Administrar StorageGRID

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-120/admin/index.html on July 23, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Administrar StorageGRID . . . 1
- Administrar StorageGRID . . . 1
  - ${post_edited_translations.segment} . . . 1
  - Antes de empezar . . . 1
- ${post_edited_translations.segment} . . . 1
  - Requisitos del navegador web para StorageGRID . . . 1
  - ${post_edited_translations.segment} . . . 2
  - Sign out de StorageGRID Grid Manager . . . 4
  - Cambia tu contraseña de StorageGRID Grid Manager . . . 4
  - Ver la información de la licencia de StorageGRID . . . 5
  - Actualizar la información de la licencia de StorageGRID . . . 6
  - Usa la API . . . 6
- Controlar el acceso a StorageGRID . . . 28
  - Controlar el acceso a StorageGRID . . . 28
  - Cambia la contraseña de aprovisionamiento de StorageGRID . . . 29
  - Cambia las contraseñas de la consola de nodo en StorageGRID . . . 29
  - Cambia las contraseñas de acceso SSH para StorageGRID Admin Nodes . . . 32
  - Usa la federación de identidades en StorageGRID . . . 34
  - Administra grupos de administración en StorageGRID . . . 39
  - Permisos del grupo Admin en StorageGRID . . . 42
  - Administra usuarios en StorageGRID . . . 45
  - Utiliza el inicio de sesión único (SSO) . . . 48
- ${post_edited_translations.segment} . . . 73
  - Conoce la federación de grid de StorageGRID . . . 73
  - Conoce la clonación de cuentas en StorageGRID . . . 76
  - Conoce la replicación entre grids en StorageGRID . . . 79
  - Compara la replicación entre grids y la replicación CloudMirror en StorageGRID . . . 86
  - Crear conexiones de federación de grid StorageGRID . . . 88
  - Administra las conexiones de la federación de grid de StorageGRID . . . 91
  - Administra los inquilinos permitidos para la federación de grid de StorageGRID . . . 96
  - Soluciona errores de federación de grid en StorageGRID . . . 102
  - Identifica y vuelve a intentar las operaciones de replicación fallidas de StorageGRID . . . 107
- Gestiona la seguridad . . . 111
  - Administra la seguridad en StorageGRID . . . 111
  - Revisa los métodos de cifrado de StorageGRID . . . 112
  - Gestiona certificados . . . 115
  - Configura los ajustes de seguridad . . . 148
  - Configura servidores de gestión de claves . . . 154
  - Gestiona la configuración del proxy . . . 174
  - Controla los cortafuegos . . . 175
- Gestiona inquilinos . . . 182
  - Cuentas de tenant en StorageGRID . . . 182
  - Crear una cuenta de inquilino de StorageGRID . . . 184

Editar una cuenta de inquilino de StorageGRID . . . 189
Cambiar la contraseña del usuario raíz local de un tenant de StorageGRID . . . 191
Eliminar una cuenta de inquilino de StorageGRID . . . 191
${post_edited_translations.segment} . . . 192
Administra S3 Select para cuentas de inquilinos en StorageGRID . . . 201
Configura las conexiones de los clientes . . . 202
Configura conexiones de cliente S3 a StorageGRID . . . 202
Seguridad para clientes S3 en StorageGRID . . . 204
Usa el asistente de configuración de S3 . . . 206
Gestiona grupos de alta disponibilidad . . . 215
Gestiona el equilibrio de carga . . . 226
Configura los nombres de dominio del endpoint S3 en StorageGRID . . . 241
Direcciones IP y puertos para conexiones de cliente de StorageGRID . . . 243
Gestiona redes y conexiones . . . 245
Configura los ajustes de red de StorageGRID . . . 245
Directrices para redes StorageGRID . . . 245
Ver direcciones IP en StorageGRID . . . 247
Configura interfaces VLAN en StorageGRID . . . 248
${post_edited_translations.segment} . . . 252
Gestiona las políticas de clasificación del tráfico . . . 253
Cifrados admitidos para conexiones TLS salientes en StorageGRID . . . 260
Beneficios de las conexiones HTTP activas, inactivas y concurrentes en StorageGRID . . . 260
Administra los costes de enlace en StorageGRID . . . 262
Usa AutoSupport . . . 264
Conoce AutoSupport en StorageGRID . . . 264
Configura AutoSupport en StorageGRID . . . 269
Activar manualmente un paquete de AutoSupport en StorageGRID . . . 273
Soluciona problemas de los paquetes StorageGRID AutoSupport . . . 274
Envía paquetes de E-Series AutoSupport a través de StorageGRID . . . 275
${post_edited_translations.segment} . . . 279
${post_edited_translations.segment} . . . 279
Administra el almacenamiento de metadatos de objetos en StorageGRID . . . 282
Aumenta la configuración de espacio reservado para metadatos en StorageGRID . . . 289
Comprime objetos almacenados en StorageGRID . . . 291
Gestiona nodos de almacenamiento completos en StorageGRID . . . 292
Gestionar nodos de administración . . . 292
Usa varios nodos de administración en StorageGRID . . . 292
Identifica el nodo de administración principal en StorageGRID . . . 293

Administrar StorageGRID

Administrar StorageGRID

Sigue estas instrucciones para configurar y administrar un sistema StorageGRID.

${post_edited_translations.segment}

Las tareas principales para configurar y administrar StorageGRID te permiten:

- Utiliza el Grid Manager para configurar grupos y usuarios
- Crea cuentas de inquilino para permitir que las aplicaciones cliente de S3 almacenen y recuperen objetos
- ${post_edited_translations.segment}
- Configura AutoSupport
- Gestiona la configuración del nodo

Antes de empezar

- Tienes un conocimiento general del sistema StorageGRID.
- ${post_edited_translations.segment}

${post_edited_translations.segment}

Requisitos del navegador web para StorageGRID

Debes utilizar un navegador web compatible.

Navegador web	Versión mínima compatible
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Ajusta el ancho de la ventana del navegador al recomendado.

Ancho del navegador	${post_edited_translations.segment}
Mínimo	1024
Óptimo	1280

${post_edited_translations.segment}

Accedes a la página de inicio de sesión de Grid Manager introduciendo el nombre de dominio completo (FQDN) o la dirección IP de un nodo de administración en la barra de direcciones de un navegador web compatible.

Cada sistema StorageGRID incluye un nodo de administración principal y cualquier número de nodos de administración no principales. Puedes iniciar sesión en el Grid Manager en cualquier nodo de administración para gestionar el sistema StorageGRID. Sin embargo, algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

Conéctate al grupo de alta disponibilidad

Si los nodos de administración están incluidos en un grupo de alta disponibilidad (HA), te conectas usando la dirección IP virtual del grupo HA o un nombre de dominio completo que apunte a la dirección IP virtual. El nodo de administración principal debe seleccionarse como la interfaz principal del grupo, así que cuando accedas a Grid Manager, lo harás en el nodo de administración principal a menos que este no esté disponible. Consulta "Gestiona grupos de alta disponibilidad".

${post_edited_translations.segment}

Los pasos para iniciar sesión son un poco diferentes si "El inicio de sesión único (SSO) ha sido configurado".

Inicia sesión en Grid Manager en el primer nodo de administración

Antes de empezar

- Ya tienes tus datos de acceso.
- Estás usando un "navegador web compatible".
- Las cookies están activadas en tu navegador web.
- Perteneces a un grupo de usuarios que tiene al menos un permiso.
- Ya tienes la URL del Grid Manager:

  `https://FQDN_or_Admin_Node_IP/`

  Puedes utilizar el nombre de dominio completo, la dirección IP de un nodo de administración o la dirección IP virtual de un grupo de HA de nodos de administración.

  Para acceder al Grid Manager en un puerto distinto al puerto predeterminado para HTTPS (443), incluye el número de puerto en la URL:

  `https://FQDN_or_Admin_Node_IP:port/`

  > El SSO no está disponible en el puerto restringido de Grid Manager. Debes utilizar el puerto 443.

Pasos

1. Abre un navegador web compatible.
2. En la barra de direcciones del navegador, introduce la URL del Grid Manager.
3. Si te aparece una alerta de seguridad, instala el certificado utilizando el asistente de instalación del navegador. Consulta "Gestiona certificados de seguridad".

4. Inicia 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 usas SSO

   a. Introduce tu nombre de usuario y contraseña para el Grid Manager.

   b. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   - ${post_edited_translations.segment}

     i. Selecciona **Iniciar sesión**. Puedes dejar el 0 en el campo Cuenta.

     ii. Introduce tus credenciales habituales de SSO en la página de inicio de sesión único de tu organización.

     Por ejemplo, si StorageGRID utiliza el inicio de sesión único (SSO) y ya has accedido anteriormente al Grid Manager o a una cuenta de inquilino:

     A. ${post_edited_translations.segment}

     B. Selecciona **Sign in**.

     C. Inicia sesión con tus credenciales estándar de SSO en la página de inicio de sesión único de tu organización.

Cuando hayas iniciado sesión, aparecerá la página de inicio de Grid Manager, que incluye el panel de control. Para saber qué información se ofrece, consulta "Ver y gestionar el panel de control".

${post_edited_translations.segment}

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

No usas SSO

Pasos

1. En la barra de direcciones del navegador, introduce el nombre de dominio completo o la dirección IP del otro Admin Node. Incluye el número de puerto si es necesario.
2. Introduce tu nombre de usuario y contraseña para el Grid Manager.
3. ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

Pasos

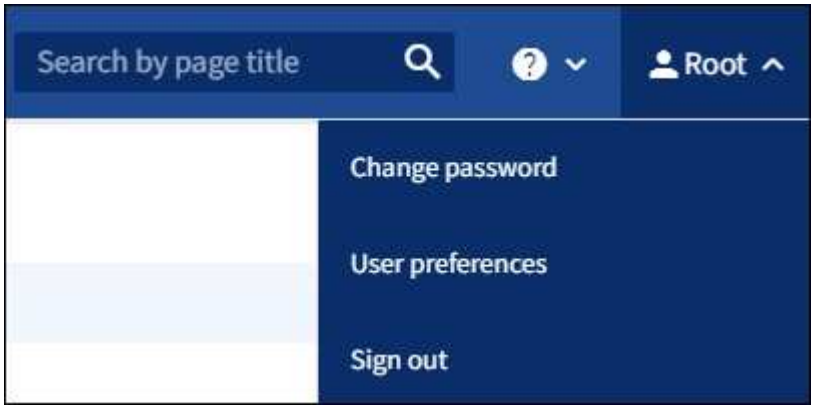
1. Introduce el nombre de dominio completo o la dirección IP del otro nodo de administración en la barra de direcciones del navegador.
2. Si tu sesión de SSO ha caducado, vuelve a introducir tus credenciales.

Sign out de StorageGRID Grid Manager

Cuando hayas terminado de trabajar con Grid Manager, debes cerrar la sesión para garantizar que los usuarios no autorizados no puedan acceder al sistema StorageGRID. Cerrar el navegador podría no cerrar tu sesión en el sistema, según la configuración de las cookies del navegador.

Pasos

1. Selecciona tu nombre de usuario en la esquina superior derecha.



2. Selecciona **Cerrar sesión**.

Opción	Descripción
${post_edited_translations.segment}	Has cerrado sesión en el nodo de administración. Se muestra la página de inicio de sesión de Grid Manager. ${post_edited_translations.segment}
SSO activado	Se ha cerrado la sesión en todos los nodos de administración a los que tenías acceso. Se muestra la página de inicio de sesión de StorageGRID. **Grid Manager** aparece como opción predeterminada en el menú desplegable **Cuentas recientes**, y el campo **ID de cuenta** muestra 0. **Nota:** Si el inicio de sesión único (SSO) está activado y además has iniciado sesión en Tenant Manager, también debes "${post_edited_translations.segment}" a "cerrar sesión de SSO".

Cambia tu contraseña de StorageGRID Grid Manager

Si eres un usuario local de Grid Manager, puedes cambiar tu propia contraseña.

Antes de empezar

Has iniciado sesión en Grid Manager mediante un "navegador web compatible".

Acerca de esta tarea

Si te logueas en StorageGRID como usuario federado o si el inicio de sesión único (SSO) está habilitado, no puedes cambiar tu contraseña en Grid Manager. En su lugar, debes cambiar tu contraseña en la fuente de identidad externa, por ejemplo, Active Directory u OpenLDAP.

Pasos

1. En la barra de menú de Grid Manager, selecciona ***tu nombre*** > **Cambiar contraseña**.
2. Introduce tu contraseña actual.
3. Escribe una nueva contraseña.

