para evitar interrupciones en el cliente, actualice las aplicaciones cliente S3 afectadas antes de eliminar 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.

Pasos

1. Seleccione **Configuración** > **Red** > **Grupos de alta disponibilidad**.
2. Revise la columna **Load Balancer Endpoints** para cada grupo HA que desee eliminar. Si se muestra algún punto final del equilibrador de carga:
   a. Vaya a **Configuración** > **Red** > **Puntos finales del balanceador de carga**.
   b. Seleccione la casilla de verificación para el punto final.
   c. Seleccione **acciones** > **Editar modo de enlace de punto final**.
   d. Actualice el modo de enlace para eliminar el grupo HA.
   e. Seleccione **Guardar cambios**.
3. Si no aparece ningún punto final del equilibrador de carga, seleccione la casilla de verificación de cada grupo de alta disponibilidad que desee quitar.
4. Selecciona **Acciones** > **Eliminar grupo HA**.
5. Revise el mensaje y seleccione **Eliminar grupo ha** para confirmar su selección.

   Se eliminan todos los grupos de alta disponibilidad seleccionados. Aparecerá un banner verde de éxito en la página grupos de alta disponibilidad.

Gestione el equilibrio de carga

Consideraciones que tener en cuenta al equilibrio de carga

Es posible utilizar el balanceo de carga para manejar cargas de trabajo de procesamiento y recuperación de clientes S3.

¿Qué es el equilibrio de carga?

Cuando una aplicación cliente guarda o recupera datos de un sistema StorageGRID, StorageGRID utiliza un balanceador de carga para gestionar la carga de trabajo de ingesta y recuperación. El equilibrio de carga maximiza la velocidad y la capacidad de conexión mediante la distribución de la carga de trabajo entre varios nodos de almacenamiento.

El servicio de equilibrador de carga de StorageGRID se instala en todos los nodos de administrador y en todos los nodos de puerta de enlace, y ofrece balanceo de carga de capa 7. Realiza la terminación de las solicitudes de cliente de Seguridad de capa de transporte (TLS), inspecciona las solicitudes y establece nuevas conexiones seguras a los nodos de almacenamiento.

El servicio Load Balancer de cada nodo funciona de forma independiente cuando se reenvía tráfico de clientes 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.

> Si bien el servicio StorageGRID Load Balancer es el mecanismo de equilibrio de carga recomendado, es posible que desees integrar un equilibrador de carga de terceros. Para obtener más información, comuníquese con su representante de cuenta de NetApp o consulte "Utilice balanceadores de carga de terceros con StorageGRID".

¿Cuántos nodos de equilibrio de carga se necesitan?

Como práctica recomendada general, cada sitio del sistema StorageGRID debe incluir dos o más nodos con el servicio de equilibrador de carga. Por ejemplo, un sitio puede incluir dos nodos de puerta de enlace, o bien un nodo de administrador y un nodo de puerta de enlace. Asegúrese de que haya una infraestructura de red, hardware o virtualización adecuada para cada nodo de equilibrio de carga, ya sea que utilice dispositivos de servicios, nodos de configuración básica o nodos basados en máquinas virtuales (VM).

¿Qué es un extremo de equilibrador de carga?

Un punto final de equilibrio de carga define el puerto y el protocolo de red (HTTPS o HTTP) que utilizarán las solicitudes de aplicación cliente entrantes y salientes para acceder a los nodos que contienen el servicio de equilibrio de carga. El extremo también define el tipo de cliente (S3), el modo de enlace y, opcionalmente, una lista de inquilinos permitidos o bloqueados.

Para crear un punto final de balanceador de carga, utilice el Administrador de cuadrícula o complete los asistentes de configuración de S3 y FabricPool :

- "Configurar puntos finales del equilibrador de carga"
- "Use el asistente de configuración de S3"
- "Use el asistente de configuración de FabricPool"

Consideraciones para el almacenamiento en caché del balanceador de carga

El almacenamiento en caché mejora significativamente el rendimiento cuando una carga de trabajo opera en un subconjunto de datos y accede a los objetos varias veces. Además, el almacenamiento en caché proporciona acceso remoto al almacenamiento de objetos sin una implementación de red completa. El almacenamiento en caché del equilibrador de carga solo está disponible para los nodos de puerta de enlace.

A medida que crea puntos finales del balanceador de carga:

- Habilite el almacenamiento en caché solo para cargas de trabajo que se puedan almacenar en caché. Las cargas de trabajo que acceden a datos no almacenados en caché con mayor frecuencia que a datos almacenados en caché tendrán un peor rendimiento que si la caché no los hubiera atendido. En algunos casos, las cargas de trabajo con altas tasas de sobrescritura y desalojo también pueden exceder la resistencia de escritura de la unidad garantizada.
- Considere agregar puntos finales o nodos adicionales para almacenar en caché cargas de trabajo individuales que sean buenos candidatos para el almacenamiento en caché.
- Utilice puntos finales distintos para cargas de trabajo almacenables en caché y no almacenables en caché. Esta separación garantiza que los mecanismos de almacenamiento en caché se apliquen de forma adecuada y no interfieran con el procesamiento de datos no almacenables en caché.
- Evalúe una carga de trabajo potencialmente almacenable en caché dirigiéndola al punto final habilitado para caché. Supervisar y verificar la tasa de aciertos de caché para determinar la idoneidad de la carga de

trabajo para el almacenamiento en caché. Esta evaluación ayuda a optimizar el rendimiento y garantizar el uso eficiente de los recursos de caché.

- "Revisar los registros de auditoría"para determinar si una carga de trabajo existente sería un buen candidato para el almacenamiento en caché. Para un período de tiempo determinado, determine qué porcentaje de GET son para objetos únicos. Para que sea adecuado para el almacenamiento en caché, este valor debe ser inferior al 50%.

Ejemplos de cargas de trabajo que podrían ser buenos candidatos para el almacenamiento en caché

- Lagos de datos
- Computación de alto rendimiento (HPC)
- Entrenamiento de IA/ML
- Redes de distribución de contenido (CDN)
- Gestión de activos multimedia
- Producción de vídeo

- Se pueden almacenar en caché múltiples versiones de objetos.
- Se admiten operaciones de lectura de rango.

Ejemplos de cargas de trabajo que no son buenos candidatos para el almacenamiento en caché

- Piscina de telas
- Aplicaciones de respaldo
- Nivelación de almacenamiento

Si algún contenido que se va a servir mediante la caché requiere cifrado en reposo, "habilitar el cifrado de nodo o unidad" en el nodo de caché.

Tipos de objetos y solicitudes que no se almacenarán en caché

- El `response-content-encoding` parámetro de consulta
- El `partNumber` parámetro de consulta
- Encabezados condicionales
  - `If-Match`
  - `If-Modified-Since`
  - `If-None-Match`
  - `If-Unmodified-Since`
- Solicitudes que se cifraron en reposo con cualquiera de los siguientes:
  - SSE (cifrado del lado del servidor con claves administradas por StorageGRID)
  - SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente)
  - Cifrado de objetos almacenados

Cualquier solicitud que no esté almacenada en caché se reenvía a un LDR ascendente como si el caché no estuviera habilitado.

Información relacionada

- "Solucionar problemas de almacenamiento en caché del balanceador de carga"
- Para obtener más información sobre el almacenamiento en caché del equilibrador de carga, comuníquese con el soporte técnico.

Consideraciones para el puerto

El puerto para un punto final de equilibrio de carga es por defecto 10433 para el primer punto final que cree, pero puede especificar cualquier puerto externo no utilizado entre 1 y 65535. Si utiliza el puerto 80 o 443, el punto final utilizará el servicio Equilibrador de Carga sólo en los nodos de Gateway. Estos puertos están reservados en los nodos de administrador. Si utiliza el mismo puerto para más de un punto final, debe especificar un modo de enlace diferente para cada punto final.

No se permiten puertos utilizados por otros servicios de la red. Ver "Puertos internos StorageGRID" .

Consideraciones para el protocolo de red

En la mayoría de los casos, las conexiones entre las aplicaciones cliente y StorageGRID deben utilizar el cifrado de seguridad de la capa de transporte (TLS). Aunque no se recomienda la conexión a StorageGRID sin cifrado TLS, especialmente en entornos de producción. Al seleccionar el protocolo de red para el punto final del equilibrador de carga StorageGRID, debe seleccionar **HTTPS**.

Consideraciones sobre los certificados de punto final del equilibrador de carga

Si selecciona **HTTPS** como protocolo de red para el punto final del equilibrador de carga, debe proporcionar un certificado de seguridad. Puede utilizar cualquiera de estas tres opciones al crear el punto final del equilibrador de carga:

- **Sube un certificado firmado (recomendado)**. Este certificado puede estar firmado por una entidad de certificación (CA) de confianza pública o una entidad de certificación (CA) privada. El uso de un certificado de servidor de CA de confianza pública para proteger la conexión es la práctica recomendada. A diferencia de los certificados generados, los certificados firmados por una CA pueden rotarse de forma no disruptiva, lo que puede ayudar a evitar problemas de caducidad.

  Debe obtener los siguientes archivos antes de crear el punto final del equilibrador de carga:

  - El archivo de certificado del servidor personalizado.
  - El archivo de claves privadas del certificado de servidor personalizado.
  - De manera opcional, un paquete de CA de los certificados de cada entidad emisora intermedia.
- **Generar un certificado autofirmado**.
- **Utilice el certificado global StorageGRID S3**. Debe cargar o generar una versión personalizada de este certificado antes de poder seleccionarlo para el punto final del equilibrador de carga. Consulte "Configure los certificados de API S3".

¿Qué valores necesito?

Para crear el certificado, debe conocer todos los nombres de dominio y direcciones IP que utilizarán las aplicaciones cliente S3 para acceder al punto final.

La entrada **Subject DN** (Nombre Distinguido) para el certificado debe incluir el nombre de dominio completo que la aplicación cliente utilizará para StorageGRID. Por ejemplo:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Según sea necesario, el certificado puede utilizar comodines para representar los nombres de dominio totalmente cualificados de todos los nodos de administración y nodos de gateway que ejecutan el servicio de equilibrio de carga. Por ejemplo, `*.storagegrid.example.com` utiliza el comodín * para representar `adm1.storagegrid.example.com` y `gn1.storagegrid.example.com`.

Si planea utilizar S3 solicitudes virtuales de estilo hospedado, el certificado también debe incluir una entrada de **Nombre Alternativo** para cada una de las "Nombre de dominio de punto final S3" que haya configurado, incluidos los nombres comodín. Por ejemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> ⓘ Si utiliza comodines para los nombres de dominio, revise el "Directrices de refuerzo para certificados de servidor".

También debe definir una entrada DNS para cada nombre en el certificado de seguridad.

¿Cómo se gestionan los certificados que caducan?

> ⚠ Si el certificado utilizado para proteger la conexión entre la aplicación S3 y StorageGRID caduca, la aplicación podría perder temporalmente el acceso a StorageGRID.

Para evitar problemas de caducidad de certificados, siga las siguientes prácticas recomendadas:

- Monitoree cuidadosamente cualquier alerta que advierta de fechas de vencimiento de certificados que se acercan, como el **Caducidad del certificado de punto final del equilibrador de carga** y **Caducidad del certificado de servidor global para las alertas de S3 API**.
- Mantenga siempre sincronizadas las versiones del certificado de la aplicación StorageGRID y S3. Si reemplaza o renueva el certificado utilizado para un punto final de equilibrio de carga, debe reemplazar o renovar el certificado equivalente utilizado por la aplicación S3.
- Utilice un certificado de CA firmado públicamente. Si utiliza un certificado firmado por una CA, puede sustituir certificados próximos a caducar de forma no disruptiva.
- Si generó un certificado StorageGRID autofirmado y ese certificado está a punto de caducar, debe reemplazar manualmente el certificado tanto en StorageGRID como en la aplicación S3 antes de que caduque el certificado existente.

Consideraciones sobre el modo de enlace

El modo de enlace le permite controlar qué direcciones IP se pueden utilizar para acceder a un punto final de equilibrio de carga. Si un punto final utiliza un modo de enlace, las aplicaciones cliente solo pueden acceder al punto final si utilizan una dirección IP permitida o su nombre de dominio completo (FQDN) correspondiente. Las aplicaciones cliente que utilizan cualquier otra dirección IP o FQDN no pueden acceder al punto final.

Puede especificar cualquiera de los siguientes modos de enlace:

- **Global** (por defecto): Las aplicaciones cliente pueden acceder al punto final utilizando la dirección IP de

cualquier Nodo de Gateway o Nodo de Administración, la dirección IP virtual (VIP) de cualquier grupo HA en cualquier red, o un FQDN correspondiente. Utilice esta configuración a menos que necesite restringir la accesibilidad de un punto final.

- **IPs virtuales de grupos HA**. Las aplicaciones cliente deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad.
- **Interfaces de nodo**. Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas.
- **Tipo de nodo**. En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace.

Consideraciones para el acceso de inquilinos

El acceso de inquilino es una función de seguridad opcional que le permite controlar qué cuentas de inquilino de StorageGRID pueden usar un extremo de equilibrador de carga para acceder a sus buckets. Puede permitir que todos los inquilinos accedan a un punto final (valor predeterminado) o puede especificar una lista de los inquilinos permitidos o bloqueados para cada punto final.

Puede utilizar esta función para proporcionar un mejor aislamiento de seguridad entre los inquilinos y sus extremos. Por ejemplo, puede utilizar esta función para asegurarse de que los materiales de alto secreto o altamente clasificados propiedad de un arrendatario permanezcan completamente inaccesibles para otros arrendatarios.

> Para fines de control de acceso, el inquilino se determina a partir de las claves de acceso utilizadas en la solicitud del cliente, si no se proporcionan claves de acceso como parte de la solicitud (como con acceso anónimo), el propietario del depósito se utiliza para determinar el inquilino.

Ejemplo de acceso de inquilinos

Para entender cómo funciona esta característica de seguridad, considere el siguiente ejemplo:

1. Ha creado dos puntos finales de equilibrio de carga, de la siguiente manera:
   - **Punto final público**: Utiliza el puerto 10443 y permite el acceso a todos los inquilinos.
   - **Top SECRET** punto final: Utiliza el puerto 10444 y permite el acceso al inquilino **Top SECRET** solamente. Todos los demás inquilinos tienen bloqueado el acceso a este punto final.
2. El `top-secret.pdf` está en un cubo propiedad del inquilino **Top secret**.

Para acceder a `top-secret.pdf` , un usuario del inquilino **Top secret** puede enviar una solicitud GET a `https://w.x.y.z:10444/top-secret.pdf`. Como este inquilino puede usar el extremo 10444, el usuario puede acceder al objeto. Sin embargo, si un usuario que pertenece a cualquier otro arrendatario emite la misma solicitud a la misma URL, recibe un mensaje de acceso denegado inmediato. Se deniega el acceso aunque las credenciales y la firma sean válidas.

Disponibilidad de CPU

El servicio Load Balancer en cada nodo de administración y nodo de pasarela funciona de forma independiente cuando se reenvía tráfico S3 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.

Configurar puntos finales del equilibrador de carga

Los extremos del equilibrador de carga determinan los puertos y protocolos de red que los clientes S3 pueden utilizar al conectarse al equilibrador de carga de StorageGRID en los nodos de gateway y admin. También puede utilizar puntos finales para acceder a Grid Manager, Tenant Manager o ambos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".
- Ha revisado el "consideraciones que tener en cuenta al equilibrio de carga".
- Si ha reasignado anteriormente un puerto que desea utilizar para el punto final del equilibrador de carga, tiene "se ha eliminado el mapa de puertos".
- Ha creado cualquier grupo de alta disponibilidad que desee utilizar. Se recomiendan los grupos de ALTA DISPONIBILIDAD, pero no es obligatorio. Consulte "Gestión de grupos de alta disponibilidad".
- Si va a utilizar el punto final del equilibrador de carga "Inquilinos de S3 para S3 Select", no debe utilizar las direcciones IP ni los FQDN de ningún nodo bare-metal. Solo se permiten dispositivos de servicios y nodos de software basados en VMware para los extremos del equilibrador de carga utilizados para S3 Select.
- Ha configurado las interfaces VLAN que desea utilizar. Consulte "Configure las interfaces VLAN".
- Si crea un extremo de HTTPS (recomendado), tiene la información del certificado de servidor.

> ⓘ Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

  - Para cargar un certificado, necesita el certificado de servidor, la clave privada de certificado y, opcionalmente, un bundle de CA.
  - Para generar un certificado, se necesitan todos los nombres de dominio y las direcciones IP que utilizarán los clientes S3 para acceder al punto final. También debe conocer el asunto (nombre distintivo).
  - Si desea usar el certificado de API de StorageGRID S3 (que también puede utilizarse para conexiones directamente a nodos de almacenamiento), ya sustituyó el certificado predeterminado por un certificado personalizado firmado por una entidad de certificación externa. Consulte "Configure los certificados de API S3".

Cree un extremo de equilibrador de carga

Cada punto final del balanceador de carga del cliente S3 especifica un puerto, un tipo de cliente (S3) y un protocolo de red (HTTP o HTTPS). Los puntos finales del balanceador de carga de la interfaz de administración especifican un puerto, un tipo de interfaz y una red de cliente no confiable.

Acceda al asistente

Pasos

1. Seleccione **Configuración** > **Red** > **Puntos finales del balanceador de carga**.
2. Para crear un punto final para un cliente S3, seleccione la pestaña **Cliente S3**.
3. Para crear un punto final para acceder a Grid Manager, Tenant Manager o ambos, seleccione la pestaña **Interfaz de administración**.
4. Seleccione **Crear**.

Introduzca los detalles de los extremos

Pasos

1. Seleccione las instrucciones adecuadas para introducir los detalles del tipo de punto final que desea crear.

Cliente S3

Campo	Descripción
Nombre	Nombre descriptivo para el punto final, que aparecerá en la tabla de la página Load equilibrer Endpoints.
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. Este campo se establece por defecto en 10433 para el primer punto final que cree, pero puede introducir cualquier puerto externo no utilizado de 1 a 65535. Si ingresa **80** o **8443**, el punto final se configura solo en los nodos de Gateway, a menos que haya liberado el puerto 8443. A continuación, puede utilizar el puerto 8443 como punto final S3 y el puerto se configurará en los nodos Gateway y Admin.
Tipo de cliente	Debe ser **S3**.
Protocolo de red	El protocolo de red que utilizarán los clientes al conectarse a este extremo. • Seleccione **HTTPS** para una comunicación segura cifrada con TLS (recomendado). Debe asociar un certificado de seguridad para poder guardar el extremo. • Seleccione **HTTP** para una comunicación no cifrada y menos segura. Utilice HTTP sólo para una cuadrícula que no sea de producción.
Habilitar el almacenamiento en caché	Habilitar o deshabilitar"almacenamiento en caché en los nodos de puerta de enlace" para este punto final del balanceador de carga. Si surgen problemas con el almacenamiento en caché, consulte"Solucionar problemas de almacenamiento en caché del balanceador de carga" .

Interfaz de gestión

Campo	Descripción
Nombre	Nombre descriptivo para el punto final, que aparecerá en la tabla de la página Load equilibrer Endpoints.
Puerto	El puerto StorageGRID que desea utilizar para acceder al Administrador de grid, el Administrador de inquilinos o ambos. • Grid Manager: **8443** • Administrador de Inquilinos: **9443** • Tanto Grid Manager como Tenant Manager: **443** **Nota**: Puede utilizar estos puertos preestablecidos u otros puertos disponibles.

Campo	Descripción
Tipo de interfaz	Seleccione el botón de opción de la interfaz StorageGRID a la que accederá desde este punto final.
Red cliente no confiable	Seleccione **Sí** si este punto final debe ser accesible para las redes de clientes que no sean de confianza. De lo contrario, seleccione **No**. Cuando selecciona **Sí**, el puerto está abierto en todas las redes cliente que no sean de confianza. **Nota**: Solo puede configurar un puerto para que esté abierto o cerrado a las redes de clientes que no sean de confianza al crear el punto final del equilibrador de carga.

1. Seleccione **continuar**.

Seleccione un modo de enlace

Pasos

1. Seleccione un modo de enlace para el punto final para controlar cómo se accede al punto final mediante cualquier dirección IP o mediante direcciones IP e interfaces de red específicas.

   Algunos modos de vinculación están disponibles para extremos de cliente o para extremos de interfaz de gestión. Aquí se enumeran todos los modos para ambos tipos de punto final.

Modo	Descripción
Global (por defecto para puntos finales de cliente)	Los clientes pueden acceder al punto final mediante la dirección IP de cualquier nodo de gateway o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice la configuración **Global** a menos que necesite restringir la accesibilidad de este punto final.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad para acceder a este extremo. Los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que seleccione para los puntos finales no se superpongan.
Interfaces de nodos	Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo (solo extremos de cliente)	En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este extremo.

Modo	Descripción
Todos los nodos de administración (predeterminado para los extremos de la interfaz de gestión)	Los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración para acceder a este extremo.

Si más de un punto final utiliza el mismo puerto, StorageGRID utiliza este orden de prioridad para decidir qué punto final utilizar: **IP virtuales de grupos HA** > **Interfaces de nodo** > **Tipo de nodo** > **Global**.

Si va a crear extremos de la interfaz de gestión, solo se permiten los nodos de administrador.

2. Si ha seleccionado **IP virtuales de grupos ha**, seleccione uno o más grupos ha.

   Si va a crear extremos de interfaz de gestión, seleccione VIP asociadas sólo a nodos de administración.

3. Si ha seleccionado **interfaces de nodo**, seleccione una o más interfaces de nodo para cada nodo de administración o nodo de puerta de enlace que desee asociar con este extremo.
4. Si seleccionó **Tipo de nodo**, seleccione Nodos de administración, que incluye tanto el nodo de administración principal como cualquier nodo de administración no principal, o Nodos de puerta de enlace.

Controle el acceso de inquilinos

> Un punto final de la interfaz de gestión puede controlar el acceso de inquilino sólo cuando el punto final tiene el Tipo de interfaz de gestor de inquilinos.

Pasos

1. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir todos los inquilinos (predeterminado)	Todas las cuentas de inquilino pueden usar este extremo para acceder a sus bloques. Debe seleccionar esta opción si aún no ha creado ninguna cuenta de arrendatario. Después de agregar cuentas de arrendatario, puede editar el punto final del equilibrador de carga para permitir o bloquear cuentas específicas.
Permitir arrendatarios seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este extremo para acceder a sus bloques.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este punto final para acceder a sus bloques. Todos los demás inquilinos pueden usar este extremo.

2. Si está creando un punto final **HTTP**, no necesita adjuntar un certificado. Seleccione **Crear** para agregar el nuevo punto final del equilibrador de carga. A continuación, vaya a Después de terminar. De lo contrario, seleccione **continuar** para adjuntar el certificado.

Adjunte el certificado

Pasos

1. Si está creando un extremo **HTTPS**, seleccione el tipo de certificado de seguridad que desea asociar al extremo.

   El certificado protege las conexiones entre los clientes S3 y el servicio Load Balancer en los nodos de administración o Gateway.

   - **Cargar certificado**. Seleccione esta opción si tiene certificados personalizados para cargar.
   - **Generar certificado**. Seleccione esta opción si tiene los valores necesarios para generar un certificado personalizado.
   - **Utilice el certificado StorageGRID S3**. Seleccione esta opción si desea usar el certificado API global de S3, que también se puede utilizar para conexiones directamente a nodos de almacenamiento.

     No puede seleccionar esta opción a menos que haya reemplazado el certificado API S3 predeterminado, firmado por la CA de grid, con un certificado personalizado firmado por una entidad de certificación externa. Consulte "Configure los certificados de API S3".

   - **Utilice el certificado de interfaz de gestión**. Seleccione esta opción si desea usar el certificado de interfaz de gestión global, que también se puede utilizar para conexiones directas a los nodos de administración.
2. Si no está utilizando el certificado StorageGRID S3, cargue o genere el certificado.

Cargue el certificado

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

- **Certificado de servidor**: El archivo de certificado de servidor personalizado en codificación PEM.
- **Clave privada del certificado**: 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 opcional 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.

c. Expanda **Detalles del certificado** para ver los metadatos de cada certificado que haya cargado. Si cargó un paquete de CA opcional, cada certificado aparece en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

  Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

d. Seleccione **Crear**. + se crea el punto final del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones subsiguientes entre los clientes S3 o la interfaz de gestión y el extremo.

Generar certificado

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o varios nombres de dominio completos que se deben incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
IP	Una o más direcciones IP que se incluirán en el certificado.

Campo	Descripción
Asunto (opcional)	X,509 Asunto o nombre distinguido (DN) del propietario del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la dirección IP como nombre común del asunto (CN).
Días válidos	Núm. De días después de la creación que caduca el certificado.
Agregue extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de claves y uso de claves ampliado se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. **Nota**: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyen estas extensiones.

c. Seleccione **generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

   - Seleccione **Descargar certificado** para guardar el archivo de certificado.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

e. Seleccione **Crear**.

   Se crea el punto final del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones subsiguientes entre clientes S3 o la interfaz de gestión y este extremo.

Después de terminar

Pasos

1. Si utiliza un DNS, asegúrese de que el DNS incluya un registro para asociar el nombre de dominio completo (FQDN) de StorageGRID a cada dirección IP que utilizarán los clientes para realizar conexiones.

   La dirección IP que introduzca en el registro DNS depende de si se utiliza un grupo de alta disponibilidad de nodos con balanceo de carga:

   - Si ha configurado un grupo de alta disponibilidad, los clientes se conectarán a las direcciones IP virtuales de dicho grupo de alta disponibilidad.

- Si no está utilizando un grupo HA, los clientes se conectarán al servicio de equilibrador de carga de StorageGRID mediante la dirección IP de un nodo de puerta de enlace o nodo de administración.

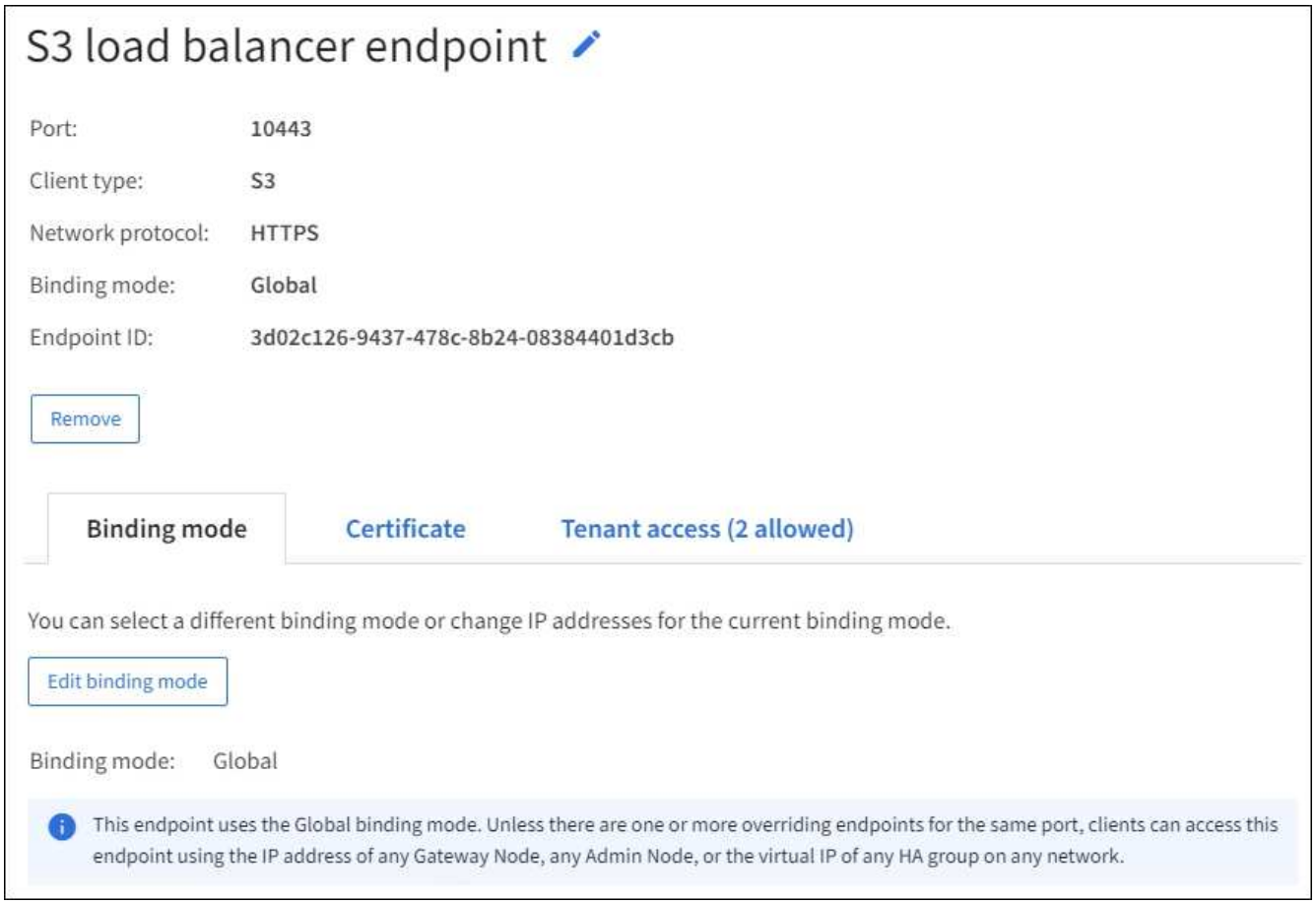
  También debe asegurarse de que el registro DNS hace referencia a todos los nombres de dominio de extremo requeridos, incluidos los nombres de comodín.

2. Proporcione a los clientes S3 la información necesaria para conectarse al punto final:
   - Número de puerto
   - Nombre de dominio o dirección IP completos
   - Los detalles de certificado necesarios

Ver y editar puntos finales del equilibrador de carga

Puede ver detalles de los extremos de equilibrador de carga existentes, incluidos los metadatos de certificado para un extremo protegido. Puede cambiar determinados valores para un punto final.

- Para ver información básica de todos los puntos finales de equilibrio de carga, revise las tablas en la página Puntos Finales de Equilibrador de Carga.
- Para ver todos los detalles acerca de un extremo específico, incluidos los metadatos del certificado, seleccione el nombre del extremo en la tabla. La información que se muestra varía en función del tipo de punto final y de cómo se configura.



- Para editar un punto final, utilice el menú **Acciones** de la página Puntos Finales de Equilibrador de Carga.

Si pierde acceso a Grid Manager al editar el puerto de un extremo de interfaz de gestión, actualice la URL y el puerto para recuperar el acceso.

Después de editar un extremo, es posible que deba esperar hasta 15 minutos para que los cambios se apliquen a todos los nodos.

Tarea	Menú Actions	Detalles
Editar el nombre del extremo	a. Seleccione la casilla de verificación para el punto final. b. Seleccione **acciones** > **Editar nombre de punto final**. c. Introduzca el nuevo nombre. d. Seleccione **Guardar**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione el icono de edición . c. Introduzca el nuevo nombre. d. Seleccione **Guardar**.
Edite el puerto de punto final	a. Seleccione la casilla de verificación para el punto final. b. Selecciona **Acciones** > **Editar puerto de punto final** c. Introduzca un número de puerto válido. d. Seleccione **Guardar**.	*n/a*
Edite el modo de enlace de punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione **acciones** > **Editar modo de enlace de punto final**. c. Actualice el modo de enlace según sea necesario. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione **Editar modo de enlace**. c. Actualice el modo de enlace según sea necesario. d. Seleccione **Guardar cambios**.
Editar certificado de extremo	a. Seleccione la casilla de verificación para el punto final. b. Seleccione **acciones** > **Editar certificado de punto final**. c. Cargue o genere un nuevo certificado personalizado o comience a utilizar el certificado global S3, según sea necesario. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione la ficha **Certificado**. c. Seleccione **Editar certificado**. d. Cargue o genere un nuevo certificado personalizado o comience a utilizar el certificado global S3, según sea necesario. e. Seleccione **Guardar cambios**.

Tarea	Menú Actions	Detalles
Editar el acceso de inquilinos	a. Seleccione la casilla de verificación para el punto final. b. Selecciona **Acciones** > **Editar acceso de inquilino**. c. Elija una opción de acceso diferente, seleccione o elimine arrendatarios de la lista, o realice ambas acciones. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione la pestaña **Acceso de inquilino**. c. Selecciona **Editar acceso de inquilino**. d. Elija una opción de acceso diferente, seleccione o elimine arrendatarios de la lista, o realice ambas acciones. e. Seleccione **Guardar cambios**.

Retire los extremos del equilibrador de carga

Puede eliminar uno o varios puntos finales mediante el menú **acciones** o puede eliminar un único punto final de la página de detalles.

> Para evitar interrupciones en el cliente, actualice las aplicaciones cliente S3 afectadas antes de eliminar un punto final del equilibrador de carga. Actualice cada cliente para que se conecte utilizando un puerto asignado a otro extremo de equilibrador de carga. Asegúrese de actualizar también la información de certificado necesaria.

> Si pierde el acceso a Grid Manager al eliminar un extremo de interfaz de gestión, actualice la dirección URL.

- Para eliminar uno o varios puntos finales:
  a. En la página Equilibrador de Carga, seleccione la casilla de verificación de cada punto final que desee eliminar.
  b. Seleccione **acciones** > **Quitar**.
  c. Seleccione **OK**.
- Para eliminar un extremo de la página de detalles:
  a. En la página Equilibrador de Carga, seleccione el nombre del punto final.
  b. Seleccione **Quitar** en la página de detalles.
  c. Seleccione **OK**.

Configure los nombres de dominio de punto final S3

Para admitir S3 solicitudes de estilo hospedado virtual, debe utilizar Grid Manager para configurar la lista de S3 nombres de dominio de punto final a los que se conectan los clientes S3.

> El uso de una dirección IP para un nombre de dominio de punto final no es compatible. Las próximas versiones impedirán esta configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Ha confirmado que no hay una actualización de grid en curso.

> No realice ningún cambio en la configuración del nombre de dominio cuando haya una actualización de cuadrícula en curso.

Acerca de esta tarea

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

- Use Grid Manager para añadir los nombres de dominio de extremo S3 al sistema StorageGRID.
- Asegúrese de que el "Certificado que el cliente utiliza para las conexiones HTTPS a StorageGRID"está firmado para todos los nombres de dominio que el cliente requiere.

  Por ejemplo, si el punto final es `s3.company.com`, debe asegurarse de que el certificado utilizado para las conexiones HTTPS incluye el `s3.company.com` punto final y el comodín Nombre Alternativo de Asunto (SAN) del punto final `*.s3.company.com`: .

- Configure el servidor DNS que utiliza el cliente. Incluya registros DNS para las direcciones IP que los clientes utilizan para realizar conexiones y asegúrese de que los registros hacen referencia a todos los nombres de dominio de punto final S3 necesarios, incluidos los nombres 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.

Los clientes que usan conexiones HTTPS (recomendadas) a la cuadrícula pueden usar cualquiera de los siguientes certificados:

- Los clientes que se conectan a un extremo de equilibrador de carga pueden utilizar un certificado personalizado para ese extremo. Cada punto final de equilibrio de carga se puede configurar para reconocer diferentes nombres de dominio de punto final S3.
- Los clientes que se conectan a un extremo de balanceador de carga o directamente a un nodo de almacenamiento pueden personalizar el certificado de API global S3 para incluir todos los nombres de dominio de extremo S3 necesarios.

> Si no agrega nombres de dominio de punto final S3 y la lista está vacía, se deshabilitará el soporte para S3 solicitudes de estilo hospedado virtual.

Agregue un nombre de dominio de punto final S3

Pasos

1. Seleccione **Configuración** > **Red** > **Nombres de dominio de punto final S3**.
2. Introduzca el nombre de dominio en el campo **Nombre de dominio 1**. Seleccione **Agregar otro nombre de dominio** para agregar más nombres de dominio.

3. Seleccione **Guardar**.
4. Asegúrese de que los certificados de servidor que utilizan los clientes coinciden con los nombres de dominio de punto final S3 necesarios.
   - Si los clientes se conectan a un punto final del equilibrador de carga que utiliza su propio certificado, "actualice el certificado asociado al punto final".
   - Si los clientes se conectan a un extremo del equilibrador de carga que utiliza el certificado de API S3 global o directamente a los nodos de almacenamiento, "Actualice el certificado de API global S3".
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 punto final `bucket.s3.company.com`, el servidor DNS se resuelve en el punto final correcto y el certificado autentica el punto final como se esperaba.

Cambie el nombre de un nombre de dominio de punto final S3

Si cambia un nombre utilizado por las aplicaciones S3, las solicitudes de estilo hospedado virtual fallarán.

Pasos

1. Seleccione **Configuración** > **Red** > **Nombres de dominio de punto final S3**.
2. Seleccione el campo de nombre de dominio que desea editar y realice los cambios necesarios.
3. Seleccione **Guardar**.
4. Selecciona **Sí** para confirmar tu cambio.

Suprimir un nombre de dominio de punto final S3

Si elimina un nombre utilizado por las aplicaciones S3, las solicitudes de estilo hospedado virtual fallarán.

Pasos

1. Seleccione **Configuración** > **Red** > **Nombres de dominio de punto final S3**.
2. Seleccione el icono de eliminación ✕ junto al nombre de dominio.
3. Seleccione **Sí** para confirmar la eliminación.

Información relacionada

- "USE LA API DE REST DE S3"
- "Ver direcciones IP"
- "Configuración de grupos de alta disponibilidad"

Resumen: Direcciones IP y puertos para conexiones cliente

Para almacenar o recuperar objetos, las aplicaciones cliente S3 se conectan al servicio de equilibrio de carga, que se incluye en todos los nodos de administración y de puerta de enlace, o al servicio de enrutador de distribución local (LDR), que se incluye en todos los nodos de almacenamiento.

Las aplicaciones cliente se pueden conectar a StorageGRID mediante la dirección IP de un nodo de cuadrícula y el número de puerto del servicio en ese nodo. Opcionalmente, puede crear grupos de alta

disponibilidad (HA) de nodos de equilibrio de carga para proporcionar conexiones altamente disponibles que utilicen direcciones IP virtuales (VIP). Si desea conectarse a StorageGRID con un nombre de dominio completo (FQDN) en lugar de una dirección IP o VIP, puede configurar entradas de DNS.

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. Si ya ha creado puntos finales del equilibrador de carga y grupos de alta disponibilidad (HA), consulte Dónde encontrar direcciones IP para localizar estos valores en Grid Manager.

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	Puerto asignado al punto final del equilibrador de carga
Nodo de administración	Equilibrador de carga	La dirección IP del nodo de administrador	Puerto asignado al punto final del equilibrador de carga
Nodo de puerta de enlace	Equilibrador de carga	La dirección IP del nodo de puerta de enlace	Puerto asignado al punto final del equilibrador de carga
Nodo de almacenamiento	LDR	La dirección IP del nodo de almacenamiento	Puertos S3 predeterminados: • HTTPS: 18082 • HTTP: 18084

URL de ejemplo

Para conectar una aplicación cliente al punto final del equilibrador de carga de un grupo 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 HA es 192.0.2.5 y el número de puerto del extremo del equilibrador de carga es 10443, una aplicación podría utilizar la siguiente URL para conectarse a StorageGRID:

```
https://192.0.2.5:10443
```

Dónde encontrar direcciones IP

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Para encontrar la dirección IP de un nodo de grid:
   a. Seleccionar **Nodos**.
   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. Seleccione **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** > **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** > **Red** > **Puntos finales del balanceador de carga**.
   b. Tenga en cuenta el número de puerto del punto final que desea utilizar.

> Si el número de puerto es 80 o 443, el punto final se configura sólo en los nodos de Gateway, ya que esos puertos están reservados en los nodos Admin. Todos los demás puertos están configurados tanto en los nodos de puerta de enlace como en los de administración.

   c. Seleccione el nombre del punto final de la tabla.
   d. Confirme que el **Tipo de cliente** (S3) coincide con la aplicación cliente que utilizará el punto final.

Administrar redes y conexiones

Configure los ajustes de red

Puede configurar varios ajustes de red desde el Gestor de cuadrícula para ajustar el funcionamiento del sistema StorageGRID.

Configure las interfaces VLAN

Puede "Cree interfaces de LAN virtual (VLAN)"aislar y crear particiones de tráfico para mejorar la seguridad, la flexibilidad y el rendimiento. Cada interfaz de VLAN está asociada con una o varias interfaces principales en los nodos de administración y de puerta de enlace. Puede utilizar interfaces VLAN en grupos de alta disponibilidad y en extremos de equilibrador de carga para segregar el tráfico cliente o administrador por aplicación o inquilino.

Directivas de clasificación de tráfico

Puede utilizar "políticas de clasificación de tráfico" para identificar y gestionar diferentes tipos de tráfico de red, incluido el tráfico relacionado con bloques específicos, inquilinos, subredes de clientes o extremos de equilibrador de carga. Estas políticas pueden ayudar a limitar y supervisar el tráfico.

Directrices para redes StorageGRID

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

Consulte "Configure las conexiones de cliente S3" para obtener más información sobre cómo conectar clientes S3.

Redes StorageGRID predeterminadas

De forma predeterminada, StorageGRID admite tres interfaces de red por nodo de grid, lo que permite configurar las redes para cada nodo de grid individual de modo que se ajusten a sus requisitos de seguridad y acceso.

Para obtener más información sobre la topología de red, consulte "Directrices sobre 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 normalmente se utiliza para proporcionar acceso a las aplicaciones cliente S3, por lo que la red de red se puede aislar y proteger. La red de cliente puede comunicarse con cualquier subred accesible a través de la puerta de enlace local.

Directrices

- Cada nodo StorageGRID requiere una interfaz de red dedicada, dirección IP, máscara de subred y pasarela para cada red a la que se asigna.
- 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.

Interfaces opcionales

Opcionalmente, se pueden añadir interfaces adicionales a un nodo. Por ejemplo, puede que desee agregar una interfaz troncal a un nodo de administración o puerta de enlace, de modo que pueda utilizar "Interfaces de VLAN" para segregar el tráfico que pertenece a diferentes aplicaciones o inquilinos. O bien, puede que desee agregar una interfaz de acceso para utilizarla en una "Grupo de alta disponibilidad".

Para añadir enlaces troncales o interfaces de acceso, consulte lo siguiente:

- **VMware (después de instalar el nodo)**: "VMware: Añada tronco o interfaces de acceso a un nodo"
  - **Linux (antes de instalar el nodo)**:"Crear archivos de configuración del nodo"
  - **Linux (después de instalar el nodo)**:"Agregar interfaces troncales o de acceso a un nodo"

> "Linux" se refiere a una implementación de RHEL, Ubuntu o Debian. Para obtener una lista de las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp (IMT)" .

Ver direcciones IP

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

Antes de empezar

Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".