   Tu contraseña debe tener al menos 8 y no más de 32 caracteres. Las contraseñas distinguen entre mayúsculas y minúsculas.
4. Vuelve a introducir la nueva contraseña.
5. Selecciona **Guardar**.

Ver la información de la licencia de StorageGRID

Puedes ver la información de la licencia de tu sistema StorageGRID, como la capacidad de almacenamiento máxima de tu grid, cuando lo necesites.

Antes de empezar

Has iniciado sesión en Grid Manager mediante un "navegador web compatible".

Acerca de esta tarea

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

Pasos

1. ${post_edited_translations.segment}
   - Selecciona **Mantenimiento** > **Sistema** > **Licencia**.
   - ${post_edited_translations.segment}

     Este enlace solo aparece si hay algún problema con la licencia.

2. Consulta los detalles de solo lectura de la licencia actual:
    - ${post_edited_translations.segment}
    - Número de serie de la licencia
    - ${post_edited_translations.segment}
    - Capacidad de almacenamiento autorizada de la grid
    - ${post_edited_translations.segment}
    - Fecha de vencimiento de la licencia. **N/A** aparece para una licencia perpetua.
    - ${post_edited_translations.segment}

      Esta fecha se lee desde el archivo de licencia actual y podría estar desactualizada si ampliaste o renovaste el contrato de servicio de soporte después de obtener el archivo de licencia. Para actualizar este valor, consulta "Actualizar la información de la licencia de StorageGRID". También puedes ver la fecha de finalización real del contrato usando Active IQ.

    - Contenido del archivo de texto de la licencia

Actualizar la información de la licencia de StorageGRID

Debes actualizar la información de la licencia de tu sistema StorageGRID cada vez que cambien las condiciones de tu licencia. Por ejemplo, debes actualizar la información de la licencia si adquieres capacidad de almacenamiento adicional para tu grid.

Antes de empezar

- Tienes un nuevo archivo de licencia que debes aplicar a tu sistema StorageGRID.
- Tienes "permisos de acceso específicos".
- Tienes la frase de contraseña de aprovisionamiento.

Pasos

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

   El nuevo archivo de licencia se valida y se muestra.

4. Introduce la contraseña de aprovisionamiento.
5. Selecciona **Guardar**.

Usa la API

Usa la API de gestión de StorageGRID Grid

Puedes realizar tareas de administración de sistemas mediante la API de REST de Grid Management en lugar de la interfaz de usuario de Grid Manager. Por ejemplo, es posible que quieras utilizar la API para automatizar operaciones o para crear varias entidades, como usuarios, de forma más rápida.

Recursos de primer nivel

La API de gestión de la red ofrece los siguientes recursos de primer nivel:

- `/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 pertenezcan a un grupo LDAP local o federado de una cuenta de inquilino. Para obtener más información, consulta "Utiliza 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 endpoints privados de StorageGRID también ignoran la versión de la API de la solicitud.

Realizar solicitudes a la API

La API de gestión de la red utiliza la plataforma de API de código abierto Swagger. Swagger ofrece una interfaz de usuario intuitiva que permite tanto a desarrolladores como a usuarios sin conocimientos de programación realizar operaciones en tiempo real en StorageGRID mediante la API.

La interfaz de usuario de Swagger ofrece información completa y documentación detallada para cada operación de la API.

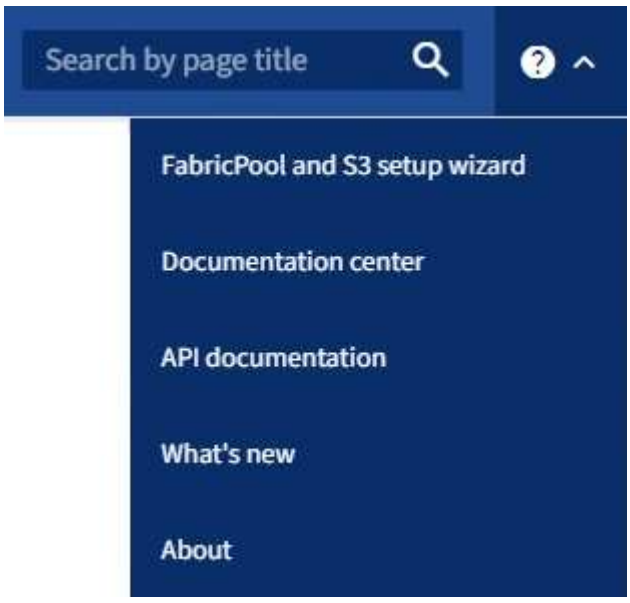
Antes de empezar

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

> Cualquier operación de la API que realices a través de la página web de la documentación de la API es una operación en tiempo real. Ten cuidado de no crear, actualizar ni eliminar por error datos de configuración u otros datos.

Pasos

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



2. Para realizar una operación con la API privada, selecciona **Ir a la documentación de la API privada** en la

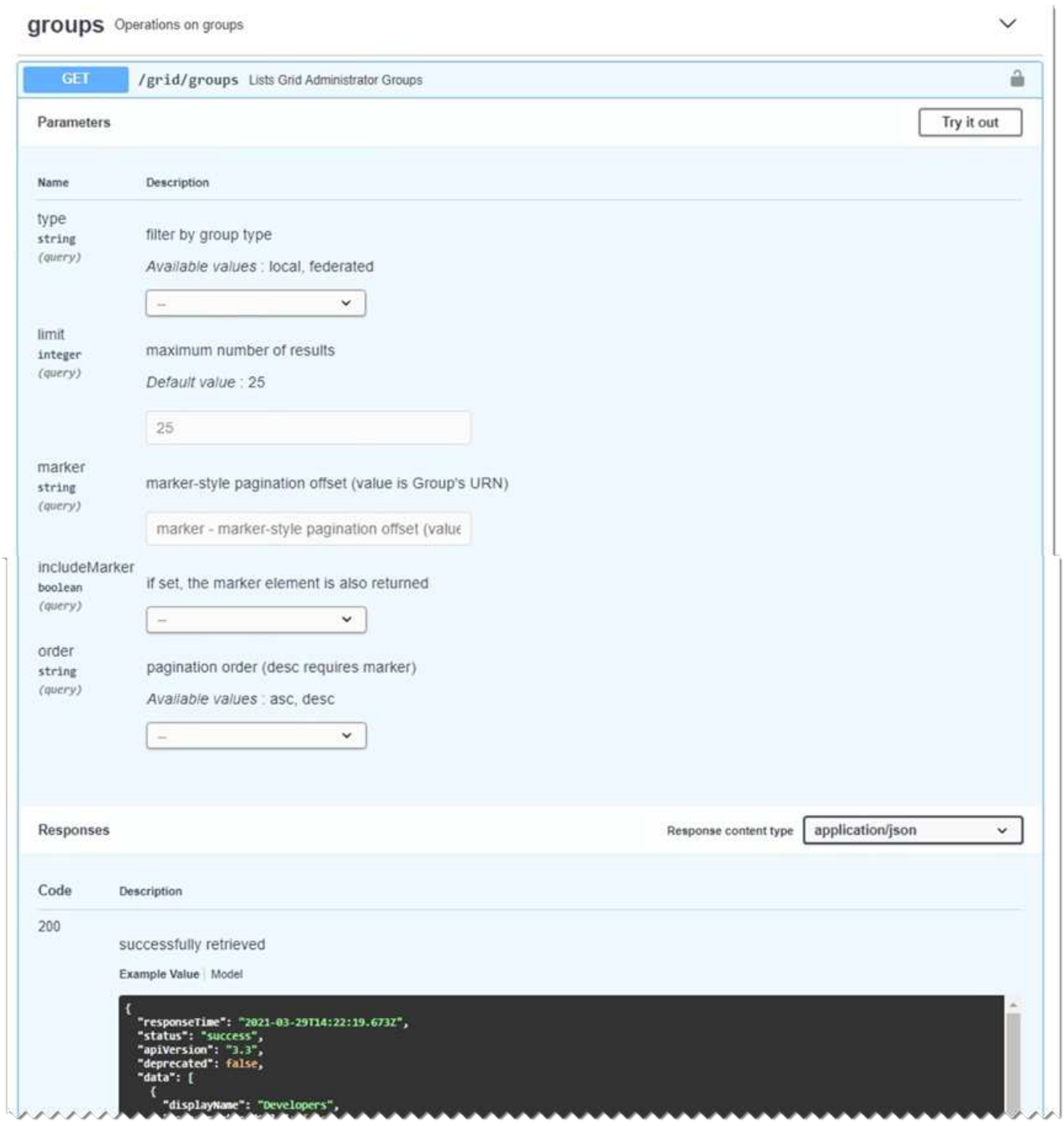
página StorageGRID Management API.

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

3. Selecciona la operación que desees.

   Al desplegar una operación de la API, podrás ver las acciones HTTP disponibles, como GET, PUT, UPDATE y DELETE.

4. Selecciona una acción HTTP para ver los detalles de la solicitud, incluyendo la URL del endpoint, una lista de los parámetros obligatorios u opcionales, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.



5. Comprueba si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. Luego, obtén estos valores. Puede que primero tengas que enviar otra solicitud a la API para obtener la información que necesitas.
6. Comprueba si es necesario modificar el cuerpo de la solicitud de ejemplo. Si es así, puedes seleccionar **Modelo** para conocer los requisitos de cada campo.
7. ${post_edited_translations.segment}
8. Introduce los parámetros necesarios o modifica el cuerpo de la solicitud según sea necesario.
9. Selecciona **Ejecutar**.
10. Revisa el código de respuesta para determinar si la solicitud fue exitosa.

Operaciones de Grid Management API en StorageGRID

${post_edited_translations.segment}

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

- **cuentas**: Operaciones para gestionar cuentas de inquilinos de almacenamiento, incluyendo la creación de nuevas cuentas y la obtención del uso de almacenamiento para una cuenta determinada.
- **historial-alertas**: Operaciones en alertas resueltas.
- **alert-receivers**: Operaciones sobre los receptores de notificaciones de alertas (correo electrónico).
- ${post_edited_translations.segment}
- **alert-silences**: Operaciones sobre el silenciamiento de alertas.
- **alertas**: Operaciones sobre alertas.
- ${post_edited_translations.segment}
- **auth**: Operaciones para realizar la autenticación de la sesión del usuario.

  La API de gestión de la red es compatible con el esquema de autenticación mediante token de portador. Para iniciar sesión, debes introducir 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 debe incluirse en el encabezado de las solicitudes posteriores a la API ("Authorization: Bearer *token*"). El token caduca después de 16 horas.

  Si el inicio de sesión único está habilitado para el sistema StorageGRID, debes realizar pasos diferentes para autenticarte. Consulta "Autenticación en la API si el inicio de sesión único está habilitado".

  Consulta «Protección contra la falsificación de solicitudes entre sitios» para obtener información sobre cómo mejorar la seguridad de autenticación.

- ${post_edited_translations.segment}
- **config**: operaciones relacionadas con la versión del producto y las versiones de la Grid Management API. Puedes enumerar la versión del producto y las versiones principales de la Grid Management API compatibles con esa versión, y puedes desactivar las versiones obsoletas de la API.
- ${post_edited_translations.segment}
- **dns-servers**: Operaciones para ver y modificar los servidores DNS externos configurados.
- **drive-details**: Operaciones en unidades para modelos específicos de dispositivos de almacenamiento.

- **endpoint-domain-names**: Operaciones para mostrar y cambiar los nombres de dominio de los endpoints de S3.
- **código de borrado**: Operaciones sobre perfiles de código de borrado.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **emplazamientos-de-expansión**: Operaciones de expansión (a nivel de emplazamiento).
- **grid-networks**: Operaciones para mostrar y cambiar la lista de la Grid Network.
- **grid-passwords**: Operaciones para la gestión de contraseñas de grid.
- **grupos**: Operaciones para gestionar los grupos de administradores de Grid locales y para recuperar los grupos de administradores de Grid federados desde un servidor LDAP externo.
- **fuente-de-identidad**: Operaciones para configurar una fuente de identidad externa y para sincronizar manualmente la información de grupos y usuarios federados.
- **ilm**: Operaciones sobre la gestión del ciclo de vida de la información (ILM).
- **procedimientos-en-curso**: Recupera los procedimientos de mantenimiento que están en curso.
- **licencia**: Operaciones para recuperar y actualizar la licencia de StorageGRID.
- **registros**: Operaciones para recopilar y descargar archivos de registro.v
- **métricas**: Operaciones con métricas de StorageGRID, incluidas consultas de métricas instantáneas en un único punto en el tiempo y consultas de métricas en un intervalo de tiempo. La Grid Management API utiliza la herramienta de monitoreo de sistemas Prometheus como fuente de datos backend. Para obtener información sobre cómo crear consultas de Prometheus, consulta el sitio web de Prometheus.