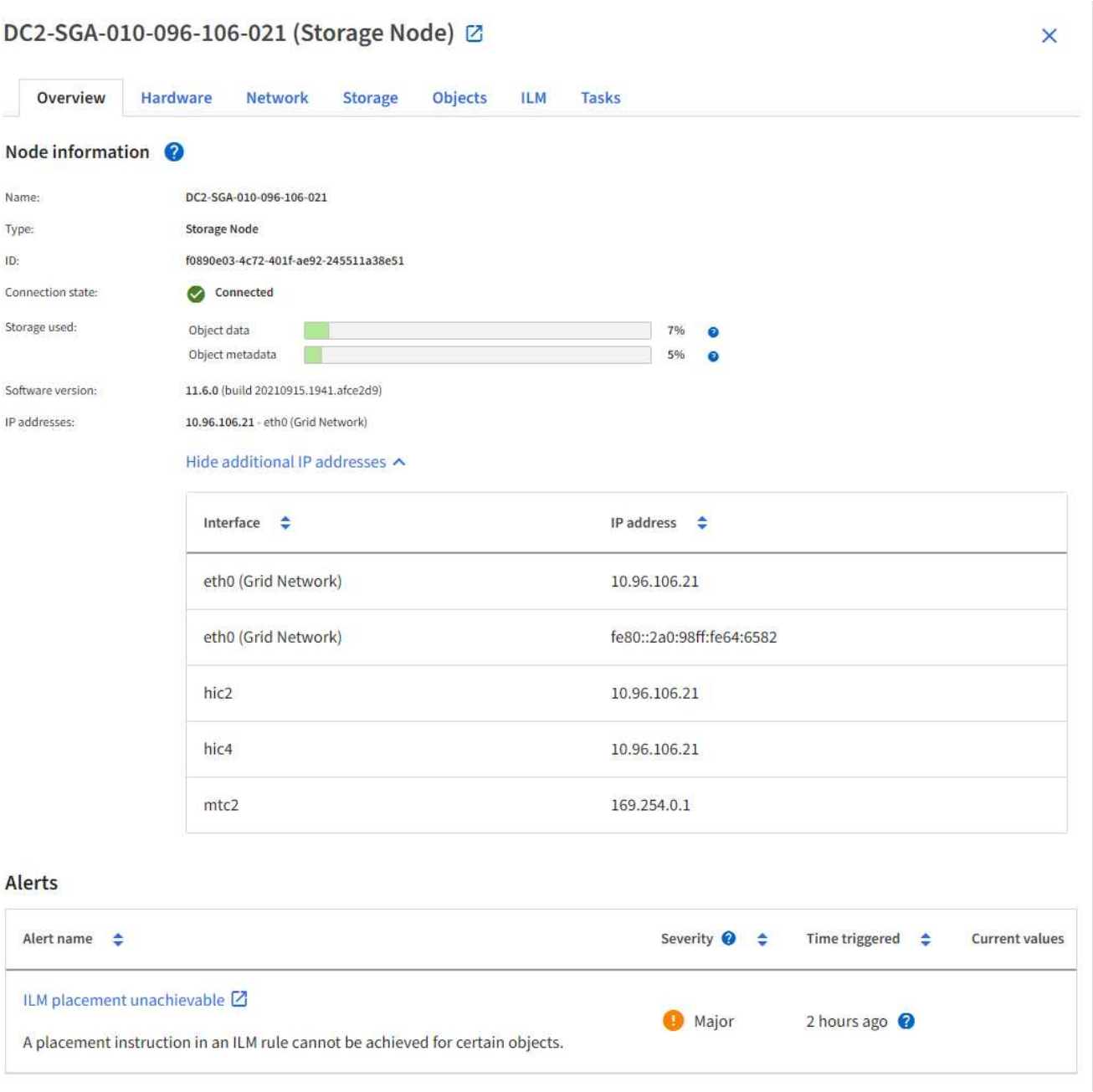
Acerca de esta tarea

Para obtener información sobre cómo cambiar direcciones IP, consulte "Configurar las direcciones IP".

Pasos

1. Seleccione **Nodos** > ***nodo de cuadrícula*** > **Descripción general**.
2. Seleccione **Mostrar más** a la derecha del título direcciones IP.

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



Configure las interfaces VLAN

Cree interfaces de LAN virtual (VLAN) en nodos de administración y nodos de puerta de enlace y úselas en grupos de alta disponibilidad y puntos finales de balanceador de carga para aislar y particionar el tráfico para lograr seguridad, flexibilidad y rendimiento. Los nodos seleccionados en el grupo HA pueden usar las interfaces VLAN para compartir hasta 10 direcciones IP virtuales, de modo que si un nodo deja de funcionar, otro nodo se hace cargo del tráfico hacia y desde las direcciones IP virtuales.

Consideraciones sobre las interfaces VLAN

- Para crear una interfaz de VLAN, introduzca un ID de VLAN y elija una interfaz principal en uno o varios nodos.

- Se debe configurar una interfaz padre como interfaz troncal en el conmutador.
- Una interfaz principal puede ser Grid Network (eth0), Client Network (eth2) o una interfaz troncal adicional para la máquina virtual o el host con configuración básica (por ejemplo, ens256).
- Para cada interfaz de VLAN, solo puede seleccionar una interfaz principal para un nodo determinado. Por ejemplo, no puede utilizar la interfaz de red de grid y la interfaz de red de cliente en el mismo nodo de gateway que la interfaz principal para la misma VLAN.
- Si la interfaz de VLAN es para el tráfico del nodo de administración, que incluye tráfico relacionado con el administrador de grid y el administrador de inquilinos, seleccione interfaces sólo en nodos de administración.
- Si la interfaz VLAN es para el tráfico de clientes S3, seleccione Interfaces en los nodos Admin o Gateway.
- Si necesita agregar interfaces de línea externa, consulte lo siguiente para obtener más información:
  - **VMware (después de instalar el nodo)**: "VMware: Añada tronco o interfaces de acceso a un nodo"
  - **Linux (antes de instalar el nodo)**:"Crear archivos de configuración del nodo"
  - **Linux (después de instalar el nodo)**:"Agregar interfaces troncales o de acceso a un nodo"

> "Linux" se refiere a una implementación de RHEL, Ubuntu o Debian. Para obtener una lista de las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp (IMT)" .

Cree una interfaz VLAN

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".
- Se ha configurado una interfaz de línea externa en la red y está conectada al nodo de máquina virtual o Linux. Conoce el nombre de la interfaz troncal.
- Conoce el ID de la VLAN que desea configurar.

Acerca de esta tarea

El administrador de red podría haber configurado una o más interfaces troncales y una o varias VLAN para separar el tráfico de administración o cliente que pertenezca a diferentes aplicaciones o inquilinos. Cada VLAN se identifica por un ID o etiqueta numéricos. Por ejemplo, la red puede utilizar VLAN 100 para el tráfico FabricPool y VLAN 200 para una aplicación de archivado.

Puede utilizar Grid Manager para crear interfaces VLAN que permitan a los clientes acceder a StorageGRID en una VLAN específica. Cuando se crean interfaces VLAN, se especifica el identificador de VLAN y se seleccionan las interfaces principales (troncales) en uno o varios nodos.

Acceda al asistente

Pasos

1. Seleccione **Configuración** > **Red** > **Interfaces VLAN**.
2. Seleccione **Crear**.

Introduzca los detalles de las interfaces de VLAN

Pasos

1. Especifique el ID de la VLAN en la red. Puede introducir cualquier valor entre 1 y 4094.

   Los ID de VLAN no tienen por qué ser únicos. Por ejemplo, puede utilizar el identificador de VLAN 200 para el tráfico de administración en un sitio y el mismo identificador de VLAN para el tráfico de cliente en otro sitio. Puede crear interfaces VLAN independientes con diferentes conjuntos de interfaces principales en cada sitio. Sin embargo, dos interfaces de VLAN con el mismo ID no pueden compartir la misma interfaz en un nodo. Si especifica un ID que ya se ha utilizado, aparecerá un mensaje.

2. De manera opcional, introduzca una breve descripción para la interfaz de VLAN.
3. Seleccione **continuar**.

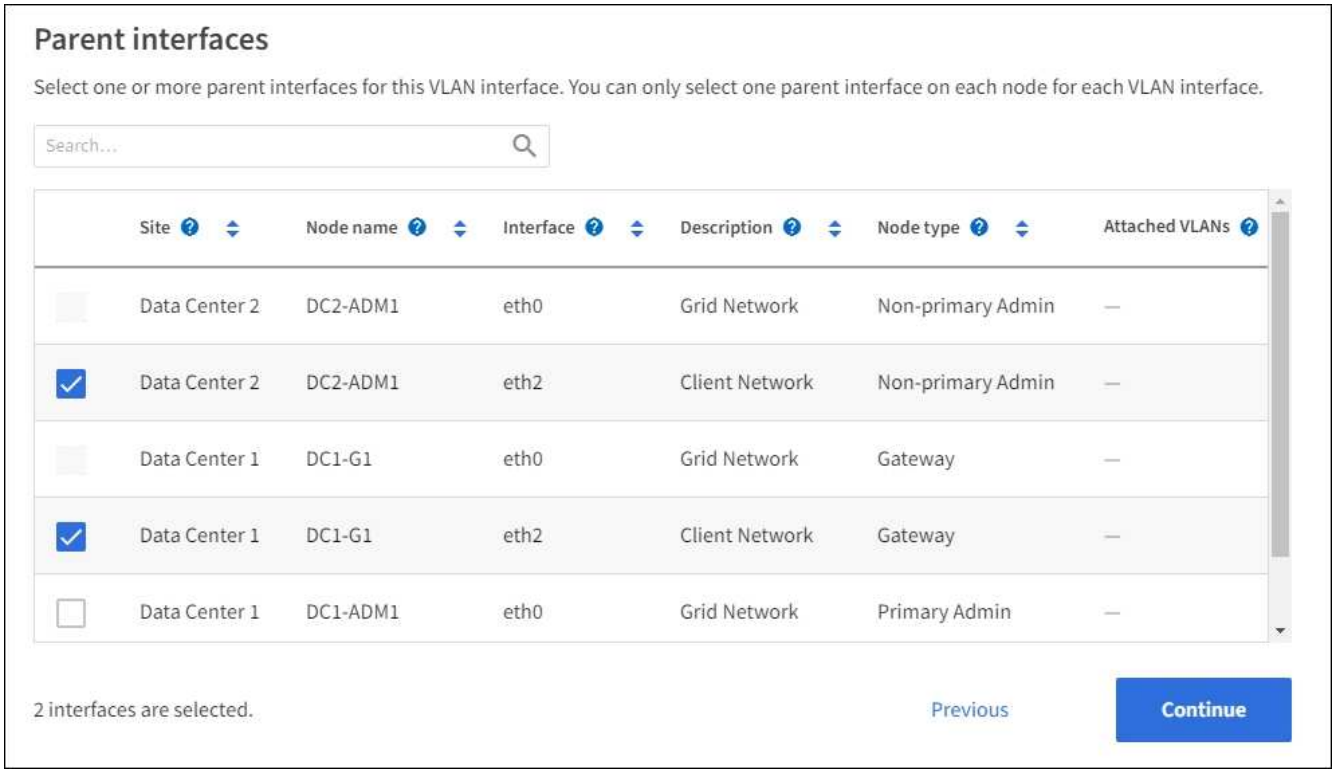
Elija interfaces padre

En la tabla, se enumeran las interfaces disponibles para todos los nodos de administrador y los nodos de puerta de enlace en cada sitio del grid. Las interfaces de la red de administración (eth1) no se pueden utilizar como interfaces principales y no se muestran.

Pasos

1. Seleccione una o varias interfaces primarias para asociar esta VLAN.

   Por ejemplo, es posible que desee conectar una VLAN a la interfaz de red de cliente (eth2) para un nodo de puerta de enlace y un nodo de administrador.



2. Seleccione **continuar**.

Confirme la configuración

Pasos

1. Revise la configuración y realice cualquier cambio.
   - Si necesita cambiar el ID de VLAN o la descripción, seleccione **introducir detalles de VLAN** en la

parte superior de la página.

- Si necesita cambiar una interfaz padre, seleccione **elegir interfaces padre** en la parte superior de la página o seleccione **anterior**.
- Si necesita eliminar una interfaz principal, seleccione la papelera .

2. Seleccione **Guardar**.
3. Espere hasta 5 minutos para que la nueva interfaz aparezca como una selección en la página Grupos de alta disponibilidad y se incluya en la tabla **Interfaces de red** del nodo (**Nodos** > ***nodo de interfaz principal*** > **Red**).

Edite una interfaz VLAN

Cuando edite una interfaz de VLAN, puede realizar los siguientes tipos de cambios:

- Cambie el ID o la descripción de la VLAN.
- Agregar o quitar interfaces principales.

Por ejemplo, es posible que desee quitar una interfaz principal de una interfaz VLAN si va a retirar el nodo asociado.

Tenga en cuenta lo siguiente:

- No puede cambiar un ID de VLAN si la interfaz VLAN se utiliza en un grupo de alta disponibilidad.
- No puede quitar una interfaz principal si se utiliza esa interfaz principal en un grupo de alta disponibilidad.

  Por ejemplo, supongamos que VLAN 200 está conectada a interfaces principales en los nodos A y B. Si un grupo de alta disponibilidad utiliza la interfaz VLAN 200 para el nodo A y la interfaz eth2 para el nodo B, puede eliminar la interfaz principal no utilizada para el nodo B, pero no puede eliminar la interfaz principal utilizada para el nodo A.

Pasos

1. Seleccione **Configuración** > **Red** > **Interfaces VLAN**.
2. Seleccione la casilla de comprobación de la interfaz de VLAN que desea editar. A continuación, seleccione **acciones** > **Editar**.
3. Si lo desea, actualice el ID de VLAN o la descripción. A continuación, seleccione **continuar**.

   No se puede actualizar un identificador de VLAN si la VLAN se utiliza en un grupo de alta disponibilidad.

4. Opcionalmente, active o desactive las casillas de verificación para agregar interfaces principales o para eliminar las interfaces no utilizadas. A continuación, seleccione **continuar**.
5. Revise la configuración y realice cualquier cambio.
6. Seleccione **Guardar**.

Quite una interfaz VLAN

Puede eliminar una o varias interfaces VLAN.

No puede quitar una interfaz VLAN si actualmente se utiliza en un grupo de alta disponibilidad. Para poder eliminarlo, debe quitar la interfaz VLAN del grupo ha.

Para evitar cualquier interrupción en el tráfico de cliente, considere realizar una de las siguientes acciones:

- Añada una nueva interfaz VLAN al grupo de alta disponibilidad antes de eliminar esta interfaz de VLAN.
- Cree un nuevo grupo de alta disponibilidad que no utilice esta interfaz VLAN.
- Si la interfaz VLAN que desea quitar tiene actualmente la interfaz activa, edite el grupo de alta disponibilidad. Mueva la interfaz de VLAN que desea quitar a la parte inferior de la lista de prioridades. Espere hasta que se establezca la comunicación en la nueva interfaz principal y, a continuación, quite la interfaz antigua del grupo de alta disponibilidad. Por último, elimine la interfaz de VLAN en ese nodo.

Pasos

1. Seleccione **Configuración** > **Red** > **Interfaces VLAN**.
2. Seleccione la casilla de comprobación de cada interfaz de VLAN que desea quitar. A continuación, seleccione **acciones** > **Eliminar**.
3. Seleccione **Sí** para confirmar su selección.

   Se eliminan todas las interfaces VLAN seleccionadas. Se muestra un banner verde de éxito en la página de interfaces de VLAN.

Habilitar StorageGRID CORS para una interfaz de administración

Como administrador de la red, puede habilitar el uso compartido de recursos de origen cruzado (CORS) para las solicitudes de API de administración a StorageGRID, si desea que los datos en StorageGRID sean accesibles mediante API de administración a otro dominio.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- El"Permiso de acceso raíz" Proporciona acceso a todas las solicitudes de configuración de CORS.

Acerca de esta tarea

CORS es un mecanismo de seguridad que permite que las aplicaciones web cliente de un dominio accedan a recursos de un dominio diferente. Por ejemplo, supongamos que desea crear un panel de monitoreo para StorageGRID en el dominio `http://www.example.com` . Al habilitar CORS en StorageGRID para `http://www.example.com` y "Grid Manager", el dominio StorageGRID responde a las solicitudes de API de administración de Grid de `http://www.example.com` .

Solicitudes de API de administración (mgmt-api) con `application/json` o `multipart/formdata` solicitudes de `Content-Type` son compatibles con CORS.

Pasos

1. En Grid Manager, vaya a **CONFIGURACIÓN** > **Red** > **Configuración CORS de la interfaz de administración**.
2. Seleccione **Administrador de red**, **Administrador de inquilinos** o ambas opciones.
   - **Grid Manager**: habilita CORS para solicitudes de API de administración de cuadrícula entre dominios.
   - **Administrador de inquilinos**: habilita CORS para solicitudes de API de administración de inquilinos entre dominios.
3. Introduzca la URL del otro dominio en el campo **Dominios**.

   Seleccione **Agregar otro dominio** si desea habilitar CORS en StorageGRID para más de un dominio.

4. Seleccione **Guardar**.

Información relacionada

"Configurar StorageGRID CORS para depósitos y objetos"

Administrar directivas de clasificación de tráfico

¿Qué son las políticas de clasificación de tráfico?

Las directivas de clasificación del tráfico le permiten identificar y supervisar diferentes tipos de tráfico de red. Estas políticas pueden ayudar con la limitación y la supervisión del tráfico para mejorar sus ofertas de calidad de servicio (QoS).

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

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
- Subred
- Inquilino
- 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.

Limitación del tráfico

Opcionalmente, puede agregar los siguientes tipos de límite a una política:

- Ancho de banda de agregado
- Ancho de banda por solicitud
- Solicitudes simultáneas
- Tasa de solicitud

Los valores límite se aplican por cada 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.

> Puede crear políticas para limitar el ancho de banda agregado o para limitar el ancho de banda por solicitud. Sin embargo, la 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 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. El ancho de banda consumido por la solicitud no cuenta en comparación con otras políticas que coincidan menos específicas que contengan políticas de límite de ancho de banda agregado. 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.

Utilice las políticas de clasificación del tráfico con los 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.

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	El máximo rendimiento permitido	Coste
Oro	1 PB de almacenamiento permitido	3 regla de copia de ILM	25 K solicitudes/seg 5 GB/s (40 Gbps) de ancho de banda	por mes
Plata	250 TB de almacenamiento permitido	2 regla de copia de ILM	10 K solicitudes/seg 1,25 GB/s (10 Gbps) de ancho de banda	$$ al mes
Bronce	100 TB de almacenamiento permitido	2 regla de copia de ILM	5 K solicitudes/seg 1 GB/s (8 Gbps) de ancho de banda	$ al mes

Cree directivas de clasificación de tráfico

Puede crear políticas de clasificación del tráfico si desea supervisar y, de manera opcional, limitar el tráfico de red por bloque, periodo de reunión, CIDR, extremo de equilibrador de carga o inquilino. 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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".
- Ha creado cualquier punto final de equilibrador de carga que desee que coincida.

- Ha creado los inquilinos que desea que coincidan.

Pasos

1. Seleccione **Configuración** > **Red** > **Clasificación de tráfico**.
2. Seleccione **Crear**.
3. Introduzca un nombre y una descripción (opcional) para la política y seleccione **Continuar**.

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

4. Seleccione **Añadir regla** y especifique los siguientes detalles para crear una o más reglas de coincidencia para la política. Cualquier política que cree debe tener al menos una regla de coincidencia. Seleccione **continuar**.

Campo	Descripción
Tipo	Seleccione los tipos de tráfico a los que se aplica la regla de coincidencia. Los tipos de tráfico son bucket, bucket regex, CIDR, load balancer endpoint y tenant.
Valor de coincidencia	Introduzca el valor que coincida con el tipo seleccionado. • Bucket: Introduzca uno o más nombres de bucket. • Bucket Regex: Introduzca una o más expresiones regulares utilizadas para hacer coincidir un juego de nombres de cubos. La expresión regular no está anclada. Utilice el anclaje ^ para que coincida al principio del nombre del cubo y utilice el anclaje $ para que coincida al final del nombre. La coincidencia de expresiones regulares admite un subconjunto de sintaxis PCRE (expresión regular compatible con Perl). • CIDR: Introduzca una o más subredes IPv4, en notación CIDR, que coincida con la subred deseada. • Punto final de equilibrio de carga: Seleccione un nombre de punto final. Estos son los puntos finales del equilibrador de carga definidos en la "Configurar puntos finales del equilibrador de carga". • Tenant: La coincidencia de inquilinos utiliza el ID de clave de acceso. Si la solicitud no contiene un identificador de clave de acceso (por ejemplo, acceso anónimo), la propiedad del bloque al que se accede se utiliza para determinar el inquilino.

Campo	Descripción
Coincidencia inversa	Si desea hacer coincidir todo el tráfico de red *excepto* tráfico consistente con el valor Tipo y Coincidencia que acaba de definir, seleccione la casilla de verificación **Coincidencia inversa**. De lo contrario, deje la casilla de verificación desactivada. Por ejemplo, si desea que esta política se aplique a todos los puntos finales excepto a uno de los de equilibrio de carga, especifique el punto final de equilibrio de carga que se va a excluir y seleccione **Coincidencia inversa**. 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.

5. Opcionalmente, seleccione **Agregar un límite** y seleccione los siguientes detalles para agregar uno o más límites para controlar el tráfico de red que coincide con una regla.