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

- **node-details**: Operaciones sobre los detalles de los nodos.
- **node-health**: Operaciones sobre el estado de salud del nodo.
- **node-storage-state**: Operaciones sobre el estado de almacenamiento del nodo.
- ${post_edited_translations.segment}
- **objetos**: Operaciones sobre objetos y metadatos de objetos.
- ${post_edited_translations.segment}
- **paquete-de-recuperación**: Operaciones para descargar el paquete de recuperación.
- **regiones**: Operaciones para ver y crear regiones.
- **s3-object-lock**: Operaciones sobre la configuración global de S3 Object Lock.
- ${post_edited_translations.segment}
- **snmp**: Operaciones sobre la configuración actual de SNMP.
- **marcas de agua de almacenamiento**: Marcas de agua de los nodos de almacenamiento.
- **clases-de-tráfico**: Operaciones para las políticas de clasificación de tráfico.
- ${post_edited_translations.segment}
- **Usuarios**: Operaciones para ver y gestionar usuarios de Grid Manager.

Versionado de la Grid Management API en StorageGRID

La API de gestión de la red utiliza versionado 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 incrementa cuando se realizan cambios que *no son compatibles* con las versiones anteriores. La versión secundaria de la API se incrementa cuando se realizan cambios que *sí son compatibles* con las versiones anteriores. Los cambios compatibles incluyen la adición de nuevos endpoints o nuevas propiedades.

El siguiente ejemplo ilustra cómo se incrementa la versión de la API en función del tipo de cambios realizados.

Tipo de cambio en la API	${post_edited_translations.segment}	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, al actualizar a una nueva versión funcional de StorageGRID, sigues teniendo acceso a la versión anterior de la API durante al menos una versión funcional de StorageGRID.

> Puedes configurar las versiones compatibles. Consulta la sección **config** de la documentación de la API de Swagger para el "API de gestión de grid" para más información. Debes desactivar la compatibilidad con la versión anterior después de actualizar todos los clientes de la API para que usen la versión más reciente.

Las solicitudes obsoletas se marcan como en desuso de las siguientes maneras:

- ${post_edited_translations.segment}
- El cuerpo de la respuesta JSON incluye "deprecated": true
- Se añade una advertencia de obsolescencia a nms.log. Por ejemplo:

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

Averigua qué versiones de la API son compatibles en la versión actual

Utiliza la solicitud de API `GET /versions` para devolver una lista de las versiones principales de la API compatibles. 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
  ]
}
```

Especifica una versión de la API para una solicitud

Puedes especificar la versión de la API utilizando un parámetro de ruta (`/api/v4`) o un encabezado (`Api-Version: 4`). Si proporcionas ambos valores, el valor del encabezado tiene prioridad sobre el de la ruta.

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

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

Protege contra la falsificación de petición en sitios cruzados (CSRF) en StorageGRID

Puedes ayudar a proteger StorageGRID contra los ataques de falsificación de solicitudes entre sitios (CSRF) utilizando tokens CSRF para reforzar la autenticación que usa cookies. Grid Manager y Tenant Manager activan automáticamente esta función de seguridad; otros clientes de la API pueden elegir si desean activarla al iniciar sesión.

${post_edited_translations.segment}

StorageGRID ayuda a proteger contra los ataques CSRF mediante el uso de tokens CSRF. Cuando está habilitado, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro específico del cuerpo de POST.

Para habilitar la función, establece el parámetro `csrfToken` 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, se establece una cookie `GridCsrfToken` con un valor aleatorio para los inicios de sesión en el Grid Manager, y la cookie `AccountCsrfToken` se establece con un valor aleatorio para los inicios de sesión en el Tenant Manager.

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

- La cabecera `X-Csrf-Token`, con el valor de la cabecera establecido en el valor de la cookie de token CSRF.
- Para los puntos finales que aceptan un cuerpo codificado en formato form-encoded: un parámetro del cuerpo de la solicitud codificado en formato form-encoded. `csrfToken`

Consulta la documentación en línea de la API para ver más ejemplos y detalles.

> Las solicitudes que tengan configurada una cookie con un token CSRF también aplicarán el encabezado "Content-Type: application/json" a cualquier solicitud que requiera un cuerpo de solicitud en formato JSON como protección adicional contra los ataques CSRF.

${post_edited_translations.segment}

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

Si tienes "configurado y activado el inicio de sesión único (SSO)" y usas Active Directory como proveedor de inicio de sesión único, debes hacer una serie de solicitudes de API para obtener un token de autenticación válido para la Grid Management API o la Tenant Management API.

Inicia sesión en la API si está activado el inicio de sesión único

Estas instrucciones aplican si usas Active Directory como proveedor de identidad de inicio de sesión único (SSO).

Antes de empezar

- Conoces el nombre de usuario y la contraseña de inicio de sesión único de un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si quieres acceder a la API de gestión de inquilinos, sabes el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puedes usar uno de los siguientes ejemplos:

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

  El flujo de trabajo de curl podría agotar el tiempo de espera si lo ejecutas demasiado despacio. Es posible que aparezca el siguiente error: `A valid SubjectConfirmation was not found on this Response`.

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

Si tienes un problema de codificación de URL, es posible que veas el error: `Unsupported SAML version`.

Pasos

1. Selecciona uno de los siguientes métodos para obtener un token de autenticación:
   - Utiliza el `storagegrid-ssoauth.py` script de Python. Ve al paso 2.
   - Utiliza solicitudes con curl. Ve al paso 3.
2. Si quieres utilizar el script `storagegrid-ssoauth.py`, pásalo al intérprete de Python y ejecútalo.

   Cuando se te solicite, introduce los valores para los siguientes argumentos:

   - El método SSO. Introduce ADFS o adfs.
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID
   - La dirección de StorageGRID
   - El ID de la cuenta del tenant, si deseas acceder a la API de Tenant Management.

   ```
   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 aparece en la salida. Ahora puedes utilizar el token para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.
3. Si quieres utilizar solicitudes curl, usa el siguiente procedimiento.
   a. Declara 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 la red, utiliza 0 como `TENANTACCOUNTID`.

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

   Este ejemplo muestra una solicitud POST para obtener una URL de autenticación firmada para `TENANTACCOUNTID`. Los resultados se enviarán 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 URL firmada que está codificada como URL, pero no incluye la capa adicional de codificación JSON.

```
{
    "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. Guarda el `SAMLRequest` de la respuesta para usarlo en comandos posteriores.

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

d. Obtén una URL completa que incluya el ID de la solicitud del cliente de AD FS.

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

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

   ${post_edited_translations.segment}

```
<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. Guarda el ID de la solicitud del cliente de la respuesta.

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

f. Envía tus credenciales a la acción del 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 una redirección 302, con información adicional en los encabezados.

> Si la autenticación multifactor (MFA) está habilitada para tu sistema de SSO, el envío 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. Guarda la `MSISAuth` cookie de la respuesta.

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

h. Envía una solicitud GET a la ubicación especificada con las cookies de la autenticación POST.

```
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 la sesión de AD FS para uso posterior en el cierre de sesión, y el cuerpo de la respuesta contiene el SAMLResponse en un campo oculto del formulario.

```
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. Guarda el `SAMLResponse` del campo oculto:

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

j. Utilizando el archivo guardado `SAMLResponse`, haz una solicitud StorageGRID`/api/saml-response` para generar un token de autenticación de StorageGRID.

Para `RelayState`, usa el ID de la cuenta de inquilino o usa 0 si quieres 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. Guarda el token de autenticación de la respuesta como `MYTOKEN`.

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

Ahora puedes utilizar `MYTOKEN` para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

Cierra sesión en la API si el inicio de sesión único está activado

Si se ha habilitado el inicio de sesión único (SSO), debes realizar una serie de solicitudes de API para cerrar la sesión en la Grid Management API o en la Tenant Management API. Estas instrucciones aplican si usas Active Directory como proveedor de identidad de SSO.

Acerca de esta tarea

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

Pasos

1. Para generar una solicitud de cierre de sesión con firma, pasa `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. Guarda la URL de cierre de sesión.

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

3. ${post_edited_translations.segment}

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

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de la 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. ${post_edited_translations.segment}

Eliminar el token de portador de StorageGRID funciona igual que sin SSO. Si no se proporciona la `cookie "sso=true"`, el usuario se desconecta de StorageGRID sin afectar el estado de SSO.

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

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

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

Usa la API de StorageGRID si el inicio de sesión único está activado (Entra ID)

Si tienes "configurado y activado el inicio de sesión único (SSO)" y usas Entra ID como proveedor de inicio de sesión único, puedes usar dos scripts de ejemplo para obtener un token de autenticación válido para la API de gestión de Grid o la API de gestión de Tenant.

Inicia sesión en la API si está activado el inicio de sesión único de Entra ID

Estas instrucciones aplican si usas Entra ID como proveedor de identidad de inicio de sesión único

Antes de empezar

- Conoces la dirección de correo electrónico y la contraseña de inicio de sesión único de un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si quieres acceder a la API de gestión de inquilinos, sabes el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puedes utilizar los siguientes scripts de ejemplo:

- El `storagegrid-ssoauth-azure.py` script de Python
- El `storagegrid-ssoauth-azure.js` 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 tu propia integración de API con Entra ID, consulta el script `storagegrid-ssoauth-azure.py`. El script de Python realiza dos solicitudes directamente a StorageGRID (primero para obtener el SAMLRequest y luego para obtener el token de autorización), y también llama al script de Node.js para interactuar con Entra ID y realizar las operaciones de inicio de sesión único.

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

Si tienes un problema de codificación de URL, es posible que veas el error: `Unsupported SAML version`.

Pasos

1. Instala las dependencias necesarias de la siguiente manera:
   a. Instala Node.js (consulta "https://nodejs.org/en/download/").
   b. Instala los módulos necesarios de Node.js (puppeteer y jsdom):

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

2. Pasa el script de Python al intérprete de Python para ejecutar el script.

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

3. Cuando se te solicite, introduce los valores de los siguientes argumentos (o pásalos mediante parámetros):
   ◦ La dirección de correo electrónico de SSO utilizada para iniciar sesión en Entra ID

- La dirección de StorageGRID
- El ID de la cuenta del inquilino, si quieres acceder a la API de gestión de inquilinos

4. Cuando se te solicite, introduce la contraseña y prepárate para proporcionar una autorización MFA a Entra ID si se te pide.

```
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'}
```

> El script parte de la base de que la autenticación multifactor (MFA) se realiza usando Microsoft Authenticator. Es posible que tengas que modificar el script para admitir otras formas de MFA (como ingresar un código recibido en un mensaje de texto).

El token de autorización de StorageGRID aparece en la salida. Ahora puedes utilizar el token para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

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

Si tienes "configurado y activado el inicio de sesión único (SSO)" y usas PingFederate como proveedor de inicio de sesión único, debes realizar una serie de solicitudes de API para obtener un token de autenticación válido para la Grid Management API o la Tenant Management API.

Inicia sesión en la API si está activado el inicio de sesión único

Estas instrucciones aplican si usas PingFederate como proveedor de identidad de SSO

Antes de empezar

- Conoces el nombre de usuario y la contraseña de inicio de sesión único de un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si quieres acceder a la API de gestión de inquilinos, sabes el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puedes usar uno de los siguientes ejemplos:

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

  El flujo de trabajo de curl podría agotar el tiempo de espera si lo ejecutas demasiado despacio. Es posible que aparezca el siguiente error: `A valid SubjectConfirmation was not found on this Response`.

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

Si tienes un problema de codificación de URL, es posible que veas el error: `Unsupported SAML version`.

Pasos

1. Selecciona uno de los siguientes métodos para obtener un token de autenticación:
   - Utiliza el `storagegrid-ssoauth.py` script de Python. Ve al paso 2.
   - Utiliza solicitudes con curl. Ve al paso 3.
2. Si quieres utilizar el script `storagegrid-ssoauth.py`, pásalo al intérprete de Python y ejecútalo.

   Cuando se te solicite, introduce los valores para los siguientes argumentos:

   - El método SSO. Puedes introducir cualquier variante de «pingfederate» (PINGFEDERATE, pingfederate, y así sucesivamente).
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID. Este campo no se utiliza para PingFederate. Puedes dejarlo en blanco o ingresar cualquier valor.
   - La dirección de StorageGRID
   - El ID de la cuenta del tenant, si deseas acceder a la API de Tenant Management.

   ```
   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 aparece en la salida. Ahora puedes utilizar el token para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

3. Si quieres utilizar solicitudes curl, usa el siguiente procedimiento.

   a. Declara 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 la red, utiliza 0 como `TENANTACCOUNTID`.

   b. Para recibir una URL de autenticación firmada, envía una solicitud POST a `/api/v3/authorize-`

`saml` y elimina la codificación JSON adicional de la respuesta.

Este ejemplo muestra una solicitud POST para una URL de autenticación firmada para TENANTACCOUNTID. Los resultados se pasan 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 URL firmada que está codificada como URL, pero no incluye la capa adicional de codificación JSON.

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

c. Guarda el `SAMLRequest` de la respuesta para usarlo en comandos posteriores.

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

d. Exporta la respuesta y la cookie, y muestra la respuesta:

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

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

e. Exporta el valor 'pf.adapterId' y muestra la respuesta:

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

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

f. Exporta el valor de «href» (elimina la barra al final /) y muestra la respuesta:

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

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

g. Exporta el valor 'action':

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

h. Enviar cookies junto con las 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. Guarda el `SAMLResponse` del campo oculto:

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

j. Utilizando el archivo guardado `SAMLResponse`, haz una solicitud StorageGRID`/api/saml-response` para generar un token de autenticación de StorageGRID.

Para `RelayState`, usa el ID de la cuenta de inquilino o usa 0 si quieres 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. Guarda el token de autenticación de la respuesta como `MYTOKEN`.

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

Ahora puedes utilizar `MYTOKEN` para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

Cierra sesión en la API si el inicio de sesión único está activado

Si se ha habilitado el inicio de sesión único (SSO), debes realizar una serie de solicitudes de API para cerrar la sesión en la API de gestión de Grid o en la API de gestión de Tenant. Estas instrucciones aplican si usas PingFederate como proveedor de identidad de SSO.

Acerca de esta tarea

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

Pasos

1. Para generar una solicitud de cierre de sesión con firma, pasa `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. Guarda la URL de cierre de sesión.

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

3. ${post_edited_translations.segment}

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

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de la 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. ${post_edited_translations.segment}

Eliminar el token de portador de StorageGRID funciona igual que sin SSO. Si no se proporciona la `cookie "sso=true"`, el usuario se desconecta de StorageGRID sin afectar el estado de SSO.

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

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

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

Desactiva las funciones de StorageGRID con la API

Puedes usar la API de gestión de grid para desactivar por completo ciertas funciones en el 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 te permite impedir el acceso a determinadas funciones del sistema StorageGRID. Desactivar una función es la única forma de impedir que el usuario raíz o los usuarios que pertenezcan a grupos de administración con permiso de acceso a raíz puedan utilizar esa función.

Para comprender cómo puede resultar útil esta funcionalidad, imagina la siguiente situación:

La empresa A es un proveedor de servicios que alquila la capacidad de almacenamiento de su sistema StorageGRID mediante la creación de cuentas de inquilino. Para proteger la seguridad de los objetos de sus inquilinos, la empresa A quiere asegurarse de que sus propios empleados nunca puedan acceder a ninguna cuenta de inquilino una vez que esta se haya implementado.

La empresa A puede alcanzar este objetivo utilizando el sistema Deactivate Features en la Grid Management API. Al desactivar por completo la función **Change tenant root password** en el Grid Manager (tanto en la interfaz de usuario como en la API), la empresa A se asegura de que los usuarios Admin —incluidos el

usuario raíz y los usuarios que pertenecen a grupos con el permiso **Root access**— no puedan cambiar la contraseña del usuario raíz de ninguna cuenta de tenant._

Pasos

1. Accede a la documentación de Swagger sobre la API de gestión de la red. Consulta "Usa la API de gestión de Grid".
2. Ubica el endpoint Deactivate Features.
3. Para desactivar una función, como Cambiar la contraseña raíz del inquilino, envía un cuerpo a la API como este:

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

   Cuando se completa la solicitud, la función Cambiar la contraseña de root del inquilino queda desactivada. El permiso de administración **Cambiar la contraseña de root del inquilino** ya no aparece en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña de root de un inquilino fallará con "403 Forbidden".

Reactivar las funciones desactivadas

De forma predeterminada, puedes utilizar la API de gestión de la red para reactivar una función que se haya desactivado. Sin embargo, si deseas evitar que las funciones desactivadas se vuelvan a activar en ningún momento, puedes desactivar la propia función **activateFeatures**.

> La función **activateFeatures** no se puede volver a activar. Si decides desactivar esta función, ten en cuenta que perderás de forma permanente la posibilidad de volver a activar cualquier otra función desactivada. Debes ponerte en contacto con el soporte técnico para recuperar cualquier funcionalidad perdida.

Pasos

1. Accede a la documentación de Swagger para la API de gestión de la red.
2. Ubica el endpoint Deactivate Features.
3. Para reactivar todas las funciones, envía un cuerpo a la API como este:

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

   Una vez completada esta solicitud, se reactivan todas las funciones, incluida la función **Cambiar la contraseña de root del inquilino**. El permiso de administración **Cambiar la contraseña de root del inquilino** aparece ahora en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña de root de un inquilino se ejecutará con éxito, siempre que el usuario disponga del permiso de administración **Acceso a raíz** o **Cambiar la contraseña de root del inquilino**.

> El ejemplo anterior hace que se reactiven *todas* las funciones desactivadas. Si se han desactivado otras funciones que deberían permanecer desactivadas, debes especificarlas explícitamente en la solicitud PUT. Por ejemplo, para reactivar la función Cambiar la contraseña raíz del inquilino y mantener desactivado el permiso de gestión storageAdmin, envía esta solicitud PUT: `{ "grid": {"storageAdmin": true} }`

Controlar el acceso a StorageGRID

Controlar el acceso a StorageGRID

Puedes 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. Opcionalmente, puedes habilitar el inicio de sesión único (SSO), crear certificados de cliente y cambiar las contraseñas de grid.

Controla el acceso al Grid Manager

Tú determinas quién puede acceder a Grid Manager y a la API de gestión de la red importando grupos y usuarios desde un servicio de federación de identidades o configurando grupos y usuarios locales.

Usar "federación de identidades" hace que configurar "grupos" y "${post_edited_translations.segment}" sea más rápido, y permite que los usuarios inicien sesión en StorageGRID con sus credenciales habituales. Puedes configurar la federación de identidades si usas Active Directory, OpenLDAP u Oracle Directory Server.

Ponte en contacto con el soporte técnico si deseas utilizar otro servicio LDAP v3.

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

Opcionalmente, puedes configurar un grupo para que sea de solo lectura. Los usuarios de un grupo de solo lectura solo pueden ver la configuración y las funciones. No pueden realizar ningún cambio ni llevar a cabo ninguna operación en el Grid Manager o en la Grid Management API.

Habilitar 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 que "${post_edited_translations.segment}", todos los usuarios deben autenticarse mediante un proveedor de identidad externo antes de poder acceder al Grid Manager, al Tenant Manager, a la API de Grid Management o a la API de Tenant Management. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cambiar la contraseña 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 del grid y las claves de cifrado para el sistema StorageGRID. Puedes "cambiar la contraseña" según sea necesario.

${post_edited_translations.segment}

Cada nodo de tu grid tiene una contraseña de consola de nodo, que necesitas para iniciar sesión en el nodo como "admin" usando SSH, o como usuario raíz en una conexión de consola de VM/física. Si lo necesitas, puedes "cambiar la contraseña de la consola del nodo" para cada nodo.

Cambia la contraseña de aprovisionamiento de StorageGRID

Usa 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 de paquetes de recuperación que incluyen la información de la topología de la grid, las contraseñas de la consola de los nodos de la grid y las claves de cifrado del sistema StorageGRID.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- ${post_edited_translations.segment}
- Tienes la contraseña de aprovisionamiento actual.

Acerca de esta tarea

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

Pasos

1. Selecciona **Configuración** > **Control de acceso** > **Contraseñas de grid**.
2. ${post_edited_translations.segment}
3. Introduce tu contraseña de aprovisionamiento actual.
4. Introduce la nueva frase de contraseña. La frase de contraseña debe contener al menos 8 y no más de 32 caracteres. Las frases de contraseña distinguen mayúsculas de minúsculas.

   Guarda la frase de contraseña de aprovisionamiento en un lugar seguro. Es necesaria para los procedimientos de instalación, ampliación y mantenimiento.

5. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

6. Selecciona **Paquete de recuperación**.
7. Introduce la nueva frase de contraseña de aprovisionamiento para descargar el nuevo paquete de recuperación.

   Tras cambiar la contraseña de aprovisionamiento, debes descargar inmediatamente un nuevo paquete de recuperación. El archivo del paquete de recuperación te permite restaurar el sistema en caso de que se produzca un fallo.

Cambia las contraseñas de la consola de nodo en StorageGRID

Cada nodo de tu grid tiene una contraseña de consola de nodo, que usas para iniciar

sesión en el nodo. Por defecto, cada nodo tiene una contraseña única. Puedes cambiar cada contraseña por una nueva contraseña única, o puedes cambiar la contraseña de todos los nodos para usar una contraseña global. Las contraseñas se almacenan en el paquete de recuperación.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de mantenimiento o acceso de usuario raíz".
- Tienes la contraseña de aprovisionamiento actual.

Acerca de esta tarea

Usas una contraseña de la consola del nodo para iniciar sesión en un nodo como "admin" usando SSH, o como usuario raíz en una conexión de consola de una máquina virtual o física. Puedes cambiar las contraseñas de la consola del nodo usando una de estas opciones:

- Aplicar automáticamente contraseñas aleatorias a cada nodo
- Especifica y aplica una contraseña global a todos los nodos
- Especifica y aplica una contraseña única a uno o varios nodos

Las contraseñas se almacenan en un archivo actualizado `Passwords.txt` que se encuentra en el paquete de recuperación. Las contraseñas aparecen en la columna Password del archivo.

> ⓘ El "Contraseñas de acceso SSH" de las claves SSH utilizadas para la comunicación entre nodos es independiente de las contraseñas de la consola de los nodos. Este procedimiento no cambia las contraseñas de acceso SSH.

Accede al asistente

Pasos

1. Selecciona **Configuración** > **Control de acceso** > **Contraseñas de grid**.
2. En **Cambiar contraseñas de la consola del nodo**, selecciona **Realizar un cambio**.

Descargar el paquete de recuperación actual

Antes de cambiar las contraseñas de la consola de los nodos, descarga el paquete de recuperación actual. Puedes utilizar las contraseñas de este archivo si el proceso de cambio de contraseña falla en algún nodo.

Pasos

1. Introduce la frase de contraseña de aprovisionamiento de tu grid.
2. Selecciona **Descargar paquete de recuperación**.
3. Copia el archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y distintas.

> ⚠ El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

4. Selecciona **Continuar**.

Proporciona nuevas contraseñas

1. Selecciona el método de cambio de contraseña que quieras utilizar.
   - **Automático**: StorageGRID asigna automáticamente una nueva contraseña aleatoria de consola a todos los nodos.
   - **Personalizado**: Tú proporcionas las contraseñas de la consola.

Automático

1. Selecciona **Continuar**.

Personalizado

1. Selecciona una de las siguientes:
   - **Contraseña global de la consola**: aplica la misma contraseña de la consola a todos los nodos.
   - **Contraseñas únicas de consola**: Establece una contraseña diferente en uno o varios nodos.
2. Si has seleccionado **Contraseña global de la consola**, introduce la contraseña que quieras usar para todos los nodos.
3. Si has seleccionado **Contraseñas únicas de consola**, introduce una contraseña única para uno o más nodos.
4. Selecciona **Continuar**.

Finaliza el cambio de contraseña

1. Cuando aparezca el cuadro de diálogo de confirmación, selecciona **Sí** si estás listo para que StorageGRID comience a cambiar las contraseñas de la consola de los nodos.

   No puedes cancelar este proceso después de que comienza.

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

2. Cuando el nuevo paquete de recuperación esté listo, selecciona **Descargar nuevo paquete de recuperación** y guarda el paquete de recuperación.
3. Abre el archivo `.zip`.
4. Comprueba que puedes acceder a los contenidos, incluido el archivo `Passwords.txt`, que contiene las nuevas contraseñas de la consola de nodo.
5. Copia el nuevo archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y distintas.

   No sobrescribas el paquete de recuperación anterior.

   Debes proteger el archivo de recuperación, porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

6. Marca la casilla de verificación para indicar que has descargado el nuevo paquete de recuperación y has verificado el contenido.
7. Selecciona **Continuar**.

   StorageGRID actualiza la contraseña de cada nodo.

Si se produce un error durante el proceso de actualización, la barra de progreso muestra el número de nodos en los que no se pudo cambiar la contraseña. El sistema volverá a intentar automáticamente el proceso en cualquier nodo en el que no se pudo cambiar la contraseña. Si el proceso termina y todavía hay algunos nodos en los que no se cambió la contraseña, aparece el botón **Reintentar**.

8. Si la actualización de la contraseña falló en uno o varios nodos:
   a. Revisa los mensajes de error que aparecen en la tabla.
   b. Resuelve los problemas.
   c. Selecciona **Reintentar**.

   > Al volver a intentarlo, solo se modifican las contraseñas de la consola de los nodos en los que falló el cambio de contraseña en intentos anteriores.

9. Cuando la barra de progreso indique que ya no quedan actualizaciones, selecciona **Finalizar**.
10. Una vez que se hayan cambiado las contraseñas de la consola de todos los nodos, elimina el el primer paquete de recuperación que descargaste.

Cambia las contraseñas de acceso SSH para StorageGRID Admin Nodes

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

Utiliza una clave SSH para iniciar sesión en un nodo como `admin` o como usuario raíz en una máquina virtual o mediante una conexión a la consola física.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de mantenimiento o acceso de usuario raíz".
- Tienes la contraseña de aprovisionamiento actual.

Acerca de esta tarea

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

Existen contraseñas de acceso SSH independientes para las claves SSH que se utilizan para la comunicación entre nodos. Este procedimiento no las modifica.

Accede al asistente

Pasos

1. Selecciona **Configuración** > **Control de acceso** > **Contraseñas de grid**.
2. En **Cambiar claves SSH**, selecciona **Realizar un cambio**.

Descargar el paquete de recuperación actual

Antes de cambiar las claves de acceso SSH, descarga el paquete de recuperación actual. Puedes utilizar las claves de este archivo si el proceso de cambio de claves falla en algún nodo.

Pasos

1. Introduce la frase de contraseña de aprovisionamiento de tu grid.
2. Selecciona **Descargar paquete de recuperación**.
3. Copia el archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y distintas.

   El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

4. Selecciona **Continuar**.
5. Cuando aparezca el cuadro de diálogo de confirmación, selecciona **Sí** si estás listo para empezar a modificar las claves de acceso SSH.

   No puedes cancelar este proceso después de que comienza.

Cambiar las claves de acceso SSH

Cuando se inicia el proceso de cambio de las 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. Espera 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 activo, selecciona **Descargar nuevo paquete de recuperación** y guarda el nuevo archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y separadas.
3. Cuando finalice la descarga:

   a. Abre el archivo `.zip`.

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

   c. Copia el nuevo archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y distintas.

      No sobrescribas el paquete de recuperación anterior.

   El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

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

   ${post_edited_translations.segment}

   Si se produce un error durante el proceso de actualización, un mensaje en un banner indica el número de nodos en los que no se pudo cambiar la clave. El sistema volverá a intentar automáticamente el proceso en cualquier nodo en el que no se pudo cambiar la clave. Si el proceso termina y algunos nodos siguen sin tener la clave cambiada, aparece el botón **Retry**.

Si la actualización de la clave falló en uno o varios nodos:

a. Revisa los mensajes de error que aparecen en la tabla.
b. Resuelve los problemas.
c. Selecciona **Reintentar**.

   Al volver a intentarlo, solo se modifican las claves de acceso SSH en los nodos que fallaron durante los intentos anteriores de cambio de clave.

5. Una vez que se hayan cambiado las claves de acceso SSH para todos los nodos, elimina el el primer paquete de recuperación que descargaste.
6. ${post_edited_translations.segment}

Usa la federación de identidades en StorageGRID

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 que ya conocen.

Configura la federación de identidades para Grid Manager

Puedes configurar la federación de identidades en Grid Manager si deseas que los grupos de administradores y los usuarios se gestionen en otro sistema, como Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server.

Antes de empezar

- Has iniciado sesión en Grid Manager usando una "navegador web compatible".
- Has "permisos de acceso específicos".
- Estás utilizando Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server como proveedor de identidades.

  > Si deseas utilizar un servicio LDAP v3 que no figure en la lista, ponte en contacto con soporte técnico.

- Si tienes previsto utilizar OpenLDAP, debes configurar el servidor OpenLDAP. Consulta Guía para configurar un servidor OpenLDAP.
- Si tienes previsto habilitar el inicio de sesión único (SSO), ya revisaste la "Requisitos y consideraciones para el inicio de sesión único".
- Si tienes previsto utilizar Transport Layer Security (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidad está usando TLS 1.2 o 1.3. Consulta "Algoritmos de cifrado compatibles para las conexiones TLS salientes".

Acerca de esta tarea

Puedes configurar un origen de identidad para el Grid Manager si quieres importar grupos desde otro sistema como Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server. Puedes importar los siguientes tipos de grupos:

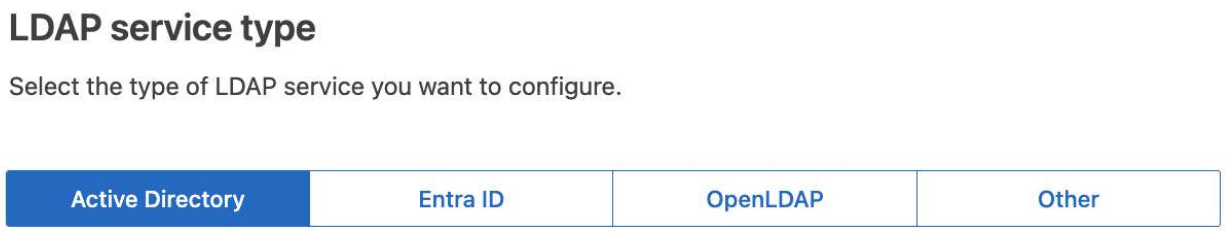
- Grupos de administradores. Los usuarios que forman parte de los grupos de administradores pueden iniciar sesión en Grid Manager y realizar tareas, en función de los permisos de gestión asignados al grupo.

- Grupos de usuarios de inquilinos para inquilinos que no usan su propia fuente de identidad. Los usuarios de los grupos de inquilinos pueden iniciar sesión en el Tenant Manager y realizar tareas según los permisos asignados al grupo en el Tenant Manager. Consulta "Crear cuenta de inquilino" y "Utiliza una cuenta de inquilino" para obtener más detalles.

Accede a la configuración

Pasos

1. Selecciona **Configuración** > **Control de acceso** > **Federación de identidades**.
2. Selecciona **Habilitar federación de identidades**.
3. ${post_edited_translations.segment}



${post_edited_translations.segment}

4. Si has seleccionado **Other**, rellena los campos de la sección «Atributos LDAP». De lo contrario, pasa al siguiente paso.
   - **Nombre único de usuario**: El nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo equivale a `sAMAccountName` para Active Directory y `uid` para OpenLDAP. Si estás configurando Oracle Directory Server, introduce `uid`.
   - **UUID de usuario**: El nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a `objectGUID` en Active Directory y `entryUUID` en OpenLDAP. Si estás configurando Oracle Directory Server, introduce `nsuniqueid`. El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos, ya sea en formato de 16 bytes o de cadena, donde se ignoran los guiones.
   - **Nombre único de 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 estás configurando Oracle Directory Server, introduce `cn`.
   - **UUID del 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 estás configurando Oracle Directory Server, introduce `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos, ya sea en formato de 16 bytes o de cadena, donde se ignoran los guiones.
5. Para todos los tipos de servicio LDAP, introduce la información necesaria sobre el servidor LDAP y la conexión de red en la sección Configurar el servidor LDAP.
   - **Nombre de host**: 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, puedes usar cualquier puerto siempre que tu firewall esté configurado correctamente.

- ${post_edited_translations.segment}

  Para Active Directory, también puedes especificar el Down-Level Logon Name o el User Principal Name.

  El usuario especificado debe tener permiso para ver la lista de grupos y usuarios y para acceder a los siguientes atributos:

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

  > Si cambias la contraseña en el futuro, debes actualizarla en esta página.

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

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

- **DN de base de usuarios**: La ruta completa del nombre distintivo (DN) de un subárbol LDAP en el que quieres buscar usuarios.

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

- **Formato de nombre de usuario de enlace** (opcional): el patrón de nombre de usuario predeterminado que StorageGRID debe utilizar si no es posible determinar el patrón automáticamente.

  Se recomienda especificar el **formato de nombre de usuario de enlace** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede enlazarse con la cuenta de servicio.

  ${post_edited_translations.segment}

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

- **Patrón de nombre distintivo**: `CN=[USERNAME],CN=Users,DC=example,DC=com`

  Incluye **[USERNAME]** tal y como aparece escrito.

6. En la sección Transport Layer Security (TLS), selecciona una configuración de seguridad.
   - **Usar STARTTLS**: Utiliza STARTTLS para proteger las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u Other, pero 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. Debes seleccionar esta opción para Microsoft Entra ID.
   - **No utilices 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.

   > El uso de la opción **No usar TLS** no se admite si tu servidor de Active Directory exige la firma LDAP. Debes usar STARTTLS o LDAPS.

7. Si has seleccionado STARTTLS o LDAPS, elige el certificado que se usa para proteger la conexión.
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

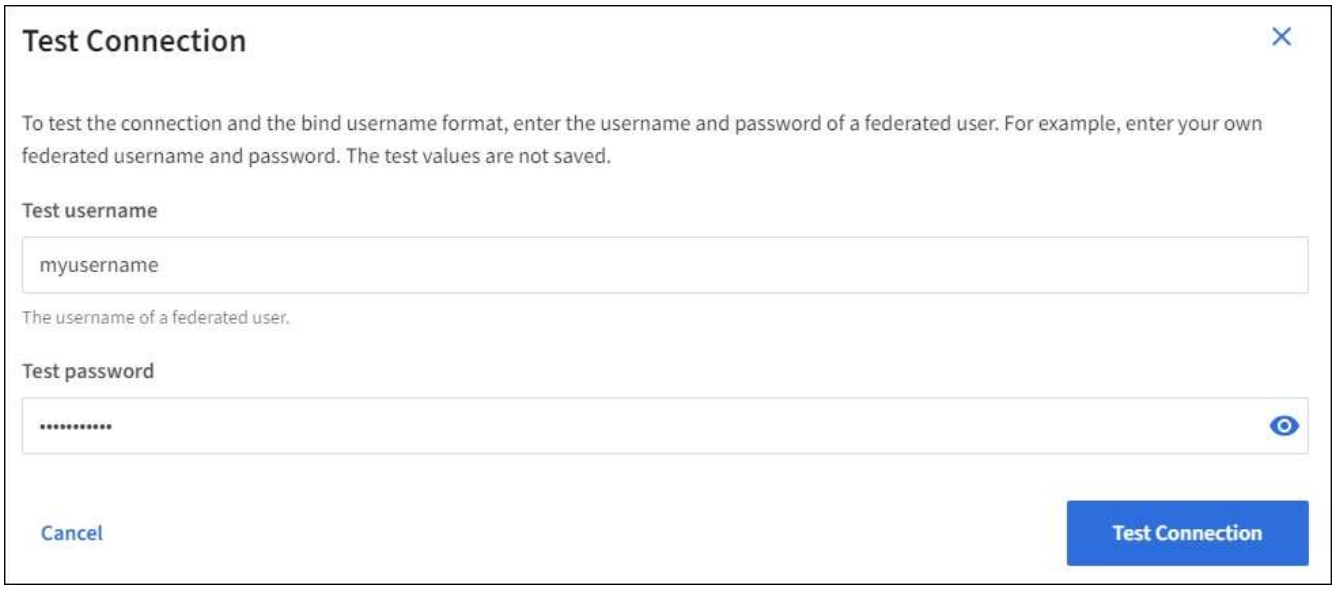
Comprueba la conexión y guarda la configuración

Una vez introducidos todos los valores, debes comprobar la conexión antes de poder guardar la configuración. StorageGRID verifica los parámetros de conexión del servidor LDAP y el formato del nombre de usuario de enlace, si has especificado alguno.

Pasos

1. Selecciona **Probar conexión**.
2. ${post_edited_translations.segment}
   - Si los parámetros de conexión son correctos, aparece el mensaje «Prueba de conexión realizada con éxito». Selecciona **Guardar** para guardar la configuración.
   - Aparecerá el mensaje «No se ha podido establecer una conexión de prueba» si la configuración de la conexión no es válida. Selecciona **Cerrar**. Luego, soluciona cualquier problema y vuelve a probar la conexión.
3. Si has especificado un formato de nombre de usuario de enlace, introduce el nombre de usuario y la contraseña de un usuario federado válido.

   Por ejemplo, introduce tu propio nombre de usuario y contraseña. No incluyas caracteres especiales en el nombre de usuario, como @ o /.



- Si los parámetros de conexión son correctos, aparece el mensaje «Prueba de conexión realizada con éxito». Selecciona **Guardar** para guardar la configuración.
- Aparece un mensaje de error si la configuración de la conexión, el formato del nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Soluciona cualquier problema y vuelve a probar la conexión.

Forzar la sincronización con la fuente de identidad

El sistema StorageGRID sincroniza periódicamente los grupos y usuarios federados desde la fuente de identidades. Puedes forzar la sincronización si quieres habilitar o restringir los permisos de los usuarios lo más rápido posible.

Pasos

1. Ve a la página de federación de identidades.
2. Selecciona **Sync server** en la parte superior de la página.

   El proceso de sincronización puede tardar un tiempo dependiendo de tu entorno.

   La alerta **Error de sincronización de la federación de identidades** se activa si hay un problema al sincronizar los grupos y usuarios federados desde la fuente de identidades.