> StorageGRID recopila métricas incluso si no agrega ningún límite, para que pueda comprender las tendencias del tráfico.

Campo	Descripción
Tipo	El tipo de límite que desea aplicar al tráfico de red coincidente con la regla. Por ejemplo, puede limitar el ancho de banda o la tasa de solicitud. **Nota**: Puede crear políticas para limitar el ancho de banda agregado o limitar el ancho de banda por solicitud. Sin embargo, la StorageGRID no puede limitar ambos tipos de ancho de banda a la vez. Cuando se utiliza el ancho de banda agregado, el ancho de banda por solicitud no está disponible. Por el contrario, cuando se utiliza el ancho de banda por solicitud, el ancho de banda agregado no estará disponible. 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 implanta las «mejores» coincidencias para los 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

Campo	Descripción
Se aplica a.	Si este límite se aplica a las solicitudes de lectura del cliente (GET o HEAD) o las solicitudes de escritura (PUT, POST o DELETE).
Valor	El valor al que se limitará el tráfico de red, en función de la unidad que seleccione. Por ejemplo, introduzca 10 y seleccione MiB/s para evitar que el tráfico de red que coincide con esta regla supere los 10 MiB/s. **Nota**: Dependiendo de la configuración de unidades, las unidades disponibles serán binarias (por ejemplo, GiB) o decimales (por ejemplo, GB). Para cambiar la configuración de unidades, seleccione la lista desplegable de usuario en la parte superior derecha del Administrador de cuadrícula y, a continuación, seleccione **Preferencias de usuario**.
Unidad	La unidad que describe el valor introducido.

Por ejemplo, si desea crear un límite de ancho de banda de 4 GB/s para un nivel de SLA, cree dos límites de ancho de banda agregados: GET/HEAD a 4 GB/s y PUT/POST/DELETE a 4 GB/s.

6. Seleccione **continuar**.
7. Lea y revise la política de clasificación de tráfico. Utilice el botón **Anterior** para volver atrás y realizar los cambios necesarios. Cuando esté satisfecho con la política, seleccione **Guardar y continuar**.

   El tráfico de clientes S3 ahora se gestiona de acuerdo con la política de clasificación de tráfico.

Después de terminar

"Ver las métricas de tráfico de red" para verificar que las políticas están aplicando los límites de tráfico que espera.

Edite la política 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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".

Pasos

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

   Aparece la página Políticas de clasificación de tráfico y las políticas existentes se muestran en una tabla.

2. Edite la política mediante el menú Acciones o la página de detalles. Consulte "crear políticas de clasificación de tráfico" para ver qué introducir.

Menú Actions

a. Seleccione la casilla de verificación de la política.

b. Selecciona **Acciones** > **Editar**.

Detalles

a. Seleccione el nombre de la política.

b. Seleccione el botón **Editar** junto al nombre de la política.

3. Para el paso Introducir nombre de política, edite opcionalmente el nombre o la descripción de la política y seleccione **Continuar**.
4. Para el paso Agregar reglas de coincidencia, opcionalmente agregue una regla o edite el **Tipo** y **Valor de coincidencia** de la regla existente, y seleccione **Continuar**.
5. Para el paso Establecer límites, opcionalmente agregue, edite o elimine un límite, y seleccione **Continuar**.
6. Revise la política actualizada y seleccione **Guardar y continuar**.

   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.

Eliminar una directiva de clasificación de tráfico

Puede eliminar una política de clasificación de tráfico si ya no la necesita. Asegúrese de eliminar la política correcta porque no se puede recuperar una política al eliminarla.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".

Pasos

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

   Aparece la página Políticas de clasificación de tráfico con las políticas existentes enumeradas en una tabla.

2. Elimine la política mediante el menú Acciones o la página de detalles.

   Menú Actions

   a. Seleccione la casilla de verificación de la política.

   b. Seleccione **acciones** > **Quitar**.

   Página de detalles de política

   a. Seleccione el nombre de la política.

   b. Seleccione el botón **Eliminar** junto al nombre de la política.

3. Seleccione **Sí** para confirmar que desea eliminar la política.

La directiva se elimina.

Ver las métricas de tráfico de red

Puede supervisar el tráfico de red mediante los gráficos que están disponibles en la página de políticas de clasificación del tráfico.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Acceso raíz o cuentas de inquilino".

Acerca de esta tarea

Para cualquier política de clasificación de tráfico existente, puede ver métricas para el servicio de equilibrio de carga para determinar si la política está limitando correctamente el tráfico en toda la red. Los datos de los gráficos pueden ayudarle a determinar si necesita 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** > **Red** > **Clasificación de tráfico**.

   Aparece la página Políticas de clasificación de tráfico y las políticas existentes se muestran en la tabla.

2. Seleccione el nombre de la política de clasificación de tráfico para la que desea ver las métricas.
3. Seleccione la pestaña **Métricas**.

   Aparecen los gráficos de política de clasificación de tráfico. Los gráficos muestran métricas solo para el tráfico que coincide con la directiva seleccionada.

   Los siguientes gráficos se incluyen en la página.

   - Tasa de solicitud: Este gráfico proporciona la cantidad de ancho de banda que coincide con esta política manejada por todos los equilibradores de carga. Los datos recibidos incluyen cabeceras de solicitud para todas las solicitudes y tamaño de datos de cuerpo para las respuestas que tienen datos de cuerpo. Enviado incluye cabeceras de respuesta para todas las solicitudes y tamaño de datos de cuerpo de respuesta para las solicitudes que incluyen datos de cuerpo en la respuesta.

     > Cuando se completan las solicitudes, este gráfico sólo muestra el uso del ancho de banda. Para solicitudes de objetos lentas o grandes, el ancho de banda instantáneo real puede diferir de los valores indicados en este gráfico.

   - Tasa de respuesta de error: Este gráfico proporciona una tasa aproximada a la que las solicitudes que coinciden con esta política devuelven errores (código de estado HTTP >= 400) a los clientes.
   - Duración media de la solicitud (sin error): Este gráfico proporciona una duración media de las solicitudes correctas que coinciden con esta política.
   - Uso de ancho de banda de política: Este gráfico proporciona la cantidad de ancho de banda que coincide con esta política manejada por todos los equilibradores de carga. Los datos recibidos incluyen cabeceras de solicitud para todas las solicitudes y tamaño de datos de cuerpo para las respuestas que tienen datos de cuerpo. Enviado incluye cabeceras de respuesta para todas las solicitudes y tamaño de datos de cuerpo de respuesta para las solicitudes que incluyen datos de cuerpo en la respuesta.

4. Coloque el cursor sobre un gráfico de líneas para ver una ventana emergente de valores en una parte específica del gráfico.
5. Seleccione **Grafana dashboard** justo debajo del título de Métricas para ver todos los gráficos de una política. Además de los cuatro gráficos de la pestaña **Métricas**, puedes ver dos gráficos más:
   - Ratio de solicitud de escritura por tamaño de objeto: Ratio de solicitudes DE PUT/POST/DELETE que coincidan con esta política. El posicionamiento en una celda individual muestra las tasas por segundo. Las tasas que se muestran en la vista flotante se truncan en números enteros y pueden informar de 0 cuando hay solicitudes que no sean cero en el bloque.
   - Tasa de solicitud de lectura por tamaño de objeto: La tasa de SOLICITUDES DE OBTENCIÓN/CABECERA que coinciden con esta política. El posicionamiento en una celda individual muestra las tasas por segundo. Las tasas que se muestran en la vista flotante se truncan en números enteros y pueden informar de 0 cuando hay solicitudes que no sean cero en el bloque.
6. Alternativamente, acceda a los gráficos desde el menú **Soporte**.
   a. Seleccione **Soporte** > **Herramientas** > **Métricas**.
   b. Selecciona **Política de clasificación de tráfico** en la sección **Grafana**.
   c. Seleccione la política en el menú en la parte superior izquierda de la página.
   d. Coloque el cursor sobre un gráfico para ver una ventana emergente que muestra la fecha y hora de la muestra, los tamaños de los objetos que se agregan al recuento y el número de solicitudes por segundo durante ese período de tiempo.

      Las directivas de clasificación del tráfico se identifican por su ID. Los ID de política se muestran en la página de políticas de clasificación de tráfico.
7. Analice los gráficos para determinar con qué frecuencia la política limita el tráfico y si necesita ajustar la política.

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.

Los cifrados TLS compatibles con el uso de sistemas externos se han seleccionado para garantizar la compatibilidad con una variedad de sistemas externos. La lista es más grande que la lista de cifrados compatibles para su uso con aplicaciones cliente S3. Para configurar cifrados, vaya a **Configuración** > **Seguridad** > **Configuración de seguridad** y seleccione **Políticas TLS y SSH**.

> Las opciones de configuración de TLS, como las versiones de protocolos, 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.

Ventajas de las conexiones HTTP activas, inactivas y simultáneas

La forma en que se configuran las conexiones HTTP puede afectar el rendimiento del sistema StorageGRID. Las configuraciones varían en función de si la conexión HTTP está activa o inactiva o si tiene varias conexiones simultáneas.

Puede identificar las ventajas en el rendimiento de los siguientes tipos de conexiones HTTP:

- Conexiones HTTP inactivas
- Conexiones HTTP activas
- Conexiones HTTP simultáneas

Ventajas de mantener abiertas las conexiones HTTP inactivas

Mantenga abiertas las conexiones HTTP cuando las aplicaciones cliente estén inactivas para permitir transacciones posteriores. Mantenga abierta una conexión HTTP inactiva durante un máximo de 10 minutos. StorageGRID podría cerrar automáticamente una conexión HTTP que esté abierta e inactiva durante más de 10 minutos.

Las conexiones HTTP abiertas y inactivas proporcionan las siguientes ventajas:

- Menor latencia desde el momento en que el sistema StorageGRID determina que debe realizar una transacción HTTP hasta el momento en que el sistema StorageGRID puede realizar la transacción

  La latencia reducida es la ventaja principal, especialmente por la cantidad de tiempo necesario para establecer las conexiones TCP/IP y TLS.

- Aumento de la velocidad de transferencia de datos mediante la preparación del algoritmo de inicio lento TCP/IP con transferencias realizadas previamente
- Notificación instantánea de varias clases de condiciones de fallo que interrumpen la conectividad entre la aplicación cliente y el sistema StorageGRID

Decide cuánto tiempo mantener abierta una conexión inactiva equilibrando los beneficios del inicio lento y la asignación de recursos.

Ventajas de las conexiones HTTP activas

Para conexiones directas a nodos de almacenamiento, debe limitar la duración de una conexión HTTP activa a un máximo de 10 minutos, incluso si la conexión HTTP realiza transacciones continuamente.

La determinación de la duración máxima de la apertura de una conexión es un intercambio entre los beneficios de la persistencia de la conexión y la asignación ideal de la conexión a los recursos internos del sistema.

Para las conexiones de cliente a los nodos de almacenamiento, la limitación de las conexiones HTTP activas proporciona las siguientes ventajas:

- Permite un balanceo de carga óptimo en el sistema StorageGRID.

  Con el tiempo, una conexión HTTP puede dejar de ser óptima a medida que cambian los requisitos de equilibrio de carga. El sistema logra su mejor equilibrio de carga cuando las aplicaciones cliente establecen una conexión HTTP separada para cada transacción, pero este método anula las valiosas ganancias asociadas con las conexiones persistentes.

- Permite a las aplicaciones cliente dirigir transacciones HTTP a servicios LDR que tengan espacio disponible.
- Permite iniciar los procedimientos de mantenimiento.

  Algunos procedimientos de mantenimiento se inician solo después de que se completen todas las conexiones HTTP en curso.

En el caso de las conexiones cliente al servicio Load Balancer, limitar la duración de las conexiones abiertas puede ser útil para permitir que algunos procedimientos de mantenimiento se inicien con rapidez. Si la duración de las conexiones de cliente no es limitada, es posible que las conexiones activas tarden varios minutos en finalizarse automáticamente.

Ventajas de las conexiones HTTP simultáneas

Debe mantener abiertas varias conexiones TCP/IP al sistema StorageGRID para permitir el paralelismo, lo que aumenta el rendimiento. El número óptimo de conexiones paralelas depende de diversos factores.

Las conexiones HTTP simultáneas proporcionan las siguientes ventajas:

- Latencia reducida

  Las transacciones pueden iniciarse inmediatamente en lugar de esperar a que se completen otras transacciones.

- Aumento de la productividad

  El sistema StorageGRID puede realizar transacciones paralelas y aumentar el rendimiento global de las transacciones.

Las aplicaciones cliente deben establecer varias conexiones HTTP. Cuando una aplicación cliente tiene que realizar una transacción, puede seleccionar y utilizar inmediatamente cualquier conexión establecida que no esté procesando actualmente una transacción.

La topología de cada sistema StorageGRID tiene un rendimiento máximo diferente para transacciones y conexiones simultáneas. El rendimiento máximo depende de los recursos informáticos, de red, de almacenamiento, de enlaces WAN y de la cantidad de servidores, servicios y aplicaciones que admite el sistema StorageGRID .

Los sistemas StorageGRID suelen admitir múltiples aplicaciones cliente. Tenga esto en cuenta al determinar el número máximo de conexiones simultáneas. Si la aplicación cliente consta de varias entidades de software que establecen conexiones con el sistema StorageGRID , sume todas las conexiones entre las entidades. Es posible que tengas que ajustar el número máximo de conexiones simultáneas en las siguientes situaciones:

- La topología del sistema StorageGRID afecta al número máximo de transacciones y conexiones simultáneas que puede admitir el sistema.
- Las aplicaciones cliente que interactúan con el sistema StorageGRID a través de una red con ancho de banda limitado pueden tener que reducir el grado de concurrencia para garantizar que las transacciones individuales se completen en un tiempo razonable.
- Cuando muchas aplicaciones cliente comparten el sistema StorageGRID, puede que tenga que reducir el nivel de concurrencia para evitar superar los límites del sistema.

Separación de grupos de conexiones HTTP para operaciones de lectura y escritura

Puede utilizar pools independientes de conexiones HTTP para operaciones de lectura y escritura y controlar la cantidad de un pool que debe utilizar para cada uno. Los grupos separados de conexiones HTTP le permiten controlar mejor las transacciones y equilibrar las cargas.

Las aplicaciones cliente pueden crear cargas que sean dominantes de la recuperación (lectura) o del almacén (escritura). Con grupos separados de conexiones HTTP para transacciones de lectura y escritura, puede ajustar la cantidad de cada pool que se va a dedicar a transacciones de lectura o escritura.

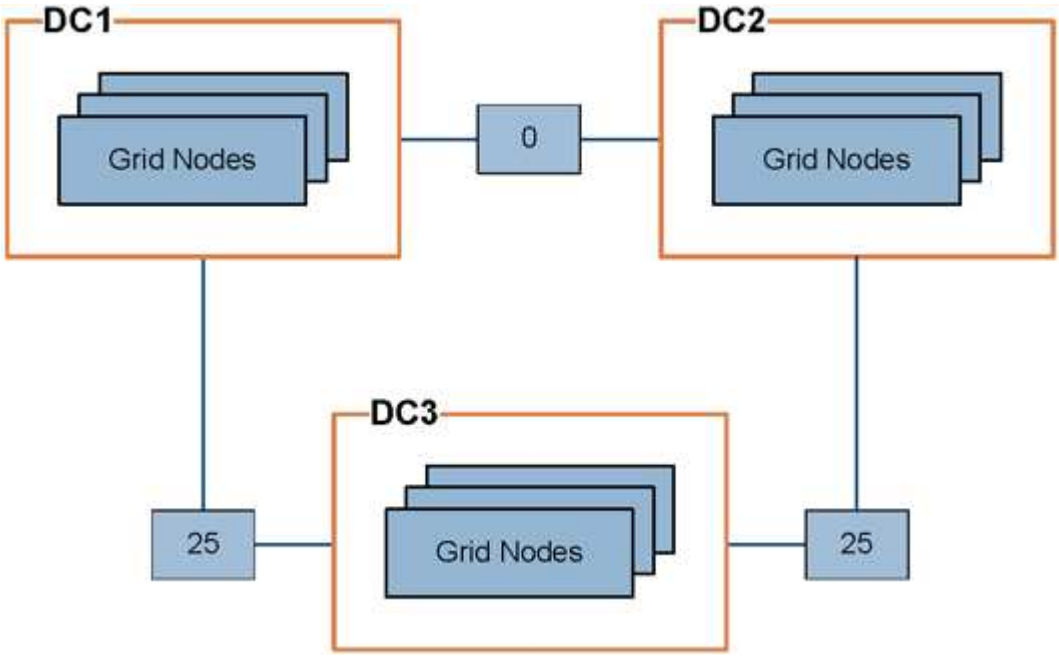
Gestionar costes de enlaces

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.

¿Qué son los costes de enlace?

- 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 de equilibrio de carga en los nodos de administración y de gateway para dirigir las conexiones de cliente. Consulte "Consideraciones que tener en cuenta al equilibrio de carga".

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



- El servicio Load Balancer en los nodos de administración y de puerta de enlace distribuye equitativamente las conexiones de los clientes a todos los nodos de almacenamiento en el 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 de DC2 recupera un objeto almacenado tanto en DC1 como en DC3, el objeto se recupera de DC1, porque el coste del enlace de DC1 a DC2 es 0, que es inferior al coste del enlace 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.

Actualizar costes de enlace

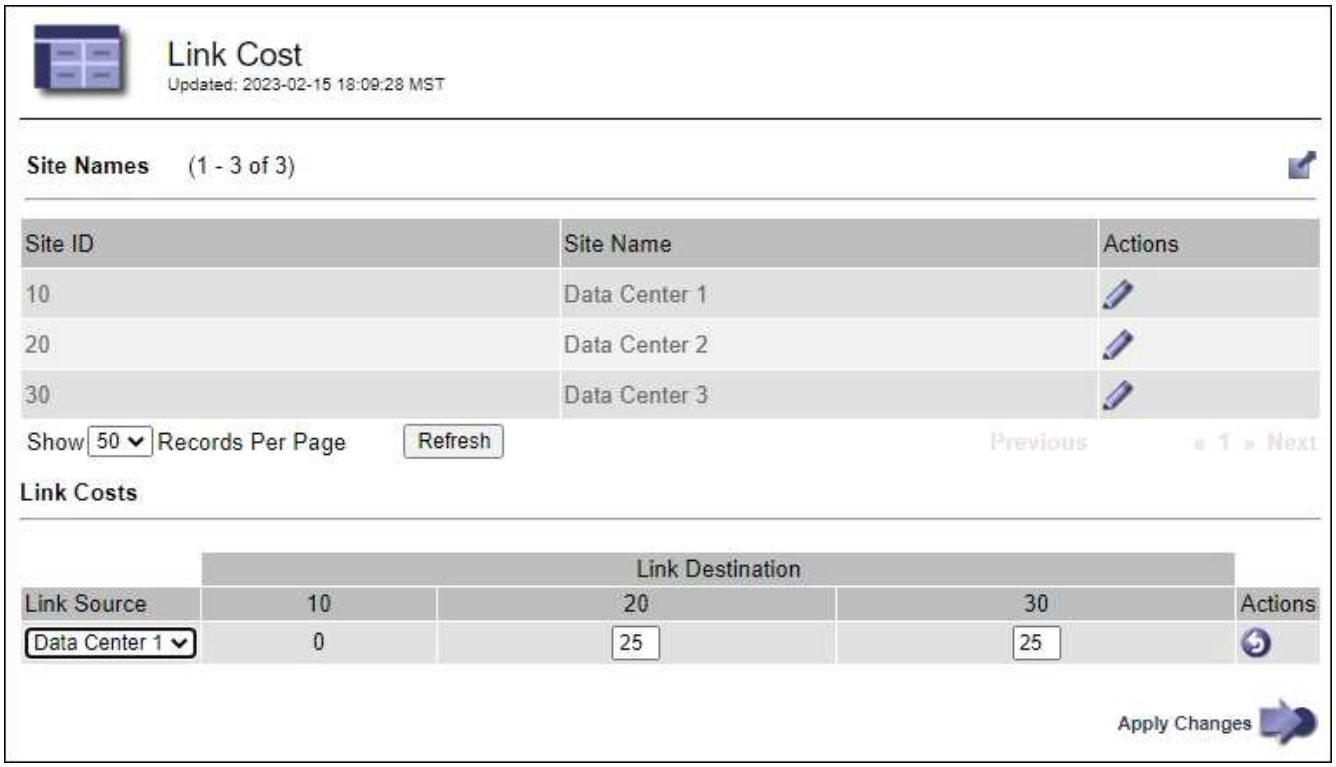
Puede actualizar los costes de enlace entre los sitios de centros de datos para reflejar la latencia entre los sitios.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tú tienes el"Otros permisos de configuración de la red" .

Pasos

1. Seleccione **Soporte** > **Otro** > **Costo del enlace**.



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

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

   Para cancelar los cambios, seleccione **Revertir**.

3. Seleccione **aplicar cambios**.

Utilice AutoSupport

¿Qué es AutoSupport?

La función AutoSupport permite que StorageGRID envíe paquetes de estado y estado al soporte técnico de NetApp.

El uso de AutoSupport ayuda a resolver problemas más rápidamente. El soporte técnico puede monitorear las necesidades de almacenamiento de su sistema y ayudarlo a determinar si necesita agregar nuevos nodos o sitios. Opcionalmente, AutoSupport puede enviar paquetes a un destino adicional.