${post_edited_translations.segment}

Puedes desactivar de forma temporal o permanente la federación de identidades para grupos y usuarios. Cuando la federación de identidades está desactivada, no hay comunicación entre StorageGRID y el origen de identidad. Sin embargo, se conserva cualquier configuración que hayas realizado, lo que te permitirá volver a activar fácilmente la federación de identidades en el futuro.

Acerca de esta tarea

Antes de desactivar la federación de identidades, debes tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que están conectados actualmente seguirán teniendo acceso al sistema StorageGRID hasta que su sesión expire, pero no podrán iniciar sesión después de que su sesión expire.

- No se llevará a cabo la sincronización entre el sistema StorageGRID y la fuente de identidades, y no se generarán alertas para las cuentas que no se hayan sincronizado.
- La casilla de selección **Habilitar federación de identidades** aparece desactivada si el estado del inicio de sesión único (SSO) es **Habilitado** o **Modo Sandbox**. El estado del SSO en la página de inicio de sesión único debe estar **Desactivado** antes de que puedas desactivar la federación de identidades. Consulta "Desactivar el inicio de sesión único".

Pasos

1. Ve a la página de federación de identidades.
2. Desmarca la casilla **Habilitar federación de identidades**.

Guía para configurar un servidor OpenLDAP

Si deseas utilizar un servidor OpenLDAP para la federación de identidades, debes configurar determinados parámetros en el servidor OpenLDAP.

> En el caso de 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 hayan sido desactivados externamente. Para bloquear el acceso a S3, elimina cualquier clave de S3 del usuario o elimina al usuario de todos los grupos.

${post_edited_translations.segment}

Los overlays memberof y refint deben estar habilitados. Para obtener más información, consulta las instrucciones para el mantenimiento de la pertenencia inversa a grupos en "Documentación de OpenLDAP: Guía del administrador versión 2.4".

Indexación

Debes configurar los siguientes atributos de 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, asegúrate de que los campos mencionados en la ayuda para Nombre de usuario estén indexados para un rendimiento óptimo.

Consulta la información sobre el mantenimiento inverso de la pertenencia a grupos en la "Documentación de OpenLDAP: Guía del administrador versión 2.4".

Administra grupos de administración en StorageGRID

Puedes crear grupos de administradores para gestionar los permisos de seguridad de uno o varios usuarios administradores. Los usuarios deben pertenecer a un grupo para que se les conceda acceso al sistema StorageGRID.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".

- Tienes "permisos de acceso específicos".
- ${post_edited_translations.segment}

Crear un grupo de administradores

${post_edited_translations.segment}

Accede al asistente

Pasos

1. ${post_edited_translations.segment}
2. Selecciona **Crear grupo**.

${post_edited_translations.segment}

Puedes crear un grupo local o importar un grupo federado.

- ${post_edited_translations.segment}
- Crea un grupo federado para importar usuarios desde la fuente de identidad.

Grupo local

Pasos

1. ${post_edited_translations.segment}
2. Introduce un nombre para mostrar para el grupo, que podrás modificar más adelante si es necesario. Por ejemplo, «Usuarios de mantenimiento» o «Administradores de ILM».
3. Introduce un nombre único para el grupo, que no podrás actualizar más adelante.
4. Selecciona **Continuar**.

${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}
2. Introduce el nombre del grupo que deseas importar, exactamente como aparece en la fuente de identidad configurada.
   - ${post_edited_translations.segment}
   - Para OpenLDAP, usa el CN (Common Name).
   - Para otro LDAP, utiliza el nombre único correspondiente para el servidor LDAP.
3. Selecciona **Continuar**.

${post_edited_translations.segment}

Pasos

1. Para **Modo de acceso**, selecciona si los usuarios del grupo pueden cambiar la configuración y realizar operaciones en el Grid Manager y la Grid Management API o si solo pueden ver la configuración y las funciones.
   - **Lectura/escritura** (por defecto): los usuarios pueden modificar la configuración y realizar las operaciones que les permiten sus permisos de gestión.

- **Solo lectura**: los usuarios solo pueden ver la configuración y las funciones. No pueden realizar ningún cambio ni llevar a cabo ninguna operación en el Grid Manager o la Grid Management API. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

> ${post_edited_translations.segment}

2. Selecciona uno o varios "Permisos del grupo admin".

   Debes 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 vas a crear un grupo local, selecciona **Continuar**. Si vas a crear un grupo federado, selecciona **Crear grupo** y **Finalizar**.

${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}

   Si aún no has creado usuarios locales, puedes guardar el grupo sin añadir usuarios. Puedes añadir este grupo al usuario en la página «Usuarios». Consulta "Gestiona usuarios" para obtener más información.

2. Selecciona **Crear grupo** y **Finalizar**.

${post_edited_translations.segment}

${post_edited_translations.segment}

- Para consultar la información básica de todos los grupos, revisa la tabla de la página «Grupos».
- ${post_edited_translations.segment}

Tarea	Menú de acciones	${post_edited_translations.segment}
${post_edited_translations.segment}	a. Selecciona la casilla para el grupo. b. Selecciona **Acciones** > **Ver detalles del grupo**.	${post_edited_translations.segment}
${post_edited_translations.segment}	a. Selecciona la casilla para el grupo. b. Selecciona **Acciones** > **Editar nombre del grupo**. c. ${post_edited_translations.segment} d. Selecciona **Guardar cambios**.	a. Selecciona el nombre del grupo para ver los detalles. b. Selecciona el icono de edición . c. ${post_edited_translations.segment} d. Selecciona **Guardar cambios**.

Tarea	Menú de acciones	${post_edited_translations.segment}
Editar el modo de acceso o los permisos	a. Selecciona la casilla para el grupo. b. Selecciona **Acciones** > **Ver detalles del grupo**. c. Opcionalmente, cambia el modo de acceso del grupo. d. Opcionalmente, selecciona o desmarca "Permisos del grupo admin". e. Selecciona **Guardar cambios**.	a. Selecciona el nombre del grupo para ver los detalles. b. Opcionalmente, cambia el modo de acceso del grupo. c. Opcionalmente, selecciona o desmarca "Permisos del grupo admin". d. Selecciona **Guardar cambios**.

Duplicar un grupo

Pasos

1. Selecciona la casilla para el grupo.
2. Selecciona **Acciones** > **Duplicar grupo**.
3. Completa el asistente para duplicar grupos.

Borrar un grupo

Puedes eliminar un grupo de administradores cuando quieras quitar el grupo del sistema y eliminar todos los permisos asociados con el grupo. Al eliminar un grupo de administradores, se eliminan los usuarios del grupo, pero no se eliminan los usuarios.

Pasos

1. En la página «Grupos», marca la casilla correspondiente a cada grupo que quieras eliminar.
2. Selecciona **Acciones** > **Eliminar grupo**.
3. Selecciona **Eliminar grupos**.

Permisos del grupo Admin en StorageGRID

Al crear grupos de usuarios administradores, seleccionas uno o varios permisos para controlar el acceso a funciones específicas de Grid Manager. Luego, puedes asignar a cada usuario a uno o varios de estos grupos de administradores para determinar qué tareas puede realizar ese usuario.

${post_edited_translations.segment}

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

- Inicia sesión en Grid Manager
- Ver el panel de control
- Ver las páginas de Nodes
- Ver alertas actuales y resueltas

- Cambiar su propia contraseña (solo usuarios locales)
- Ver determinada información que aparece en las páginas de Configuración y Mantenimiento

${post_edited_translations.segment}

Para todos los permisos, la configuración del **modo de acceso** del grupo determina si los usuarios pueden cambiar los ajustes y realizar operaciones o si solo pueden ver los ajustes y funciones relacionados. Si un usuario pertenece a varios grupos y cualquier grupo está configurado como **solo lectura**, el usuario tendrá acceso de solo lectura a todos los ajustes y funciones seleccionados.

En los apartados siguientes se describen los permisos que puedes asignar al crear o editar un grupo de administradores. Cualquier funcionalidad que no se mencione explícitamente requiere el permiso **Root access**.

Acceso a raíz

${post_edited_translations.segment}

${post_edited_translations.segment}

Este permiso proporciona acceso a la opción **Cambiar contraseña de root** en la página Tenants, lo que te permite controlar quién puede cambiar la contraseña del usuario raíz local del tenant. Este permiso también se utiliza para migrar claves S3 cuando la función de importación de claves S3 está habilitada. Los usuarios que no tengan este permiso no pueden ver la opción **Cambiar contraseña de root**.

Para conceder acceso a la página Tenants, que contiene la opción **Change root password**, asigna también el permiso **Tenant accounts**.

ILM

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

- ${post_edited_translations.segment}
- Políticas
- Etiquetas de políticas
- Grupos de almacenamiento
- Grados de almacenamiento
- Regiones
- Búsqueda de metadatos de objetos

${post_edited_translations.segment}

${post_edited_translations.segment}

Los usuarios deben tener el permiso de Mantenimiento para usar estas opciones:

- ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
- ${post_edited_translations.segment}

    - Nombres de dominio de los endpoints S3
- ${post_edited_translations.segment}
    - Decomisionar
    - Expansión
    - Comprobación de la existencia de un objeto
    - Recuperación
- **Mantenimiento** > **Sistema**:
    - Paquete de recuperación
    - Actualización de software
- **Soporte** > **Herramientas**:
    - Registros

Los usuarios que no tengan el permiso de Maintenance pueden ver, pero no editar, estas páginas:

- ${post_edited_translations.segment}
    - Servidores DNS
    - Red de grid
    - Servidores NTP
- **Mantenimiento** > **Sistema**:
    - Licencia
- ${post_edited_translations.segment}
    - Nombres de dominio de los endpoints S3
- ${post_edited_translations.segment}
    - Certificados
- **Configuración** > **Supervisión**:
    - ${post_edited_translations.segment}

Gestiona alertas

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

Consulta de métricas

Este permiso permite acceder a:

- **Soporte** > **Herramientas** > **Métricas** página
- ${post_edited_translations.segment}
- Tarjetas del panel de control de Grid Manager que contienen métricas

Búsqueda de metadatos de objetos

Este permiso permite acceder a la página **ILM** > **Búsqueda de metadatos de objetos**.

Otra configuración de grid

${post_edited_translations.segment}

- ${post_edited_translations.segment}
  - Grados de almacenamiento
- **Configuración** > **Sistema**:
- ${post_edited_translations.segment}
  - ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

- Acceso al E-Series SANtricity System Manager en los dispositivos de almacenamiento a través de Grid Manager.
- La posibilidad de realizar tareas de resolución de problemas y mantenimiento en la pestaña Manage drives para los dispositivos que admiten estas operaciones.

${post_edited_translations.segment}

Este permiso permite:

- ${post_edited_translations.segment}
- Ver las políticas de clasificación de tráfico existentes
- Ver las tarjetas del panel de Grid Manager que contienen los detalles de los inquilinos

Administra usuarios en StorageGRID

Puedes ver los usuarios locales y federados. También puedes crear usuarios locales y asignarlos a grupos de administradores locales para determinar a qué funciones de Grid Manager pueden acceder dichos usuarios.

Antes de empezar

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

${post_edited_translations.segment}

Puedes 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 de Grid Management API puede acceder el usuario.

Solo puedes crear usuarios locales. Utiliza la fuente de identidades externa para gestionar usuarios y grupos federados.

El Grid Manager incluye un usuario local predefinido, llamado "root". No puedes eliminar el usuario raíz.

${post_edited_translations.segment}

Accede al asistente

Pasos

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

${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}
2. Si lo deseas, selecciona **Sí** si este usuario no debe tener acceso a Grid Manager ni a Grid Management API.
3. Selecciona **Continuar**.

${post_edited_translations.segment}

Pasos

1. Si lo deseas, asigna al usuario a uno o varios grupos para determinar sus permisos.

   Si aún no has creado ningún grupo, puedes guardar el usuario sin seleccionar grupos. Puedes añadir este usuario a un grupo en la página Grupos.

   Si un usuario pertenece a varios grupos, los permisos son acumulativos. Consulta "${post_edited_translations.segment}" para ver los detalles.

2. Selecciona **Crear usuario** y selecciona **Finalizar**.

${post_edited_translations.segment}

Puedes consultar los detalles de los usuarios locales y federados existentes. Puedes modificar un usuario local para cambiar su nombre completo, contraseña o pertenencia a grupos. También puedes impedir temporalmente que un usuario acceda a Grid Manager y a la Grid Management API.

Solo puedes editar usuarios locales. Utiliza la fuente de identidades externa para gestionar usuarios federados.

- Para consultar la información básica de todos los usuarios locales y federados, revisa la tabla de la página Usuarios.
- Para ver todos los detalles de un usuario concreto, editar un usuario local o cambiar la contraseña de un usuario local, utiliza el menú **Acciones** o la página de detalles.

  Cualquier cambio se aplica la próxima vez que el usuario cierre sesión y vuelva a iniciar sesión en Grid Manager.

  > Los usuarios locales pueden cambiar sus propias contraseñas mediante la opción **Cambiar contraseña** del banner de Grid Manager.

Tarea	Menú de acciones	${post_edited_translations.segment}
Ver los datos del usuario	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment}	Selecciona el nombre del usuario en la tabla.

Tarea	Menú de acciones	${post_edited_translations.segment}
Editar nombre completo (solo usuarios locales)	a. ${post_edited_translations.segment} b. Selecciona **Acciones** > **Editar nombre completo**. c. ${post_edited_translations.segment} d. Selecciona **Guardar cambios**.	a. Selecciona el nombre del usuario para ver los detalles. b. Selecciona el icono de edición . c. ${post_edited_translations.segment} d. Selecciona **Guardar cambios**.
${post_edited_translations.segment}	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. Selecciona la pestaña Acceso. d. Selecciona **Sí** para impedir que el usuario inicie sesión en Grid Manager o en la Grid Management API, o selecciona **No** para permitirle iniciar sesión. e. Selecciona **Guardar cambios**.	a. Selecciona el nombre del usuario para ver los detalles. b. Selecciona la pestaña Acceso. c. Selecciona **Sí** para impedir que el usuario inicie sesión en Grid Manager o en la Grid Management API, o selecciona **No** para permitirle iniciar sesión. d. Selecciona **Guardar cambios**.
Cambiar contraseña (solo usuarios locales)	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. Selecciona la pestaña «Contraseña». d. ${post_edited_translations.segment} e. Selecciona **Cambiar contraseña**.	a. Selecciona el nombre del usuario para ver los detalles. b. Selecciona la pestaña «Contraseña». c. ${post_edited_translations.segment} d. Selecciona **Cambiar contraseña**.
Cambiar grupos (solo usuarios locales)	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. Selecciona la pestaña Grupos. d. Si lo deseas, selecciona el enlace que aparece junto al nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador. e. ${post_edited_translations.segment} f. Selecciona **Guardar cambios**.	a. Selecciona el nombre del usuario para ver los detalles. b. Selecciona la pestaña Grupos. c. Si lo deseas, selecciona el enlace que aparece junto al nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador. d. ${post_edited_translations.segment} e. Selecciona **Guardar cambios**.

Importar usuarios federados

Puedes importar uno o varios usuarios federados, hasta un máximo de 100 usuarios, directamente en la página de Usuarios.

Pasos

1. Selecciona **Configuración** > **Control de acceso** > **Usuarios administradores**.
2. Selecciona **Importar usuarios federados**.

3. Introduce el UUID o el nombre de usuario de uno o varios usuarios federados.

   ${post_edited_translations.segment}

4. ${post_edited_translations.segment}

   Si la importación al campo «Usuarios» falla para uno o varios usuarios, realiza los siguientes pasos:

   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}

   Después de que cierres el cuadro de diálogo **Importar usuarios federados**, la información de los usuarios federados importados correctamente se muestra en la página Usuarios.

Duplicar un usuario

${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}
2. Selecciona **Acciones** > **Duplicar usuario**.
3. ${post_edited_translations.segment}

Eliminar un usuario

Puedes eliminar un usuario local para borrarlo definitivamente del sistema.

> No puedes eliminar el usuario raíz.

Pasos

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Selecciona **Eliminar usuario**.

Utiliza el inicio de sesión único (SSO)

Conoce StorageGRID SSO

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

El sistema StorageGRID admite el inicio de sesión único (SSO) mediante el estándar Security Assertion Markup Language 2.0 (SAML 2.0).

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

Inicia sesión cuando el inicio de sesión único está habilitado

Cuando el SSO está activado y te conectas a StorageGRID, se te redirige a la página de SSO de tu organización para validar tus credenciales.

Pasos

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

   Aparece la página de Sign in de StorageGRID.

   - Si es la primera vez que accedes a la URL desde este navegador, se te pedirá que introduzcas un ID de cuenta.
   - Si ya has accedido anteriormente al Grid Manager o al Tenant Manager, se te pedirá que selecciones una cuenta reciente o que introduzcas un ID de cuenta.

   > La página de inicio de sesión de StorageGRID no aparece cuando introduces la URL completa de una cuenta de inquilino (es decir, un dominio completo o una dirección IP seguida de `/?accountId=20-digit-account-id`). En su lugar, te redirigen inmediatamente a la página de inicio de sesión único (SSO) de tu organización, donde puedes inicia sesión con tus credenciales de SSO.

2. Indica si deseas acceder al Grid Manager o al Tenant Manager:
   - Para acceder al Grid Manager, deja en blanco el campo **ID de cuenta**, introduce **0** como ID de cuenta o selecciona **Grid Manager** si aparece en la lista de cuentas recientes.
   - Para acceder al Gestor de inquilinos, introduce el ID de cuenta del inquilino de 20 dígitos o selecciona un inquilino por su nombre si aparece en la lista de cuentas recientes.
3. Selecciona **Sign in**

   StorageGRID te redirige a la página de inicio de sesión único (SSO) de tu organización. Por ejemplo:

4. Inicia sesión con tus credenciales de SSO.

   Si tus credenciales de SSO son correctas:

   a. El proveedor de identidad (IdP) proporciona una respuesta de autenticación a StorageGRID.
   b. StorageGRID valida la respuesta de autenticación.
   c. Si la respuesta es válida y perteneces a un grupo federado con permisos de acceso a StorageGRID, has iniciado sesión en Grid Manager o en Tenant Manager, dependiendo de la cuenta que hayas seleccionado.

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

5. Si lo deseas, accede a otros nodos de administración o accede al Grid Manager o al Tenant Manager, si tienes los permisos adecuados.

   No es necesario que vuelvas a introducir tus credenciales de SSO.

Cerrar sesión cuando el SSO está activado

Cuando el SSO está habilitado para StorageGRID, lo que ocurre al cerrar sesión depende de en qué hayas iniciado sesión y desde dónde la cierres.

Pasos

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

   Aparece la página de Sign in de StorageGRID. El menú desplegable **Cuentas recientes** se actualiza para incluir **Grid Manager** o el nombre del inquilino, así puedes acceder a estas interfaces de usuario más rápido en el futuro.

   La tabla resume lo que ocurre al cerrar sesión si estás usando una sola sesión del navegador. Si has iniciado sesión en StorageGRID en varias sesiones del navegador, debes cerrar sesión en todas ellas por separado.

Si has iniciado sesión en…	Y cierras sesión en…	Se te ha desconectado de…
Grid Manager en uno o varios nodos de administración	Grid Manager en cualquier nodo de administración	Grid Manager en todos los nodos de administración **Nota:** Si utilizas Entra ID para el inicio de sesión único, es posible que tardes unos minutos en cerrar sesión en todos los nodos de administración.
Tenant Manager en uno o varios nodos de administración	Tenant Manager en cualquier nodo de administración	Tenant Manager en todos los nodos de administración
Tanto Grid Manager como Tenant Manager	Grid Manager	Solo el Grid Manager. También debes cerrar la sesión en el Tenant Manager para cerrar la sesión de inicio de sesión único.

Requisitos y consideraciones para StorageGRID SSO

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

Requisitos del proveedor de identidad

StorageGRID es compatible con los siguientes proveedores de identidad (IdP) de SSO:

- Servicio de federación de Active Directory (AD FS)
- Microsoft Entra ID
- PingFederate

Debes configurar la federación de identidades para tu sistema StorageGRID antes de poder configurar un

proveedor de identidades de SSO. El tipo de servicio LDAP que utilices para la federación de identidades controla qué tipo de SSO puedes implementar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad de SSO
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

Requisitos de AD FS

Puedes utilizar cualquiera de las siguientes versiones de AD FS:

- ${post_edited_translations.segment}
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 debería estar usando el "${post_edited_translations.segment}", o una versión superior.

Requisitos adicionales

- ${post_edited_translations.segment}
- Microsoft .NET Framework, versión 3.5.1 o superior

${post_edited_translations.segment}

Si utilizas Entra ID como tipo de SSO y los usuarios tienen nombres principales de usuario que no usan sAMAccountName como prefijo, pueden ocurrir problemas de inicio de sesión si StorageGRID pierde la conexión con el servidor LDAP. Para permitir que los usuarios inicien sesión, debes restablecer la conexión con el servidor LDAP.

${post_edited_translations.segment}

De forma predeterminada, StorageGRID utiliza un certificado de interfaz de gestión en cada nodo de administración para proteger el acceso a Grid Manager, Tenant Manager, la Grid Management API y la Tenant Management API. Cuando configuras relaciones de confianza con partes de confianza (AD FS), aplicaciones empresariales (Entra ID) o conexiones de proveedor de servicios (PingFederate) para StorageGRID, utilizas el certificado de servidor como certificado de firma para las solicitudes de StorageGRID.

Si aún no has "he configurado un certificado personalizado para la interfaz de gestión", deberías hacerlo ahora. Cuando instalas un certificado de servidor personalizado, este se utiliza para todos los Admin Nodes, y puedes usarlo en todas las relying party trusts de StorageGRID, aplicaciones empresariales o conexiones SP.

No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en una relación de confianza de parte confiable, una aplicación empresarial o una conexión SP. Si el nodo falla y lo recuperas, se genera un nuevo certificado de servidor predeterminado. Antes de poder iniciar sesión en el nodo recuperado, debes actualizar la relación de confianza de parte confiable, la aplicación empresarial o la conexión SP con el nuevo certificado.

Puedes acceder al certificado de servidor de un Admin Node iniciando sesión en la línea de comandos del nodo y yendo al directorio `/var/local/mgmt-api`. Un certificado de servidor personalizado se llama `custom-server.crt`. El certificado de servidor predeterminado del nodo se llama `server.crt`.

Requisitos de puertos

El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debes utilizar el puerto HTTPS predeterminado (443) si deseas que los usuarios se autentiquen mediante el inicio de sesión único. Consulta "Controla el acceso en el cortafuegos externo".

Comprueba que los usuarios federados puedan iniciar sesión en StorageGRID

Antes de habilitar el inicio de sesión único (SSO), debes comprobar que al menos un usuario federado pueda iniciar sesión en Grid Manager y en Tenant Manager para cualquier cuenta de inquilino existente.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Ya has configurado la federación de identidades.

Pasos

1. Si ya existen cuentas de inquilinos, comprueba que ninguno de los inquilinos esté usando su propia fuente de identidad.

   Cuando habilitas el SSO, el origen de identidad configurado en el Tenant Manager se sustituye por el origen de identidad configurado en el Grid Manager. Los usuarios que pertenecen al origen de identidad del inquilino ya no podrán iniciar sesión a menos que tengan una cuenta en el origen de identidad del Grid Manager.

   a. Inicia sesión en Tenant Manager con cada cuenta de inquilino.
   b. Selecciona **Gestión de acceso** > **Federación de identidades**.
   c. Comprueba que la casilla **Habilitar federación de identidades** no esté marcada.
   d. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
   a. En Grid Manager, selecciona **Configuración** > **Control de acceso** > **Grupos de administradores**.
   b. Asegúrate de que se haya importado al menos un grupo federado desde la fuente de identidades de Active Directory y de que se le haya asignado el permiso de acceso Root.
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}

3. Si ya existen cuentas de inquilinos, confirma que un usuario federado con permiso de acceso de usuario raíz pueda iniciar sesión:
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. En la pestaña «Introducir datos», selecciona **Continuar**.
   d. Si la casilla **Usar fuente de identidad propia** está marcada, desmárcala y selecciona **Guardar**.

      ${post_edited_translations.segment}

   e. ${post_edited_translations.segment}
   f. ${post_edited_translations.segment}
   g. ${post_edited_translations.segment}
   h. ${post_edited_translations.segment}
   i. Confirma que puedes volver a iniciar sesión en el inquilino como usuario del grupo federado.

Información relacionada

- "Requisitos y aspectos a tener en cuenta para el inicio de sesión único"