StorageGRID tiene dos tipos de AutoSupport:

- **StorageGRID AutoSupport** informa de problemas de software de StorageGRID. Habilitado de forma predeterminada la primera vez que se instala StorageGRID. Usted puede "Cambie la configuración predeterminada de AutoSupport" si es necesario.

> Si StorageGRID AutoSupport no está habilitado, aparecerá un mensaje en el panel de Grid Manager. El mensaje incluye un enlace a la página de configuración de AutoSupport . Si cierra el mensaje, no volverá a aparecer hasta que se borre la memoria caché de su navegador, incluso si AutoSupport permanece deshabilitado.

- **El hardware del dispositivo AutoSupport** informa de los problemas del dispositivo StorageGRID. Usted debe "Configure el AutoSupport de hardware en cada dispositivo".

¿Qué es Active IQ?

Active IQ es un asesor digital basado en cloud que aprovecha el análisis predictivo y los conocimientos de la comunidad de la base instalada de NetApp. Sus evaluaciones de riesgos continuas, las alertas predictivas, las directrices prescriptivas y las acciones automatizadas le ayudan a evitar problemas antes de que se produzcan, lo que mejora el estado del sistema y aumenta la disponibilidad del sistema.

Si desea usar las consolas y la funcionalidad de Active IQ en el sitio de soporte de NetApp, debe habilitar AutoSupport.

"Documentación del asesor digital de Active IQ"

Información incluida en el paquete AutoSupport

Un paquete de AutoSupport contiene los siguientes archivos y detalles.

Nombre de archivo	Campos	Descripción
AUTOSUPPORT-HISTORY.XML	Núm. De Secuencia AutoSupport + Destino para este AutoSupport + Estado de Entrega + Intentos de Entrega + AutoSupport Asunto + URI de Entrega + Último Error + Nombre de Archivo AutoSupport PUT + Hora de Generación + Tamaño Comprimido AutoSupport + Tamaño Descomprimido AutoSupport + Tiempo Total de Recopilación (ms)	Archivo de historial de AutoSupport.
AUTOSUPPORT.XML	Nodo + Protocolo para contactar al soporte + URL de soporte para HTTP/HTTPS + Dirección de soporte + Estado de AutoSupport OnDemand + URL del servidor AutoSupport OnDemand + Intervalo de sondeo de AutoSupport OnDemand	Archivo de estado de AutoSupport. Proporciona detalles del protocolo utilizado, la URL y la dirección de soporte técnico, el intervalo de sondeo y OnDemand AutoSupport si se habilita o se deshabilita.

Nombre de archivo	Campos	Descripción
BUCKETS.XML	ID de bloque + ID de cuenta + Versión de compilación + Configuración de restricción de ubicación + Cumplimiento habilitado + Configuración de cumplimiento + S3 Bloqueo de objeto habilitado + S3 Configuración de bloqueo de objeto + Configuración de consistencia + CORS activado + Configuración de CORS + Hora de último acceso habilitada + Política habilitada + Configuración de política + Notificaciones habilitadas + Configuración de reflejo en la nube + Búsqueda habilitada + Configuración de búsqueda + Etiquetado de bloque activado + Configuración de control de versiones	Proporciona estadísticas y detalles de configuración a nivel de bloque. Ejemplo de configuración de bloques que incluyen servicios de plataforma, cumplimiento de normativas y coherencia de bloques.
GRID-CONFIGURATIONS.XML	ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Archivo de información de configuración de toda la cuadrícula. Contiene información sobre certificados de grid, espacio reservado de metadatos, ajustes de configuración de toda la cuadrícula (cumplimiento, bloqueo de objetos S3, compresión de objetos, alertas, configuración de syslog e ILM), detalles del perfil de codificación de borrado, nombre DNS y "Nombre de NMS".
GRID-SPEC.XML	Especificaciones de cuadrícula, XML sin procesar	Se utiliza para configurar e implementar StorageGRID. Contiene especificaciones de cuadrícula, IP del servidor NTP, IP del servidor DNS, topología de red y perfiles de hardware de los nodos.
GRID-TASKS.XML	Nodo + Ruta de Acceso de Servicio + ID de Atributo + Nombre de Atributo + Valor + Índice + ID de Tabla + Nombre de Tabla	Archivo de estado de tareas de cuadrícula (procedimientos de mantenimiento). Proporciona detalles de las tareas activas, terminadas, completadas, fallidas y pendientes de la cuadrícula.
GRID.JSON	Grid + Revisión + Versión de software + Descripción + Licencia + Contraseñas + DNS + NTP + Sitios + Nodos	Información de cuadrícula.

Nombre de archivo	Campos	Descripción
ILM-CONFIGURATION.XML	ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Lista de atributos para configuraciones de ILM.
ILM-STATUS.XML	Nodo + Ruta de Acceso de Servicio + ID de Atributo + Nombre de Atributo + Valor + Índice + ID de Tabla + Nombre de Tabla	Archivo de información de métricas de ILM. Contiene tasas de evaluación de ILM para cada nodo y métricas de todo el grid.
ILM.XML	XML sin procesar de ILM	Archivo de política activa de ILM. Contiene detalles sobre las políticas de ILM activas, como el ID de pool de almacenamiento, el comportamiento de ingesta, los filtros, las reglas y la descripción.
LOG.TGZ	*n/a*	Archivo de registro descargable. Contiene `bycast-err.log` y `servermanager.log` de cada nodo.
MANIFIESTO.XML	Orden de recopilación + nombre de archivo de contenido AutoSupport para estos datos + Descripción de este elemento de datos + Número de bytes recogidos + Tiempo de recopilación + Estado de este elemento de datos + Descripción del error + Tipo de contenido AutoSupport para estos datos	Contiene metadatos AutoSupport y breves descripciones de todos los archivos AutoSupport.
NMS-ENTITIES.XML	Índice de atributos + OID de entidad + ID de nodo + ID de modelo de dispositivo + versión de modelo de dispositivo + nombre de entidad	Entidades de grupo y servicio en la "Árbol de NMS". Proporciona detalles de topología de cuadrícula. El nodo se puede determinar en función de los servicios que se ejecutan en el nodo.
OBJECT-STATUS.XML	Nodo + Ruta de Acceso de Servicio + ID de Atributo + Nombre de Atributo + Valor + Índice + ID de Tabla + Nombre de Tabla	Estado del objeto, incluido el estado de análisis en segundo plano, transferencia activa, tasa de transferencia, total de transferencias, tasa de eliminación, fragmentos dañados, objetos perdidos, objetos perdidos, intentos de reparación, velocidad de análisis, período de análisis estimado y estado de finalización de reparación.

Nombre de archivo	Campos	Descripción
SERVER-STATUS.XML	Nodo + Ruta de Acceso de Servicio + ID de Atributo + Nombre de Atributo + Valor + Índice + ID de Tabla + Nombre de Tabla	Configuraciones de servidor. Contiene estos detalles para cada nodo: Tipo de plataforma, sistema operativo, memoria instalada, memoria disponible, conectividad de almacenamiento, número de serie del chasis del dispositivo de almacenamiento, número de unidades con errores de la controladora de almacenamiento, temperatura del chasis de la controladora de computación, número de serie de la controladora de computación, fuente de alimentación, tamaño de unidad y tipo de unidad.
SERVICE-STATUS.XML	Nodo + Ruta de Acceso de Servicio + ID de Atributo + Nombre de Atributo + Valor + Índice + ID de Tabla + Nombre de Tabla	Archivo de información del nodo de servicio. Contiene detalles como espacio de tabla asignado, espacio de tabla libre, métricas de la base de datos de Reaper, duración de la reparación de segmentos, duración del trabajo de reparación, reinicios automáticos de trabajos y terminación automática de trabajos.
STORAGE-GRADES.XML	ID de grado de almacenamiento + Nombre de grado de almacenamiento + ID de nodo de almacenamiento + Ruta de nodo de almacenamiento	Archivo de definiciones de grado de almacenamiento para cada nodo de almacenamiento.
SUMMARY-ATTRIBUTES.XML	OID de grupo + Ruta de grupo + ID de atributo de resumen + Nombre de atributo de resumen + Valor + Índice + ID de tabla + Nombre de tabla	Datos de estado del sistema de alto nivel que resumen la información de uso de StorageGRID. Proporciona detalles como el nombre de grid, los nombres de los sitios, la cantidad de nodos de almacenamiento por grid y por sitio, el tipo de licencia, la capacidad y el uso de la licencia, los términos de soporte del software y los detalles de las operaciones de S3.
SYSTEM-ALERTS.XML	Nombre + Gravedad + Nombre de nodo + Estado de alerta + Nombre de sitio + Hora de activación de alerta + Tiempo de resolución de alerta + ID de regla + ID de nodo + ID de sitio + Silenciada + Otras anotaciones + otras etiquetas	Alertas actuales del sistema que indican posibles problemas en el sistema StorageGRID.

Nombre de archivo	Campos	Descripción
USERAGENTS.XML	Agente de usuario + Núm. De días + Total de solicitudes HTTP + Total de bytes ingeridos + Total de bytes recuperados + Solicitudes PUT + SOLICITUDES GET + Solicitudes DELETE + Solicitudes HEAD + Solicitudes POST + Solicitudes OPTIONS + Tiempo Medio de Solicitud PUT (ms) + Tiempo Medio de Solicitud GET (ms) + Tiempo Medio de Solicitud POST (ms) + Tiempo Medio de Solicitud POST (ms)	Estadísticas basadas en los agentes de usuario de la aplicación. Por ejemplo, el número de operaciones PUT/GET/DELETE/HEAD por agente de usuario y el tamaño total de bytes de cada operación.
DATOS-CON-ENCABEZADOX.	X-NetApp-asup-generated-on + X-NetApp-asup-hostname + X-NetApp-asup-os-version + X-NetApp-asup-serial-num + X-NetApp-asup-subject + X-NetApp-asup-system-id + X-NetApp-asup-model-name	Datos de encabezados AutoSupport.

Configure AutoSupport

De forma predeterminada, la función StorageGRID AutoSupport se habilita cuando se instala por primera vez StorageGRID. Sin embargo, debe configurar el AutoSupport de hardware en cada dispositivo. Según sea necesario, puede cambiar la configuración de AutoSupport.

Si desea cambiar la configuración de StorageGRID AutoSupport, realice los cambios sólo en el nodo de administración principal. Debe Configure el AutoSupport de hardware colocarse en cada aparato.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".
- Si va a utilizar HTTPS para enviar paquetes AutoSupport, ha proporcionado acceso a Internet saliente al nodo de administración principal, ya sea directamente o "utilizando un servidor proxy" (conexiones entrantes no necesarias).
- Si se selecciona HTTP en la página StorageGRID AutoSupport, debe "se configuró un servidor proxy"reenviar los paquetes de AutoSupport como HTTPS. Los servidores AutoSupport de NetApp rechazarán los paquetes enviados mediante HTTP.
- Si utilizará SMTP como protocolo para paquetes de AutoSupport, habrá configurado un servidor de correo SMTP.

Acerca de esta tarea

Puede usar cualquier combinación de las siguientes opciones para enviar paquetes de AutoSupport al soporte técnico:

- **Semanal**: Envía automáticamente paquetes AutoSupport una vez por semana. Valor predeterminado: Activado.
- **Activado por eventos**: Envía automáticamente paquetes AutoSupport cada hora o cuando ocurran eventos significativos del sistema. Valor predeterminado: Activado.
- **On Demand**: Permite al soporte técnico solicitar que tu sistema StorageGRID envíe paquetes AutoSupport automáticamente, lo cual es útil cuando están trabajando activamente en un problema (requiere protocolo de transmisión HTTPS AutoSupport). Ajuste predeterminado: Desactivado.
- **Activado por el usuario**: Envía manualmente paquetes AutoSupport en cualquier momento.
- **Recopilación de registros**:"Recopilar manualmente archivos de registro y datos del sistema y enviar un paquete de AutoSupport" .

Especifique el protocolo para paquetes AutoSupport

Puede usar cualquiera de los siguientes protocolos para enviar paquetes de AutoSupport:

- **HTTPS**: Es la configuración predeterminada y recomendada para nuevas instalaciones. Este protocolo utiliza el puerto 443. Si lo desea Habilite la función AutoSupport On Demand, debe utilizar HTTPS.
- **HTTP**: Si selecciona HTTP, debe configurar un servidor proxy para reenviar paquetes AutoSupport como HTTPS. Los servidores AutoSupport de NetApp rechazan los paquetes enviados mediante HTTP. Este protocolo utiliza el puerto 80.
- **SMTP**: Utilice esta opción si desea que los paquetes de AutoSupport sean enviados por correo electrónico.

El protocolo configurado se utiliza para enviar todos los tipos de paquetes de AutoSupport.

Pasos

1. Seleccione **Soporte** > **Herramientas** > * AutoSupport* > **Configuración**.
2. Seleccione el protocolo que desea usar para enviar paquetes de AutoSupport.
3. Si seleccionó **HTTPS**, seleccione si desea usar un certificado de soporte NetApp (certificado TLS) para proteger la conexión con el servidor de soporte técnico.
   - **Verificar certificado** (por defecto): Asegura que la transmisión de los paquetes AutoSupport sea segura. El certificado de soporte de NetApp ya está instalado con el software StorageGRID.
   - **No verificar certificado**: Seleccione esta opción sólo cuando tenga un buen motivo para no utilizar la validación de certificados, como cuando haya un problema temporal con un certificado.
4. Seleccione **Guardar**. Todos los paquetes semanales, activados por el usuario y activados por eventos se envían mediante el protocolo seleccionado.

Deshabilite el AutoSupport semanal

De manera predeterminada, el sistema StorageGRID se configura para enviar un paquete de AutoSupport al soporte técnico una vez a la semana.

Para determinar cuándo se enviará el paquete AutoSupport semanal, vaya a la pestaña **AutoSupport** > **Resultados**. En la sección **AutoSupport semanal**, mira el valor de **Próxima hora programada**.

Es posible deshabilitar el envío automático de paquetes de AutoSupport semanales en cualquier momento.

Pasos

1. Seleccione **Soporte** > **Herramientas** > * AutoSupport* > **Configuración**.
2. Desactive la casilla de verificación **Activar AutoSupport semanal**.
3. Seleccione **Guardar**.

Deshabilite el AutoSupport activado por eventos

De manera predeterminada, el sistema StorageGRID está configurado para enviar un paquete de AutoSupport al soporte técnico cada hora.

Puede deshabilitar la AutoSupport activada por eventos en cualquier momento.

Pasos

1. Seleccione **Soporte** > **Herramientas** > * AutoSupport* > **Configuración**.
2. Desactive la casilla de verificación **Activar AutoSupport desencadenado por eventos**.
3. Seleccione **Guardar**.

Habilite AutoSupport bajo demanda

AutoSupport On Demand puede ayudar a resolver problemas en los que el soporte técnico está trabajando activamente.

De manera predeterminada, AutoSupport On Demand está deshabilitado. Al habilitar esta función, el soporte técnico puede solicitar que el sistema StorageGRID envíe paquetes AutoSupport automáticamente. El soporte técnico también puede establecer el intervalo de sondeo para AutoSupport en consultas bajo demanda.

El soporte técnico no puede habilitar ni deshabilitar AutoSupport On Demand.

Pasos

1. Seleccione **Soporte** > **Herramientas** > * AutoSupport* > **Configuración**.
2. Seleccione **HTTPS** para el protocolo.
3. Seleccione la casilla de verificación **Activar AutoSupport semanal**.
4. Seleccione la casilla de verificación **Activar AutoSupport On Demand**.
5. Seleccione **Guardar**.

   AutoSupport On Demand está habilitado y el soporte técnico puede enviar solicitudes AutoSupport On Demand a StorageGRID.

Desactive las comprobaciones de actualizaciones de software

De forma predeterminada, StorageGRID se pone en contacto con NetApp para determinar si hay actualizaciones de software disponibles para su sistema. Si hay disponible una revisión o versión nueva de StorageGRID, se muestra la nueva versión en la página actualización de StorageGRID.

Según sea necesario, puede desactivar opcionalmente la comprobación de actualizaciones de software. Por ejemplo, si el sistema no tiene acceso WAN, debe desactivar la comprobación para evitar errores de descarga.

Pasos

1. Seleccione **Soporte** > **Herramientas** > * AutoSupport* > **Configuración**.

2. Desactive la casilla de verificación **Comprobar si hay actualizaciones de software**.
3. Seleccione **Guardar**.

Añada un destino de AutoSupport adicional

Cuando se habilita AutoSupport, se envían paquetes de estado y estado al soporte técnico. Puede especificar un destino adicional para todos los paquetes de AutoSupport.

Para verificar o cambiar el protocolo utilizado para enviar paquetes AutoSupport, consulte las instrucciones para Especifique el protocolo para paquetes AutoSupport.

No puede usar el protocolo SMTP para enviar paquetes AutoSupport a un destino adicional.

Pasos

1. Seleccione **Soporte** > **Herramientas** > * AutoSupport* > **Configuración**.
2. Selecciona **Activar destino AutoSupport adicional**.
3. Especifique lo siguiente:

Nombre del hostl
Nombre de host o dirección IP del servidor de un servidor de destino AutoSupport adicional.

Puede introducir solo un destino adicional.

Puerto
Puerto utilizado para conectarse a un servidor de destino AutoSupport adicional. El valor predeterminado es el puerto 80 para HTTP o el puerto 443 para HTTPS.

Validación de certificado
Si se utiliza un certificado TLS para proteger la conexión al destino adicional.

- Seleccione **Verificar certificado** para utilizar la validación del certificado.
- Seleccione **No verificar certificado** para enviar sus paquetes AutoSupport sin validación de certificado.

  Seleccione esta opción sólo cuando tenga un buen motivo para no utilizar la validación de certificados, como cuando haya un problema temporal con un certificado.

4. Si seleccionó **Verificar certificado**, haga lo siguiente:
   a. Busque la ubicación del certificado de CA.
   b. Cargue el archivo de certificado de CA.

   Aparecen los metadatos del certificado de CA.
5. Seleccione **Guardar**.

Todos los futuros paquetes de AutoSupport semanales, activados por eventos y activados por el usuario se enviarán al destino adicional.

Configurar AutoSupport para dispositivos

AutoSupport para dispositivos informa de problemas de hardware de StorageGRID y StorageGRID AutoSupport informa de problemas de software de StorageGRID, con una excepción: En el caso del sistema SGF6112, StorageGRID AutoSupport informa de problemas de hardware y software. Tiene que configurar AutoSupport en cada dispositivo, excepto en SGF6112, que no requiere una configuración adicional. AutoSupport se ha implantado de forma diferente en dispositivos de servicios y dispositivos de almacenamiento.

Se utiliza SANtricity para habilitar AutoSupport para cada dispositivo de almacenamiento. Es posible configurar SANtricity AutoSupport durante la configuración inicial del dispositivo o después de haber instalado un dispositivo:

- Para dispositivos SG6000 y SG5700, "Configure AutoSupport en SANtricity System Manager"

Los paquetes AutoSupport de los dispositivos E-Series se pueden incluir en StorageGRID AutoSupport si se configura la entrega de AutoSupport por proxy en "Administrador del sistema de SANtricity".

StorageGRID AutoSupport no informa de problemas de hardware, como fallos de DIMM o de tarjeta de interfaz del host (HIC). Sin embargo, algunos fallos de componentes pueden desencadenar "alertas de hardware". En el caso de dispositivos StorageGRID con un controlador de gestión de placa base (BMC), puede configurar capturas de correo electrónico y SNMP para informar de fallos de hardware:

- "Configurar notificaciones por correo electrónico para las alertas de BMC"
- "Configurar los ajustes de SNMP para BMC"

Información relacionada

"Soporte de NetApp"

Active manualmente un paquete AutoSupport

Para ayudar al soporte técnico en la solución de problemas con el sistema StorageGRID, puede activar manualmente el envío de un paquete AutoSupport.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes acceso de root u otro permiso de configuración de red.

Pasos

1. Seleccione **Soporte** > **Herramientas** > * AutoSupport*.
2. En la pestaña **Acciones**, selecciona **Enviar AutoSupport activado por el usuario**.

   StorageGRID intenta enviar un paquete de AutoSupport al sitio de soporte de NetApp . Si el intento es exitoso, se actualizan los valores **Resultado más reciente** y **Última vez exitoso** en la pestaña **Resultados**. Si hay un problema, el valor **Resultado más reciente** se actualiza a "Error" y StorageGRID no intenta enviar el paquete AutoSupport nuevamente.

3. Después de 1 minuto, actualice la página de AutoSupport en su navegador para acceder a los resultados más recientes.

> Además, puedes"Recopilar archivos de registro y datos del sistema más extensos" y envíelos al sitio de soporte de NetApp .

Solucionar problemas de paquetes AutoSupport

Si falla un intento de enviar un paquete de AutoSupport , el sistema StorageGRID toma diferentes acciones según el tipo de paquete de AutoSupport . Puede comprobar el estado de los paquetes de AutoSupport seleccionando **Soporte** > **Herramientas** > * AutoSupport* > **Resultados**.

Cuando el paquete AutoSupport no se envía, aparece “Failure” en la pestaña **Results** de la página **AutoSupport**.

> Si ha configurado un servidor proxy para reenviar paquetes de AutoSupport a NetApp, debe "compruebe que los valores de configuración del servidor proxy son correctos".

Fallo del paquete AutoSupport semanal

Si no se puede enviar un paquete AutoSupport semanal, el sistema StorageGRID realiza las siguientes acciones:

1. Actualiza el atributo de resultado más reciente a Reintentando.
2. Intenta reenviar el paquete AutoSupport 15 veces cada cuatro minutos durante una hora.
3. Después de una hora de errores de envío, actualiza el atributo de resultado más reciente a error.
4. Intenta enviar un paquete de AutoSupport de nuevo a la siguiente hora programada.
5. Mantiene la programación regular de AutoSupport si el paquete falla porque el servicio NMS no está disponible y si un paquete se envía antes de que pasen los siete días.
6. Cuando el servicio NMS vuelve a estar disponible, envía un paquete AutoSupport inmediatamente si un paquete no se ha enviado durante siete días o más.

Error del paquete AutoSupport activado por el usuario o activado por un evento

Si no se envía un paquete de AutoSupport activado por el usuario o activado por un evento, el sistema StorageGRID realiza las siguientes acciones:

1. Muestra un mensaje de error si se conoce el error. Por ejemplo, si un usuario selecciona el protocolo SMTP sin proporcionar la configuración de correo electrónico correcta, se muestra el siguiente error: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. No intenta enviar el paquete de nuevo.
3. Registra el error en `nms.log`.

Si ocurre una falla y SMTP es el protocolo seleccionado, verifique que el servidor de correo electrónico del sistema StorageGRID esté configurado correctamente y que su servidor de correo electrónico esté ejecutándose (**Soporte** > **Alarmas (heredado)** > **Configuración de correo electrónico heredado**). El siguiente mensaje de error podría aparecer en la página de AutoSupport : `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Aprenda a "configure los ajustes del servidor de correo electrónico".

Corrija un error de paquete AutoSupport

Si se produce un error y SMTP es el protocolo seleccionado, compruebe que el servidor de correo electrónico del sistema StorageGRID está configurado correctamente y que el servidor de correo electrónico se está ejecutando. Puede aparecer el siguiente mensaje de error en la página AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envíe los paquetes AutoSupport de E-Series a través de StorageGRID

Puede enviar los paquetes AutoSupport de E-Series SANtricity System Manager al soporte técnico a través de un nodo de administración de StorageGRID en lugar de con el puerto de gestión del dispositivo de almacenamiento.

Consulte "AutoSupport de hardware E-Series" para obtener más información sobre el uso de AutoSupport con dispositivos E-Series.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso de administrador o de dispositivo de almacenamiento".
- Ha configurado SANtricity AutoSupport:
  - Para dispositivos SG6000 y SG5700, "Configure AutoSupport en SANtricity System Manager"

> Debe tener el firmware 8.70 de SANtricity o superior para acceder a SANtricity System Manager mediante Grid Manager.

Acerca de esta tarea

Los paquetes AutoSupport de E-Series contienen detalles del hardware de almacenamiento y son más específicos que otros paquetes de AutoSupport enviados por el sistema StorageGRID.

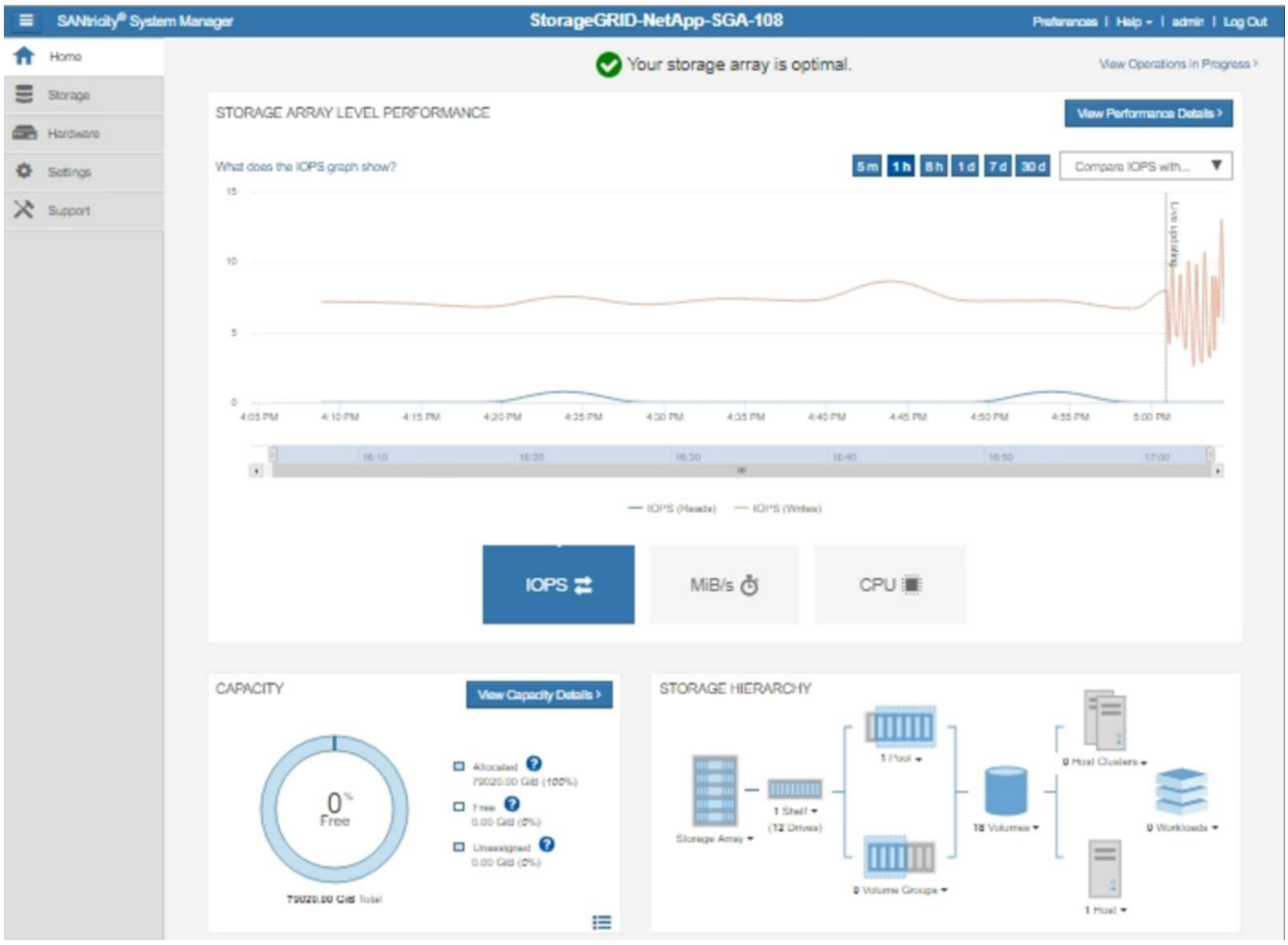
Es posible configurar una dirección de servidor proxy especial en SANtricity System Manager para transmitir paquetes AutoSupport a través de un nodo de administración de StorageGRID sin el uso del puerto de gestión del dispositivo. Los paquetes de AutoSupport transmitidos de esta manera los envía el "Nodo de administración de remitente preferido"y utilizan cualquiera que se "configuración de proxy de administración"haya configurado en Grid Manager.

> Este procedimiento solo es para configurar un servidor proxy StorageGRID para paquetes AutoSupport E-Series. Para obtener más información sobre la configuración de la serie AutoSupport, consulte la "Documentación de SANtricity y E-Series de NetApp".

Pasos

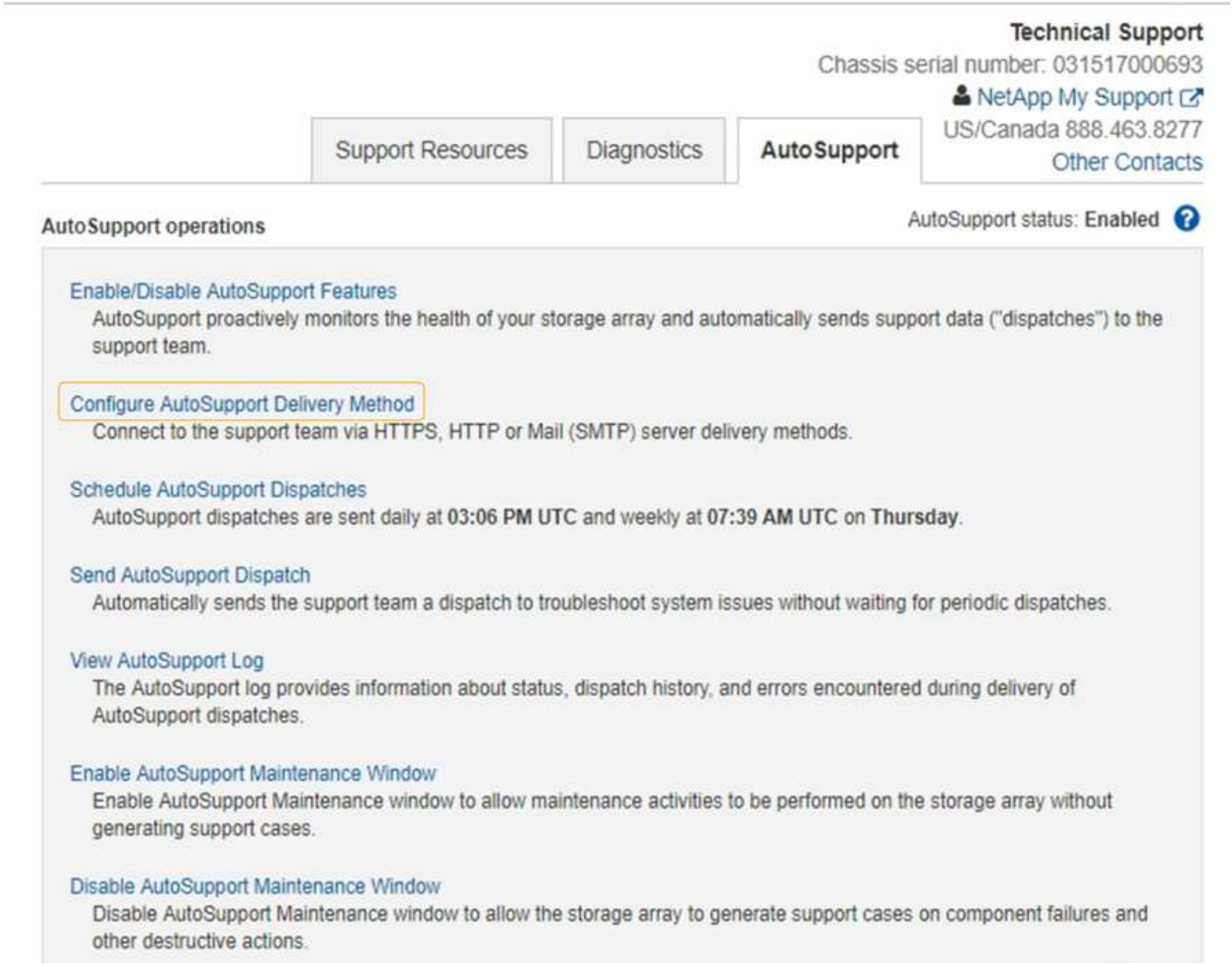
1. En el Administrador de cuadrícula, seleccione **Nodos**.
2. En la lista de nodos que aparece a la izquierda, seleccione el nodo del dispositivo de almacenamiento que desea configurar.
3. Seleccione **Administrador del sistema SANtricity**.

   Se mostrará la página de inicio de SANtricity System Manager.



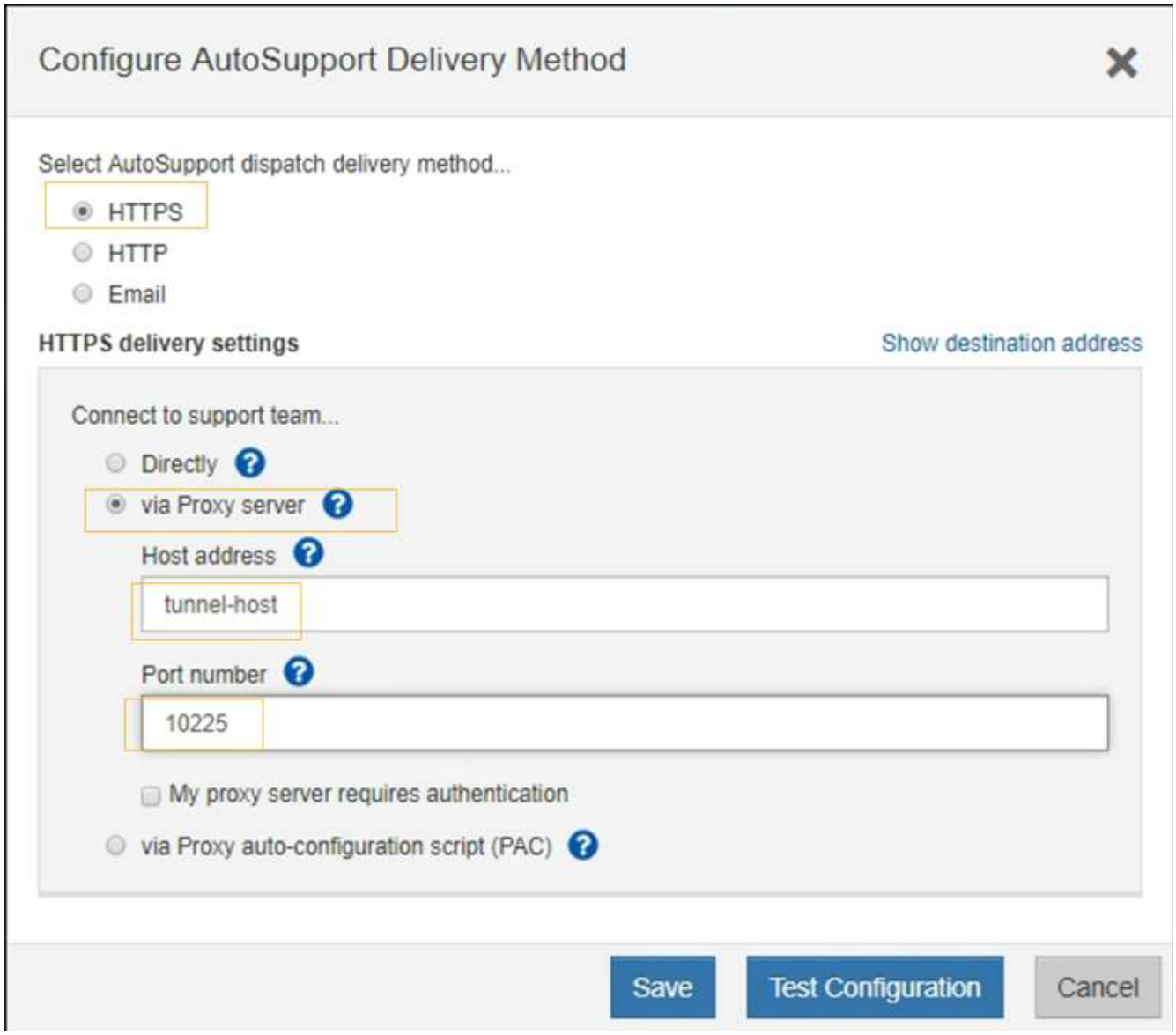
4. Seleccione **Soporte** > **Centro de soporte** > * AutoSupport*.

   Se muestra la página de operaciones AutoSupport.



5. Seleccione **Configurar método de entrega de AutoSupport**.

   Se muestra la página Configurar método de entrega de AutoSupport.



6. Seleccione **HTTPS** para el método de entrega.

   El certificado que habilita HTTPS está preinstalado.

7. Seleccione **a través del servidor proxy**.
8. `tunnel-host`Ingrese para la **Dirección de host**.

   `tunnel-host` Es la dirección especial para usar un nodo de administración para enviar paquetes AutoSupport E-Series.

9. Ingrese `10225` para el **Número de puerto**.

   `10225` Es el número de puerto del servidor proxy StorageGRID que recibe paquetes AutoSupport de la controladora E-Series del dispositivo.

10. Seleccione **Configuración de prueba** para probar el enrutamiento y la configuración del servidor proxy AutoSupport.

    Si es correcto, aparece un mensaje en un banner verde que indica que se ha verificado la configuración

de AutoSupport.

Si la prueba falla, se muestra un mensaje de error en un banner rojo. Compruebe la configuración y la red de DNS de StorageGRID, asegúrese de que el "Nodo de administración de remitente preferido" se pueda conectar al sitio de soporte de NetApp y vuelva a intentar la prueba.

11. Seleccione **Guardar**.

Se guardará la configuración y se mostrará un mensaje de confirmación: Se configuró el método de entrega de AutoSupport.

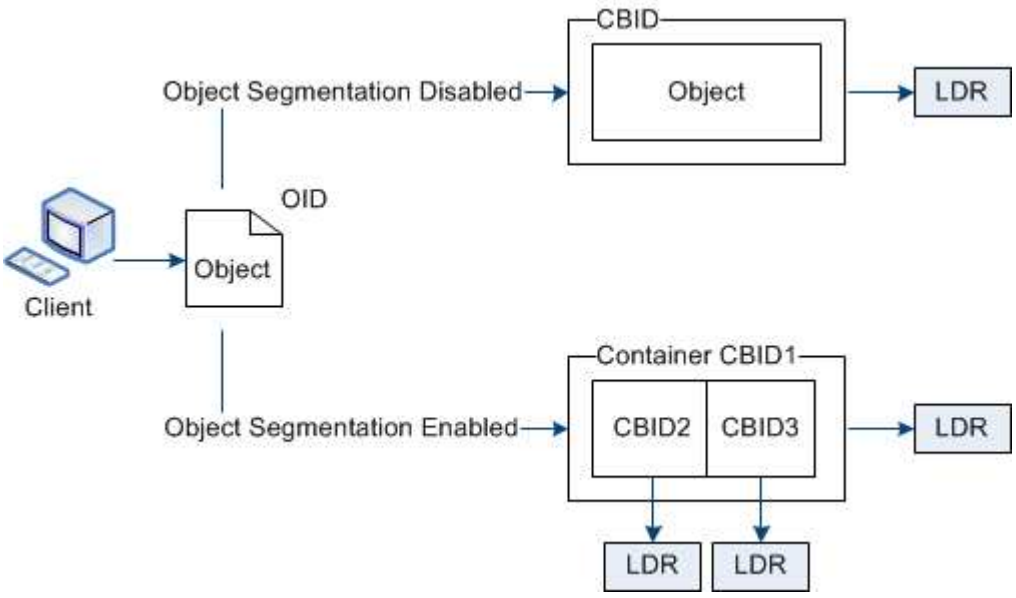
Gestione nodos de almacenamiento

Utilice las opciones de almacenamiento

¿Qué es la segmentación de objetos?

La segmentación de objetos es el proceso de dividir un objeto en una colección de objetos más pequeños de tamaño fijo para optimizar el uso de recursos y almacenamiento para objetos grandes. La carga de varias partes de S3 también crea objetos segmentados, con un objeto que representa cada parte.

Cuando un objeto se procesa en el sistema StorageGRID, el servicio LDR divide el objeto en segmentos y crea un contenedor de segmentos que enumera la información de encabezado de todos los segmentos como contenido.



Al recuperar un contenedor de segmentos, el servicio LDR reúne el objeto original de sus segmentos y devuelve el objeto al cliente.

El contenedor y los segmentos no se almacenan necesariamente en el mismo nodo de almacenamiento. El contenedor y los segmentos pueden almacenarse en cualquier nodo de almacenamiento dentro del pool de almacenamiento especificado en la regla de ILM.

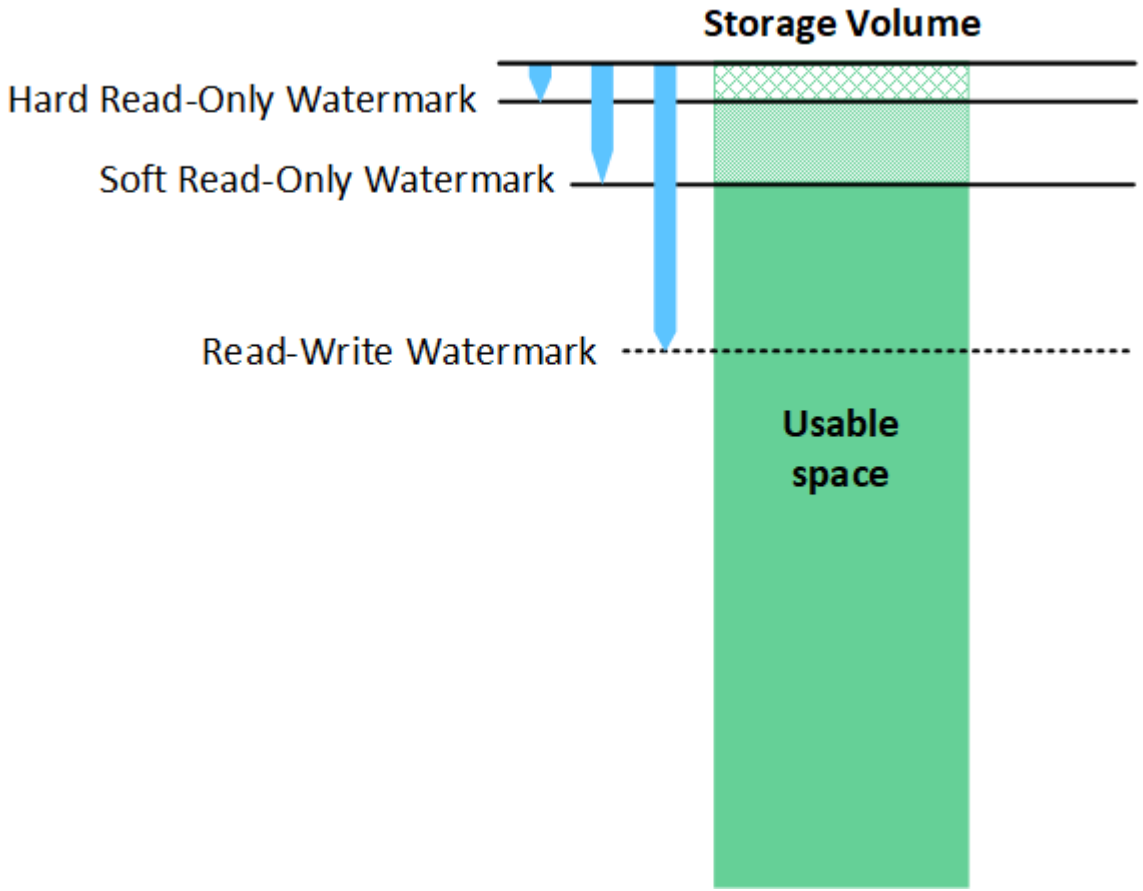
El sistema StorageGRID trata cada segmento de forma independiente y contribuye al recuento de atributos

como objetos gestionados y objetos almacenados. Por ejemplo, si un objeto almacenado en el sistema StorageGRID se divide en dos segmentos, el valor de objetos gestionados aumenta en tres una vez completada la ingesta, de la siguiente manera:

```
segment container + segment 1 + segment 2 = three stored objects
```

¿Qué son las marcas de agua del volumen de almacenamiento?

StorageGRID usa tres marcas de agua de volúmenes de almacenamiento para garantizar que los nodos de almacenamiento pasan de forma segura a un estado de solo lectura antes de que se ejecuten con un espacio mínimo y para permitir que los nodos de almacenamiento que se hayan migrado al estado de solo lectura se vuelvan a escribir.



> Las marcas de agua del volumen de almacenamiento solo se aplican al espacio utilizado para los datos de objetos replicados y codificados por borrado. Para obtener más información acerca del espacio reservado para los metadatos de objetos en el volumen 0, vaya a "Gestione el almacenamiento de metadatos de objetos".

¿Qué es la marca de agua de solo lectura suave?

El **storage volume soft read-only watermark** es la primera marca de agua que indica que el espacio utilizable de un nodo de almacenamiento para los datos de objetos se está llenando.

Si cada volumen de un nodo de almacenamiento tiene menos espacio libre que la marca de agua de solo lectura suave de ese volumen, el nodo de almacenamiento pasa al modo *de solo lectura*. El modo de solo lectura significa que el nodo de almacenamiento anuncia servicios de solo lectura al resto del sistema

StorageGRID, pero completa todas las solicitudes de escritura pendientes.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una marca de agua suave de solo lectura de 10 GB. En cuanto cada volumen tiene menos de 10 GB de espacio libre, el nodo de almacenamiento pasa al modo de solo lectura suave.

¿Cuál es la marca de agua de sólo lectura?

La marca de agua de solo lectura * del volumen de almacenamiento es la siguiente marca de agua para indicar que el espacio utilizable de un nodo para los datos de objetos se está llenando.

Si el espacio libre de un volumen es inferior a la marca de agua de solo lectura fija de ese volumen, se producirá un error al escribir en el volumen. Sin embargo, las escrituras en otros volúmenes pueden continuar hasta que el espacio libre de esos volúmenes sea inferior a sus marcas de agua de solo lectura fija.

Por ejemplo, suponga que cada volumen de un nodo de almacenamiento tiene una marca de agua fija de solo lectura de 5 GB. En cuanto cada volumen tenga menos de 5 GB de espacio libre, el nodo de almacenamiento ya no aceptará ninguna solicitud de escritura.

La marca de agua de sólo lectura dura siempre es inferior a la marca de agua de sólo lectura suave.

¿Qué es la marca de agua de lectura/escritura?

La marca de agua **storage volume read-write** solo se aplica a los nodos de almacenamiento que han pasado al modo de solo lectura. Determina cuándo el nodo puede volver a ser de lectura y escritura. Cuando el espacio libre en cualquier volumen de almacenamiento en un nodo de almacenamiento es mayor que la marca de agua de lectura y escritura de ese volumen, el nodo vuelve a realizar automáticamente la transición al estado de lectura y escritura.

Por ejemplo, supongamos que el nodo de almacenamiento ha pasado al modo de solo lectura. Suponga también que cada volumen tiene una marca de agua de lectura y escritura de 30 GB. En cuanto el espacio libre de cualquier volumen aumente a 30 GB, el nodo volverá a ser de lectura y escritura.

La marca de agua de lectura y escritura es siempre mayor que la marca de agua de sólo lectura y la marca de agua de sólo lectura.

Ver marcas de agua de volumen de almacenamiento

Puede ver los ajustes de Marca de agua actuales y los valores optimizados para el sistema. Si no se utilizan marcas de agua optimizadas, puede determinar si puede o debe ajustar la configuración.

Antes de empezar

- Ha completado la actualización a StorageGRID 11,6 o superior.
- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Usted tiene el "Permiso de acceso raíz".

Ver la configuración actual de la Marca de agua

Puede ver la configuración actual de la Marca de agua de almacenamiento en el Administrador de grid.

Pasos

1. Seleccione **Soporte** > **Otros** > **Marcas de agua de almacenamiento**.
2. En la página Marcas de agua de almacenamiento, consulte la casilla de verificación Utilizar valores

optimizados.

- Si se selecciona la casilla de comprobación, las tres marcas de agua se optimizan para cada volumen de almacenamiento en cada nodo de almacenamiento, según el tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

  Esta es la configuración predeterminada y recomendada. No actualice estos valores. Opcionalmente, puede Vea las marcas de agua de almacenamiento optimizadas.

- Si la casilla de verificación Utilizar valores optimizados no está seleccionada, se están utilizando marcas de agua personalizadas (no optimizadas). No se recomienda utilizar la configuración de Marca de agua personalizada. Utilice las instrucciones para "Solución de problemas de alertas de anulación de Marca de agua de sólo lectura baja"determinar si puede o debe ajustar la configuración.

  Al especificar la configuración de marca de agua personalizada, debe introducir valores mayores que 0.

Ver marcas de agua de almacenamiento optimizadas

StorageGRID usa dos métricas de Prometheus para mostrar los valores optimizados que ha calculado para la marca de agua variable de solo lectura del volumen de almacenamiento. Puede ver los valores mínimos y máximos optimizados para cada nodo de almacenamiento en la cuadrícula.

1. Seleccione **Soporte** > **Herramientas** > **Métricas**.
2. En la sección Prometheus, seleccione el enlace para acceder a la interfaz de usuario de Prometheus.
3. Para ver la Marca de agua blanda de sólo lectura recomendada, introduzca la siguiente métrica Prometheus y seleccione **Ejecutar**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   La última columna muestra el valor mínimo optimizado de la marca de agua soft de solo lectura para todos los volúmenes de almacenamiento en cada nodo de almacenamiento. Si este valor es mayor que la configuración personalizada para la marca de agua de solo lectura suave del volumen de almacenamiento, se activa la alerta **Baja anulación de marca de agua de solo lectura** para el nodo de almacenamiento.

4. Para ver la Marca de agua blanda de sólo lectura recomendada, introduzca la siguiente métrica Prometheus y seleccione **Ejecutar**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   La última columna muestra el valor máximo optimizado de la marca de agua soft read-only para todos los volúmenes de almacenamiento en cada nodo de almacenamiento.

Gestione el almacenamiento de metadatos de objetos

La capacidad de metadatos de objetos de un sistema StorageGRID controla la cantidad máxima de objetos que se pueden almacenar en ese sistema. Para garantizar que el sistema StorageGRID tenga espacio suficiente para almacenar objetos nuevos, debe comprender dónde y cómo StorageGRID almacena los metadatos de objetos.

¿Qué son los metadatos de objetos?

Los metadatos de objetos son cualquier información que describa un objeto. StorageGRID utiliza metadatos de objetos para realizar un seguimiento de las ubicaciones de todos los objetos en el grid y gestionar el ciclo de vida de cada objeto a lo largo del tiempo.

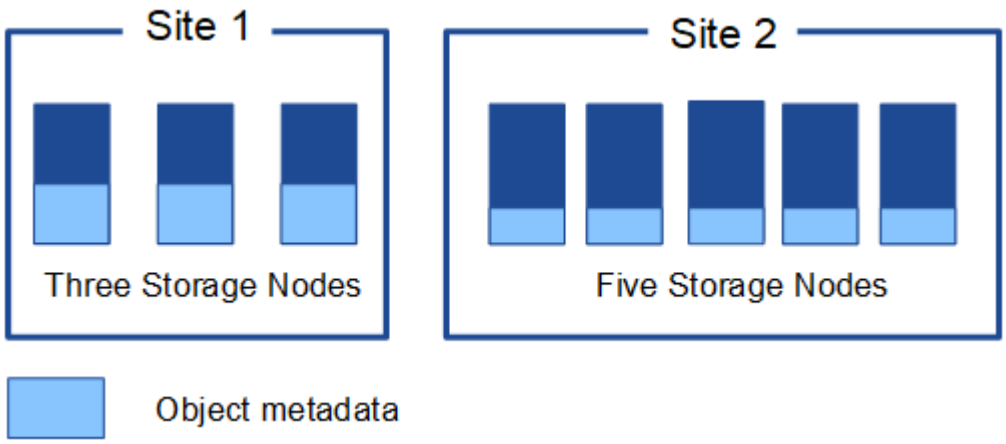
Para un objeto en StorageGRID, los metadatos de objeto incluyen los siguientes tipos de información:

- Metadatos del sistema, incluido un ID único para cada objeto (UUID), el nombre del objeto, el nombre del bloque S3, el nombre o ID de cuenta de inquilino, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez y la fecha y hora en que se modificó el objeto por última vez.
- Todos los pares de valor de clave de metadatos de usuario personalizados asociados con el objeto.
- Para los objetos S3, cualquier par de etiqueta de objeto clave-valor asociado al objeto.
- Para las copias de objetos replicadas, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos codificados de borrado, la ubicación actual de almacenamiento de cada fragmento.
- Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluido el nombre del bloque externo y el identificador único del objeto.
- Para objetos segmentados y objetos multipartes, identificadores de segmentos y tamaños de datos.

¿Cómo se almacenan los metadatos de objetos?

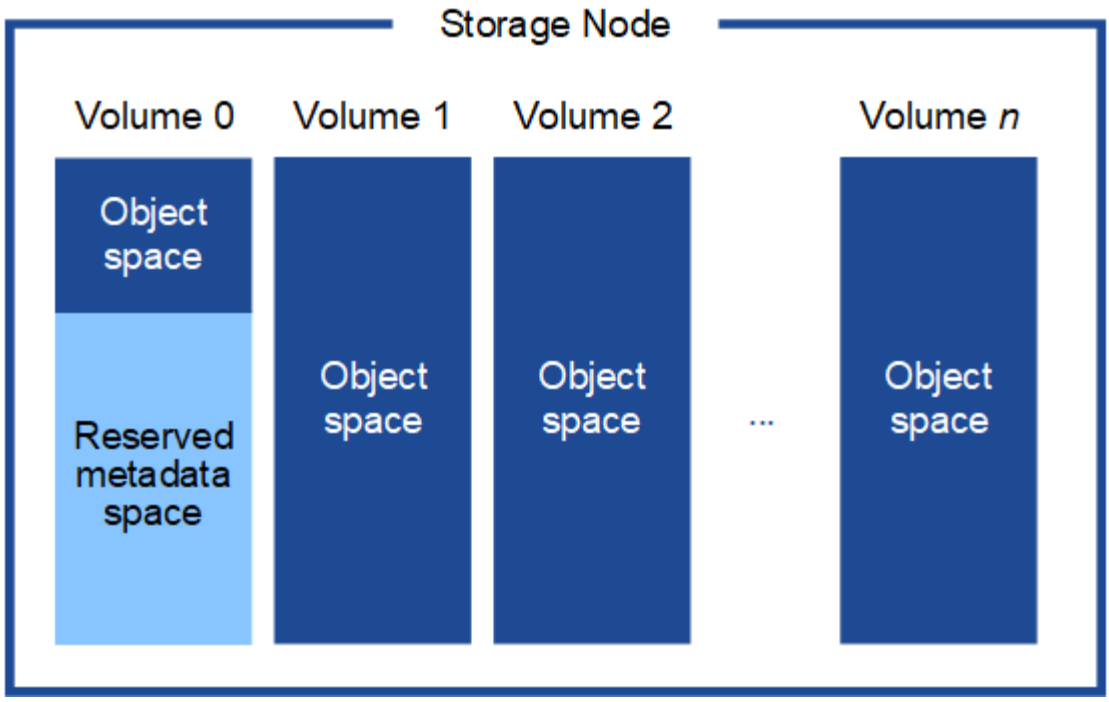
StorageGRID mantiene los metadatos de objetos en una base de datos de Cassandra, que se almacena independientemente de los datos de objetos. Para proporcionar redundancia y proteger los metadatos de objetos de la pérdida, StorageGRID almacena tres copias de los metadatos para todos los objetos del sistema en cada sitio.

Esta figura representa los nodos de almacenamiento de dos sitios. Cada sitio tiene la misma cantidad de metadatos de objeto y los metadatos de cada sitio se subdividen entre todos los nodos de almacenamiento de ese sitio.



¿Dónde se almacenan los metadatos de objetos?

En esta figura, se representan los volúmenes de almacenamiento para un único nodo de almacenamiento.



Como se muestra en la figura, StorageGRID reserva espacio para los metadatos del objeto en el volumen de almacenamiento 0 de cada nodo de almacenamiento. Utiliza el espacio reservado para almacenar metadatos de objetos y realizar operaciones esenciales de la base de datos. Cualquier espacio restante en el volumen de almacenamiento 0 y todos los demás volúmenes de almacenamiento del nodo de almacenamiento se utilizan exclusivamente para los datos de objetos (copias replicadas y fragmentos codificados de borrado).

La cantidad de espacio reservado para los metadatos de objeto en un nodo de almacenamiento en particular depende de varios factores, que se describen a continuación.

Valor de espacio reservado de metadatos

El *Metadata reserved space* es un valor para todo el sistema que representa la cantidad de espacio que se reservará para los metadatos en el volumen 0 de cada nodo de almacenamiento. Como se muestra en la tabla, el valor predeterminado de esta configuración se basa en:

- La versión de software que estaba utilizando cuando instaló inicialmente StorageGRID.
- La cantidad de RAM en cada nodo de almacenamiento.

Versión utilizada para la instalación inicial de StorageGRID	Cantidad de RAM en los nodos de almacenamiento	Valor predeterminado de espacio reservado de metadatos
11,5 a 12,0	128 GB o más en cada nodo de almacenamiento del grid	8 TB (8.000 GB)
	Debe haber menos de 128 GB en cualquier nodo de almacenamiento del grid	3 TB (3.000 GB)
11,1 a 11,4	128 GB o más en cada nodo de almacenamiento en un sitio	4 TB (4.000 GB)

Versión utilizada para la instalación inicial de StorageGRID	Cantidad de RAM en los nodos de almacenamiento	Valor predeterminado de espacio reservado de metadatos
	Menos de 128 GB en cualquier nodo de almacenamiento de cada sitio	3 TB (3.000 GB)
11,0 o anterior	Cualquier cantidad	2 TB (2.000 GB)

Ver valor de espacio reservado de metadatos

Siga estos pasos para ver la configuración de espacio reservado de metadatos para el sistema StorageGRID.

Pasos

1. Seleccione **Configuración** > **Sistema** > **Configuración de almacenamiento**.
2. En la página Configuración de almacenamiento, expanda la sección **Espacio reservado de metadatos**.

Para StorageGRID 11,8 o superior, el valor del espacio reservado de metadatos debe ser de al menos 100 GB y no más de 1 PB.

La configuración predeterminada para una nueva instalación de StorageGRID 11,6 o superior en la que cada nodo de almacenamiento tiene 128 GB o más de RAM es 8.000 GB (8 TB).

Espacio reservado real para los metadatos

En contraste con la configuración de espacio reservado de metadatos del sistema, el *espacio reservado real* para los metadatos del objeto se determina para cada nodo de almacenamiento. Para cualquier nodo de almacenamiento determinado, el espacio reservado real para los metadatos depende del tamaño del volumen 0 para el nodo y de la configuración de espacio reservado de metadatos en todo el sistema.

El tamaño del volumen 0 para el nodo	Espacio reservado real para los metadatos
Menos de 500 GB (uso fuera de producción)	10% del volumen 0
500 GB o más + o + Nodos de almacenamiento de sólo metadatos	El menor de estos valores: • Volumen 0 • Valor de espacio reservado de metadatos **Nota**: Solo se requiere un rangedb para los nodos de almacenamiento solo de metadatos.

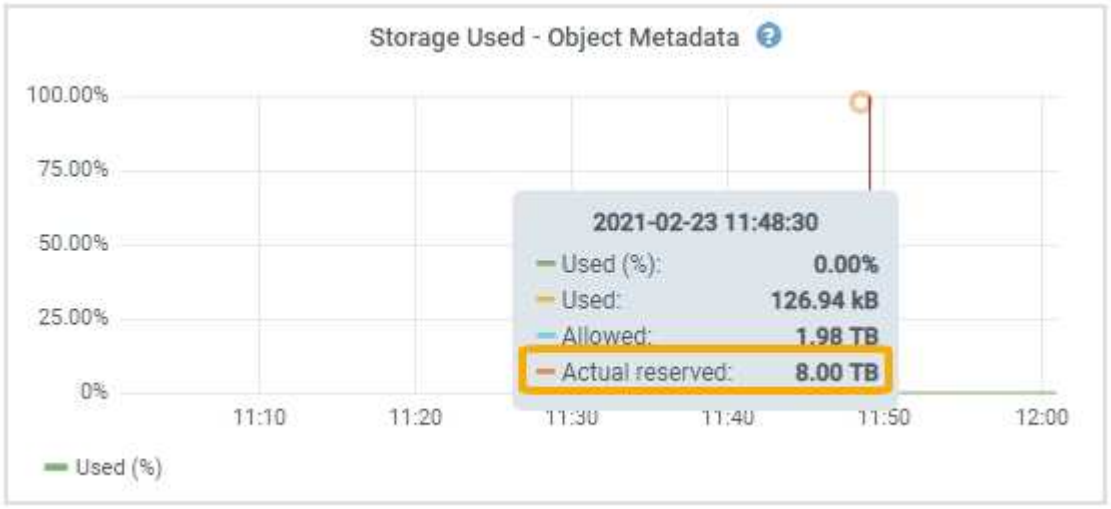
Ver el espacio reservado real para metadatos

Siga estos pasos para ver el espacio reservado real para metadatos en un nodo de almacenamiento en particular.

Pasos

1. Desde el Administrador de cuadrícula, seleccione **Nodos** > ***Nodo de almacenamiento***.

2. Seleccione la ficha **almacenamiento**.
3. Coloque el cursor sobre el gráfico Almacenamiento usado - Metadatos de objetos y localice el valor **Real reserved**.



En la captura de pantalla, el valor **Real reservado** es 8 TB. Esta captura de pantalla es para un nodo de almacenamiento grande en una nueva instalación de StorageGRID 11.6. Debido a que el valor de espacio reservado de metadatos del sistema es menor que el volumen 0 para este nodo de almacenamiento, el espacio reservado real para este nodo es igual al valor de espacio reservado de metadatos.

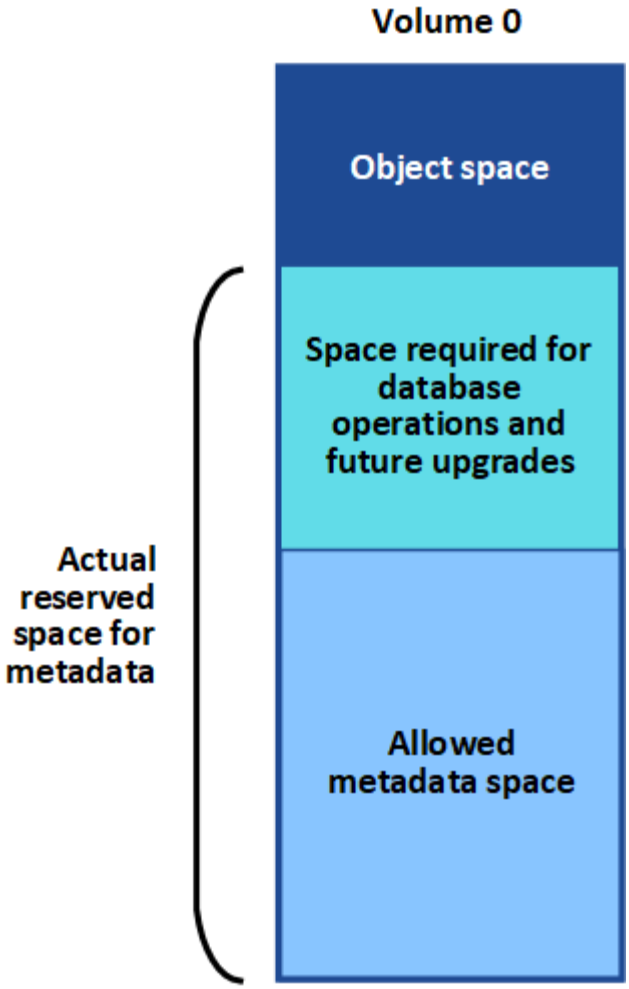
Ejemplo de espacio de metadatos reservado real

Suponga que instala un nuevo sistema StorageGRID mediante la versión 11,7 o posterior. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Según estos valores:

- El espacio reservado **Metadatos** para todo el sistema se establece en 8 TB. (Este es el valor predeterminado para una nueva instalación de StorageGRID 11,6 o superior si cada nodo de almacenamiento tiene más de 128 GB de RAM).
- El espacio reservado real para los metadatos de SN1 es de 6 TB. (Todo el volumen está reservado porque el volumen 0 es más pequeño que el ajuste **Metadatos de espacio reservado**).

Espacio de metadatos permitido

El espacio reservado real de cada nodo de almacenamiento para metadatos se subdivide en el espacio disponible para los metadatos del objeto (el *espacio de metadatos permitido*) y el espacio necesario para las operaciones esenciales de la base de datos (como compactación y reparación) y las futuras actualizaciones de hardware y software. El espacio de metadatos permitido rige la capacidad general del objeto.



En la tabla siguiente se muestra cómo StorageGRID calcula el **espacio de metadatos permitido** para diferentes nodos de almacenamiento, en función de la cantidad de memoria del nodo y del espacio reservado real para los metadatos.

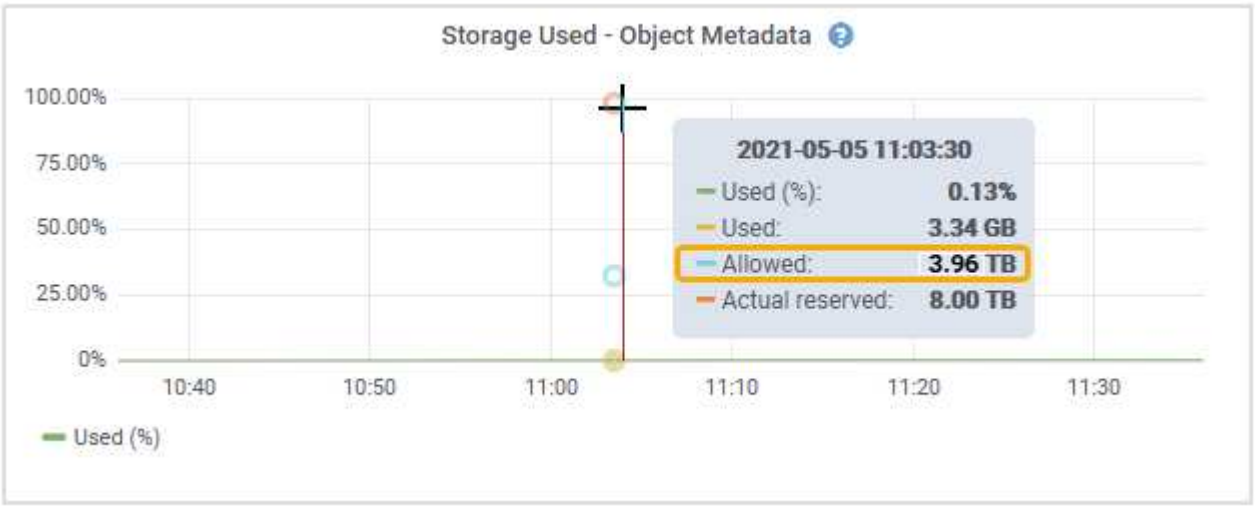
		Cantidad de memoria en el nodo de almacenamiento	
	< 128 GB	>= 128 GB	**Espacio reservado real para metadatos**
⇐ 4 TB	60 % del espacio reservado real para metadatos, hasta un máximo de 1,32 TB	60 % del espacio reservado real para metadatos, hasta un máximo de 1,98 TB	4 TB

Ver el espacio de metadatos permitido

Siga estos pasos para ver el espacio de metadatos permitido para un nodo de almacenamiento.

Pasos

1. Desde el Administrador de cuadrícula, seleccione **Nodos**.
2. Seleccione el nodo de almacenamiento.
3. Seleccione la ficha **almacenamiento**.
4. Coloque el cursor sobre el gráfico de metadatos de objetos Storage Used y localice el valor **Allowed**.



En la captura de pantalla, el valor **Permitido** es 3,96 TB, que es el valor máximo para un nodo de almacenamiento cuyo espacio reservado real para metadatos es superior a 4 TB.

El valor **permitido** corresponde a esta métrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Ejemplo de espacio de metadatos permitido

Supongamos que instala un sistema StorageGRID mediante la versión 11.6. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Según estos valores:

- El espacio reservado **Metadatos** para todo el sistema se establece en 8 TB. (Este es el valor predeterminado para StorageGRID 11,6 o superior cuando cada nodo de almacenamiento tiene más de 128 GB de RAM.)
- El espacio reservado real para los metadatos de SN1 es de 6 TB. (Todo el volumen está reservado porque el volumen 0 es más pequeño que el ajuste **Metadatos de espacio reservado**).
- El espacio permitido para metadatos en SN1 es de 3 TB, según el cálculo mostrado en la tabla para el espacio permitido para los metadatos: (espacio reservado real para metadatos − 1 TB) x 60%, hasta un máximo de 3,96 TB.

Cómo afectan los nodos de almacenamiento de diferentes tamaños a la capacidad de objetos

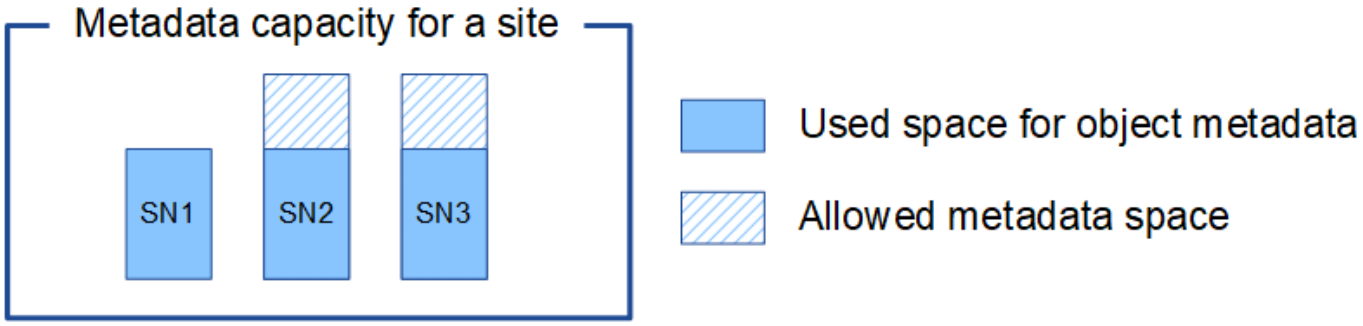
Como se ha descrito anteriormente, StorageGRID distribuye uniformemente los metadatos de objetos de los nodos de almacenamiento de cada sitio. Por este motivo, si un sitio contiene nodos de almacenamiento de distintos tamaños, el nodo más pequeño del sitio determina la capacidad de metadatos del sitio.

Observe el siguiente ejemplo:

- Hay una cuadrícula de un solo sitio que contiene tres nodos de almacenamiento de distintos tamaños.
- La configuración de espacio reservado **Metadatos** es de 4 TB.
- Los nodos de almacenamiento tienen los siguientes valores para el espacio de metadatos reservado real y el espacio de metadatos permitido.

Nodo de almacenamiento	Tamaño del volumen 0	Espacio real de metadatos reservado	Espacio de metadatos permitido
SN1	2,2TB	2,2TB	1,32TB
SN2	5TB	4TB	1,98TB
SN3	6TB	4TB	1,98TB

Como los metadatos de objetos se distribuyen uniformemente por los nodos de almacenamiento de un sitio, cada nodo de este ejemplo solo puede contener 1.32 TB de metadatos. No se pueden utilizar los 0,66 TB adicionales de espacio permitido para SN2 y SN3.



De igual modo, como StorageGRID mantiene todos los metadatos de objetos para un sistema StorageGRID en cada sitio, la capacidad general de metadatos de un sistema StorageGRID viene determinada por la capacidad de metadatos de objetos del sitio más pequeño.

Además, dado que la capacidad de metadatos de los objetos controla el recuento máximo de objetos, cuando un nodo se queda sin capacidad de metadatos, el grid está lleno de eficacia.

Información relacionada

- Para obtener información sobre cómo supervisar la capacidad de metadatos del objeto para cada nodo de almacenamiento, consulte las instrucciones para "Supervisión de StorageGRID".
- Para aumentar la capacidad de metadatos de objeto para el sistema "expanda una cuadrícula"mediante la adición de nuevos nodos de almacenamiento.

Aumentar el espacio reservado de metadatos

Es posible que pueda aumentar la configuración del sistema de espacio reservado de metadatos si los nodos de almacenamiento cumplen con los requisitos específicos de RAM y espacio disponible.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".

- Tú tienes el"Permiso de acceso root o permiso de configuración de otra red" .

Acerca de esta tarea

Es posible que pueda aumentar manualmente la configuración del espacio reservado de metadatos en todo el sistema hasta 8 TB.

Sólo puede aumentar el valor de la configuración espacio reservado de metadatos para todo el sistema si ambas sentencias son verdaderas:

- Los nodos de almacenamiento de cualquier sitio del sistema tienen 128 GB o más de RAM.
- Los nodos de almacenamiento de cualquier sitio del sistema tienen suficiente espacio disponible en el volumen de almacenamiento 0.

Tenga en cuenta que, si aumenta esta configuración, reducirá al mismo tiempo el espacio disponible para el almacenamiento de objetos en el volumen de almacenamiento 0 de todos los nodos de almacenamiento. Por este motivo, es posible que prefiera establecer el espacio reservado de metadatos en un valor inferior a 8 TB, según sus requisitos esperados de metadatos de objetos.

> En general, es mejor utilizar un valor más alto en lugar de uno más bajo. Si la configuración espacio reservado de metadatos es demasiado grande, puede disminuirla más adelante. Por el contrario, si aumenta el valor más adelante, es posible que el sistema necesite mover datos de objetos para liberar espacio.

Para obtener una explicación detallada de cómo el valor de Espacio Reservado de Metadatos afecta al espacio permitido para el almacenamiento de metadatos de objetos en un nodo de almacenamiento concreto, consulte "Gestione el almacenamiento de metadatos de objetos".

Pasos

1. Determine la configuración actual del espacio reservado de metadatos.
   a. Seleccione **Configuración** > **Sistema** > **Configuración de almacenamiento**.
   b. Tenga en cuenta el valor de **Espacio reservado para metadatos**.
2. Asegúrese de tener suficiente espacio disponible en el volumen de almacenamiento 0 de cada nodo de almacenamiento para aumentar este valor.
   a. Seleccionar **Nodos**.
   b. Seleccione el primer nodo de almacenamiento de la cuadrícula.
   c. Seleccione la pestaña almacenamiento.
   d. En la sección de volúmenes, localice la entrada **/var/local/rangedb/0**.
   e. Confirme que el valor disponible es igual o mayor que la diferencia entre el nuevo valor que desea utilizar y el valor espacio reservado de metadatos actual.

      Por ejemplo, si la configuración de espacio reservado de metadatos es actualmente 4 TB y desea aumentarla a 6 TB, el valor disponible debe ser 2 TB o superior.

   f. Repita estos pasos para todos los nodos de almacenamiento.
      - Si uno o más nodos de almacenamiento no tienen suficiente espacio disponible, no se puede aumentar el valor del espacio reservado de metadatos. No continúe con este procedimiento.
      - Si cada nodo de almacenamiento tiene suficiente espacio disponible en el volumen 0, vaya al paso siguiente.

3. Asegúrese de tener al menos 128 GB de RAM en cada nodo de almacenamiento.
   a. Seleccionar **Nodos**.
   b. Seleccione el primer nodo de almacenamiento de la cuadrícula.
   c. Seleccione la ficha **hardware**.
   d. Pase el cursor sobre el gráfico uso de memoria. Asegúrese de que **memoria total** es de al menos 128 GB.
   e. Repita estos pasos para todos los nodos de almacenamiento.
      - Si uno o más nodos de almacenamiento no tienen suficiente memoria total disponible, no es posible aumentar el valor del espacio reservado de metadatos. No continúe con este procedimiento.
      - Si cada nodo de almacenamiento tiene al menos 128 GB de memoria total, vaya al siguiente paso.
4. Actualice la configuración espacio reservado de metadatos.
   a. Seleccione **Configuración** > **Sistema** > **Configuración de almacenamiento**.
   b. Seleccione **Espacio reservado para metadatos**.
   c. Introduzca el nuevo valor.

      Por ejemplo, para introducir 8 TB, que es el valor máximo admitido, introduzca **8000000000000** (8, seguido de 12 ceros)

   d. Seleccione **Guardar**.

Comprimir objetos almacenados

Es posible habilitar la compresión de objetos para reducir el tamaño de los objetos almacenados en StorageGRID, de modo que los objetos consuman menos almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "permisos de acceso específicos".

Acerca de esta tarea

De forma predeterminada, la compresión de objetos está deshabilitada. Si habilita la compresión, StorageGRID intenta comprimir cada objeto al guardarlo, utilizando la compresión sin pérdidas.

> Si cambia este ajuste, el nuevo ajuste tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para el rendimiento y el escalado.

Antes de habilitar la compresión de objetos, tenga en cuenta lo siguiente:

- No debe seleccionar **Comprimir objetos almacenados** a menos que sepa que los datos almacenados son comprimibles.
- Las aplicaciones que guardan objetos en StorageGRID pueden comprimir objetos antes de guardarlos. Si una aplicación cliente ya ha comprimido un objeto antes de guardarlo en StorageGRID, al seleccionar esta opción no se reducirá aún más el tamaño de un objeto.
- No seleccione **Comprimir objetos almacenados** si utiliza NetApp FabricPool con StorageGRID.

- Si se selecciona **Comprimir objetos almacenados**, las aplicaciones cliente S3 deben evitar realizar operaciones GetObject que especifiquen un rango de bytes que se devolverán. Estas operaciones de «lectura de rango» son ineficientes, puesto que StorageGRID debe descomprimir los objetos de forma efectiva para acceder a los bytes solicitados. Las operaciones GetObject que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, no es eficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

  Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden tener un tiempo de espera.

  > Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

Pasos

1. Seleccione **Configuración** > **Sistema** > **Configuración de almacenamiento** > **Compresión de objetos**.
2. Seleccione la casilla de verificación **Comprimir objetos almacenados**.
3. Seleccione **Guardar**.

Gestione nodos de almacenamiento completos

A medida que los nodos de almacenamiento alcancen la capacidad, debe ampliar el sistema StorageGRID añadiendo almacenamiento nuevo. Hay tres opciones disponibles: Añadir volúmenes de almacenamiento, añadir bandejas de ampliación de almacenamiento y añadir nodos de almacenamiento.

Añadir volúmenes de almacenamiento

Cada nodo de almacenamiento es compatible con un número máximo de volúmenes de almacenamiento. El máximo definido varía según la plataforma. Si un nodo de almacenamiento contiene menos de la cantidad máxima de volúmenes de almacenamiento, es posible añadir volúmenes para aumentar su capacidad. Consulte las instrucciones para "Expandir un sistema StorageGRID".

Añada bandejas de ampliación del almacenamiento

Algunos nodos de almacenamiento de los dispositivos StorageGRID, como SG6060 o SG6160, pueden admitir bandejas de almacenamiento adicionales. Si tiene dispositivos StorageGRID con funcionalidades de expansión que todavía no se han expandido hasta la máxima capacidad, se pueden añadir bandejas de almacenamiento para aumentar la capacidad. Consulte las instrucciones para "Expandir un sistema StorageGRID".

Añada nodos de almacenamiento

Puede aumentar la capacidad de almacenamiento con la adición de nodos de almacenamiento. Al añadir almacenamiento, deben tenerse en cuenta las reglas de ILM activas y los requisitos de capacidad. Consulte las instrucciones para "Expandir un sistema StorageGRID".

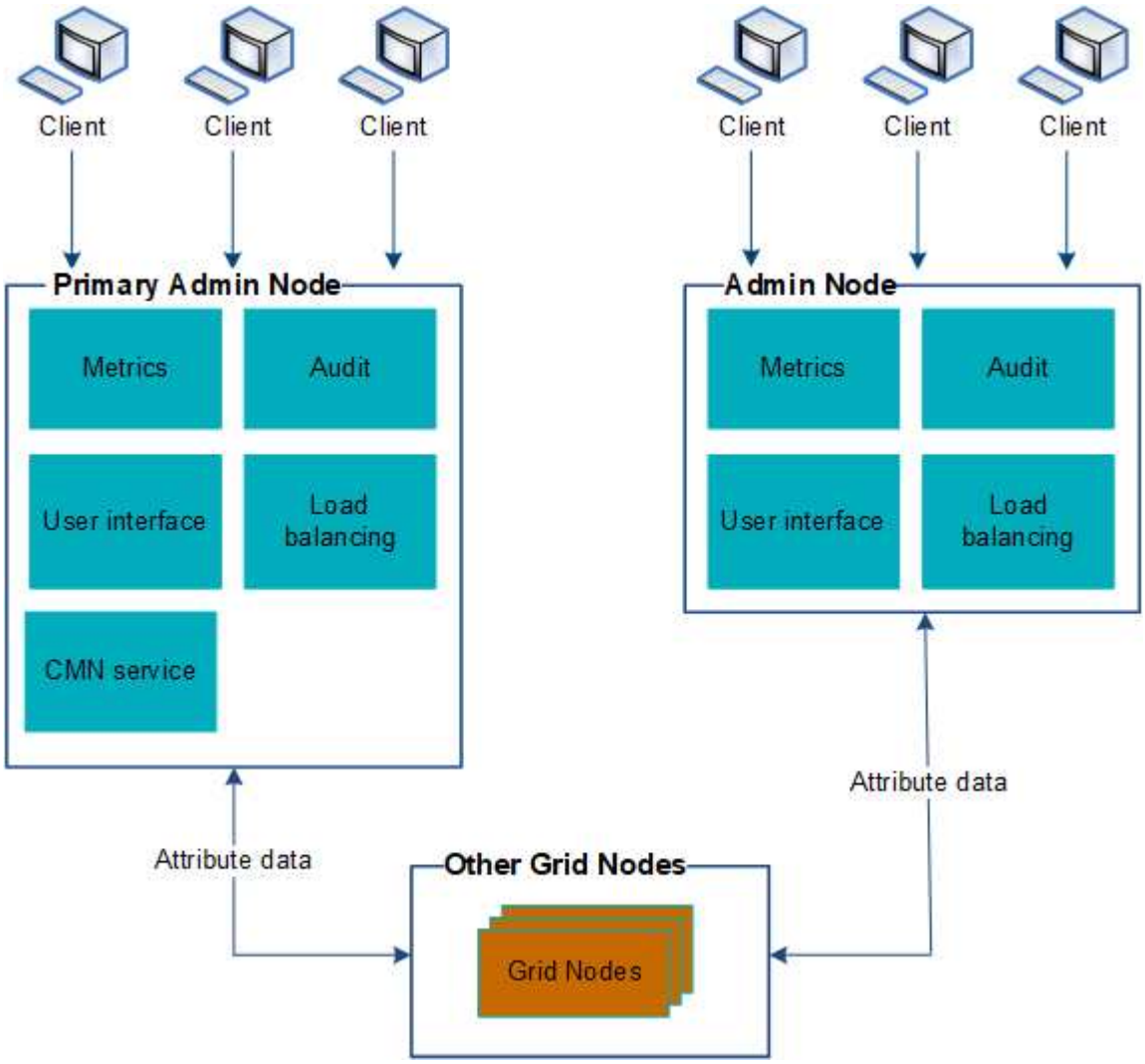
Gestione los nodos de administrador

Use varios nodos de administrador

Un sistema StorageGRID puede incluir varios nodos de administrador para permitir

supervisar y configurar continuamente el sistema StorageGRID incluso si falla un nodo de administración.

Si un nodo de administración deja de estar disponible, el procesamiento de atributos continúa, las alertas siguen activándose y las notificaciones por correo electrónico y los paquetes de AutoSupport aún se envían. Sin embargo, tener varios nodos de administración no ofrece protección de conmutación al nodo de respaldo, excepto notificaciones y paquetes de AutoSupport.



Si falla un nodo de administración, existen dos opciones para ver y configurar el sistema StorageGRID:

- Los clientes web pueden volver a conectarse a cualquier otro nodo de administrador disponible.
- Si un administrador del sistema ha configurado un grupo de nodos de administración de alta disponibilidad, los clientes web pueden seguir accediendo a Grid Manager o al Gestor de inquilinos mediante la dirección IP virtual del grupo de alta disponibilidad. Consulte "Gestión de grupos de alta disponibilidad".

> Al utilizar un grupo de alta disponibilidad, el acceso se interrumpe si el nodo de administración activo falla. Los usuarios deben volver a iniciar sesión después de que la dirección IP virtual del grupo ha conmute a otro nodo de administración del grupo.

Algunas tareas de mantenimiento solo se pueden realizar con el nodo de administrador principal. Si el nodo de

administración principal falla, debe recuperarse antes de que el sistema StorageGRID vuelva a funcionar completamente.

Identifique el nodo de administración principal

El nodo de administración principal proporciona más funcionalidad que los nodos de administración no principales. Por ejemplo, algunos procedimientos de mantenimiento se deben realizar utilizando el nodo de administración principal.

Para obtener más información sobre los nodos de administración, consulte "Qué es un nodo de administración".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "navegador web compatible".
- Tienes "permisos de acceso específicos".

Pasos

1. Seleccionar **Nodos**.
2. Introduzca **primary** en el cuadro de búsqueda.

   En los resultados de la búsqueda, identifique el nodo con el nodo de administración principal que aparece en la columna Tipo. Debe aparecer un nodo de administración principal.