- "${post_edited_translations.segment}"
- "Utiliza una cuenta de inquilino"

Configura el inicio de sesión único en StorageGRID

Puedes seguir el asistente Configurar SSO y entrar en el modo sandbox para configurar y probar el inicio de sesión único (SSO) antes de habilitarlo para todos los usuarios de StorageGRID. Después de habilitar el SSO, puedes volver al modo sandbox cuando lo necesites para cambiar o volver a probar la configuración.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".
- Has configurado la federación de identidades para tu sistema StorageGRID.
- ${post_edited_translations.segment}

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad de SSO
Servicio de federación de Active Directory (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

Acerca de esta tarea

Cuando el SSO está habilitado y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidad del SSO. A su vez, el proveedor de identidad

del SSO envía una respuesta de autenticación a StorageGRID, indicando si la solicitud de autenticación fue exitosa. Para solicitudes exitosas:

- 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 que StorageGRID (el proveedor de servicios) y el proveedor de identidad SSO puedan comunicarse de forma segura sobre las solicitudes de autenticación de los usuarios, deberás realizar estas tareas:

1. Configura los ajustes en StorageGRID.
2. Utiliza el software del proveedor de identidad de SSO para crear una confianza de parte confiable (AD FS), una aplicación empresarial (Entra ID) o un proveedor de servicios (PingFederate) para cada Admin Node.
3. Vuelve a StorageGRID para activar el inicio de sesión único.

El modo sandbox facilita realizar esta configuración iterativa y probar todos los ajustes antes de habilitar SSO. Cuando usas el modo sandbox, los usuarios no pueden iniciar sesión mediante SSO.

Accede al asistente

Pasos

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

   > ⓘ Si el botón «Configurar ajustes de SSO» aparece desactivado, comprueba que hayas configurado el proveedor de identidad como fuente de identidad federada. Consulta "Requisitos y aspectos a tener en cuenta para el inicio de sesión único".

2. Selecciona **Configurar ajustes de SSO**. Aparece la página «Proporcionar datos del proveedor de identidad».

Facilita los datos del proveedor de identidad

Pasos

1. Selecciona el **tipo de SSO** en la lista desplegable.
2. Si has seleccionado Active Directory como tipo de SSO, introduce el **nombre del servicio de federación** del proveedor de identidad, tal y como aparece en el Servicio de federación de Active Directory (AD FS).

   > ⓘ Para localizar el nombre del servicio de federación, ve al Administrador de servidores de Windows Server. Selecciona **Herramientas** > **Administración de AD FS**. En el menú Acción, selecciona **Editar propiedades del servicio de federación**. El nombre del servicio de federación aparece en el segundo campo.

3. Especifica qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe la información de configuración de inicio de sesión único en respuesta a las solicitudes de StorageGRID.
   - **Utilizar el certificado de CA del sistema operativo**: Utiliza el certificado de CA predeterminado instalado en el sistema operativo para proteger la conexión.
   - **Utilizar un certificado de CA personalizado**: Utiliza un certificado de CA personalizado para proteger la conexión.

Si seleccionas esta opción, copia el texto del certificado personalizado y pégalo en el cuadro de texto **Certificado de la CA**.

- **No utilices TLS**: No utilices un certificado TLS para proteger la conexión.

> Si cambias el certificado de la CA, "Reinicia el servicio mgmt-api en los nodos de administración" y prueba que el inicio de sesión único en Grid Manager funciona correctamente.

4. Selecciona **Continuar**. Aparece la página Proporcionar identificador de la parte confiable.

Proporciona el identificador de la parte que confía

1. Rellena los campos de la página Proporcionar el identificador de la parte que confía según el tipo de SSO que seleccionaste.

Active Directory

a. Especifica el **identificador de la parte de confianza** para StorageGRID. Este valor controla el nombre que usas para cada relación de confianza con una parte de confianza en AD FS.

   - Por ejemplo, si tu grid solo tiene un Admin Node y no tienes previsto añadir más Admin Nodes en el futuro, introduce `SG` o `StorageGRID`.
   - Si tu grid incluye más de un Admin Node, incluye la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]`. Incluir esta cadena da como resultado una tabla que muestra el identificador de la relying party para cada Admin Node en el grid, basado en el hostname del nodo.

   > Debes crear una relación de confianza de parte confiable para cada Admin Node en tu sistema StorageGRID. Contar con una relación de confianza de parte confiable para cada Admin Node garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier Admin Node.

b. Selecciona **Guardar y entrar en modo sandbox**.

Entra ID

a. En la sección «Aplicación empresarial», especifica el **nombre de la aplicación empresarial** para StorageGRID. Este valor controla el nombre que usas para cada aplicación empresarial en Entra ID.

   - Por ejemplo, si tu grid solo tiene un Admin Node y no tienes previsto añadir más Admin Nodes en el futuro, introduce `SG` o `StorageGRID`.
   - Si tu grid incluye más de un Admin Node, incluye la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]`. Incluir esta cadena da como resultado una tabla que muestra un nombre de aplicación empresarial para cada Admin Node en tu sistema, basado en el hostname del nodo.

   > Debes crear una aplicación empresarial para cada nodo de administración de tu sistema StorageGRID. Contar con una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier nodo de administración.

b. Sigue los pasos en "Crear aplicaciones empresariales en Entra ID" para crear una aplicación empresarial para cada Admin Node que aparece en la tabla.

c. En Entra ID, copia la URL de metadatos de federación de cada aplicación empresarial. Luego, pega esta URL en el campo correspondiente **Federation metadata URL** en StorageGRID.

d. Una vez que hayas copiado y pegado una URL de metadatos de federación para todos los nodos de administración, selecciona **Guardar y entrar en modo sandbox**.

PingFederate

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

   - Por ejemplo, si tu grid solo tiene un Admin Node y no tienes previsto añadir más Admin Nodes en el futuro, introduce `SG` o `StorageGRID`.
   - Si tu grid incluye más de un Admin Node, incluye la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]`. Incluir esta cadena da como resultado una tabla que muestra

el ID de conexión SP de cada Admin Node en tu sistema, según el hostname del nodo.

> Debes crear una conexión SP para cada nodo de administración de tu sistema StorageGRID. Disponer de una conexión SP para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

b. Indica la URL de los metadatos de la federación para cada Admin Node en el campo **Federation metadata URL**.

   Utiliza el siguiente formato:

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

c. Selecciona **Guardar y entrar en modo sandbox**.

Configura relaciones de confianza de terceros, aplicaciones empresariales o conexiones SP

Después de guardar la configuración y entrar en el modo de prueba, puedes completar y probar la configuración para el tipo de SSO que seleccionaste.

StorageGRID puede permanecer en modo «sandbox» todo el tiempo que sea necesario. Sin embargo, solo pueden iniciar sesión los usuarios federados y los usuarios locales.

Active Directory

Pasos

1. Ve a Servicios de federación de Active Directory (AD FS).
2. Crea una o varias relaciones de confianza con las partes confiables para StorageGRID, usando cada identificador de parte confiable que aparece en la tabla de la página Configurar SSO.

   Debes crear un trust para cada Admin Node que aparece en la tabla.

   Para obtener instrucciones, visita "Crear relaciones de confianza de terceros en AD FS".

Entra ID

Pasos

1. En la página de inicio de sesión único del Admin Node en el que has iniciado sesión actualmente, selecciona el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en tu grid, repite estos pasos:
   a. Inicia sesión en el nodo.
   b. Selecciona **Configuración** > **Control de acceso** > **inicio de sesión único**.
   c. Descarga y guarda los metadatos SAML de ese nodo.
3. Accede al portal de Azure.
4. Sigue los pasos en "Crear aplicaciones empresariales en Entra ID" para cargar el archivo de metadatos SAML de cada Admin Node en su aplicación empresarial de Entra ID correspondiente.

PingFederate

Pasos

1. En la página de inicio de sesión único del Admin Node en el que has iniciado sesión actualmente, selecciona el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en tu grid, repite estos pasos:
   a. Inicia sesión en el nodo.
   b. Selecciona **Configuración** > **Control de acceso** > **inicio de sesión único**.
   c. Descarga y guarda los metadatos SAML de ese nodo.
3. Entra en PingFederate.
4. "Crea una o varias conexiones de proveedor de servicios (SP) para StorageGRID". Utiliza el ID de conexión SP de cada nodo de administración (que aparece en la tabla de la página Configurar SSO) y los metadatos SAML que descargaste para ese nodo de administración.

   Debes crear una conexión SP para cada nodo de administración que aparece en la tabla.

Configuración de prueba

Antes de aplicar el inicio de sesión único en todo tu sistema StorageGRID, comprueba que el inicio de sesión único y el cierre de sesión único estén correctamente configurados en cada Admin Node.

Active Directory

Pasos

1. En la página Configurar SSO, busca el enlace en el paso Probar la configuración del asistente.

   La URL se deriva del valor que has introducido en el campo **Federation service name**.

2. Selecciona el enlace o copia y pega la URL en un navegador para acceder a la página de inicio de sesión de tu proveedor de identidad.
3. Para confirmar que puedes utilizar el inicio de sesión único (SSO) para iniciar sesión en StorageGRID, selecciona **Sign in to one of the following sites**, selecciona el identificador de la parte de confianza correspondiente a tu nodo de administración principal y selecciona **Sign in**.
4. Introduce tu nombre de usuario y contraseña federados.
   - Si el inicio de sesión y el cierre de sesión mediante SSO se realizan correctamente, aparece un mensaje de éxito.
   - Si la operación de SSO no se realiza correctamente, aparece un mensaje de error. Soluciona el problema, borra las cookies del navegador e inténtalo de nuevo.
5. Repite estos pasos para comprobar la conexión de inicio de sesión único (SSO) de cada Admin Node en tu grid.

Entra ID

Pasos

1. Accede a la página de inicio de sesión único en el portal de Azure.
2. Selecciona **Probar esta aplicación**.
3. Introduce las credenciales de un usuario federado.
   - Si el inicio de sesión y el cierre de sesión mediante SSO se realizan correctamente, aparece un mensaje de éxito.
   - Si la operación de SSO no se realiza correctamente, aparece un mensaje de error. Soluciona el problema, borra las cookies del navegador e inténtalo de nuevo.
4. Repite estos pasos para comprobar la conexión de inicio de sesión único (SSO) de cada Admin Node en tu grid.

PingFederate

Pasos

1. En la página Configurar SSO, selecciona el primer enlace en el mensaje de modo Sandbox.

   Selecciona y comprueba un enlace cada vez.

2. Introduce las credenciales de un usuario federado.
   - Si el inicio de sesión y el cierre de sesión mediante SSO se realizan correctamente, aparece un mensaje de éxito.
   - Si la operación de SSO no se realiza correctamente, aparece un mensaje de error. Soluciona el problema, borra las cookies del navegador e inténtalo de nuevo.
3. Selecciona el siguiente enlace para verificar la conexión de inicio de sesión único para cada Admin Node en tu grid.

   Si aparece el mensaje «Página caducada», selecciona el botón **Atrás** de tu navegador y vuelve a

introducir tus credenciales.

Habilitar el inicio de sesión único

Cuando hayas comprobado que puedes usar el inicio de sesión único (SSO) para acceder a cada nodo de administración, puedes habilitar el inicio de sesión único para todo tu sistema StorageGRID.

> Cuando el SSO está habilitado, todos los usuarios deben usar el SSO para acceder al Grid Manager, al Tenant Manager, a la Grid Management API y a la Tenant Management API. Los usuarios locales ya no pueden acceder a StorageGRID.

Pasos

1. En el paso «Configuración de la prueba» del asistente de configuración de SSO, selecciona **Enable SSO**.
2. Lee el mensaje de advertencia y selecciona **Enable SSO**.

   El inicio de sesión único ya está activado. Aparece la página de inicio de sesión único y ahora incluye los detalles del SSO que acabas de configurar.
3. Para editar la configuración, selecciona **Editar**.
4. Para desactivar el inicio de sesión único, selecciona **Desactivar SSO**.

> Si utilizas el Portal de Azure y accedes a StorageGRID desde el mismo ordenador que usas para acceder a Entra ID, asegúrate de que el usuario del Portal de Azure también sea un usuario autorizado de StorageGRID (un usuario de un grupo federado que se haya importado a StorageGRID) o cierra la sesión del Portal de Azure antes de intentar iniciar sesión en StorageGRID.

Crea confianzas de terceros en AD FS para StorageGRID

Debes utilizar los Servicios de federación de Active Directory (AD FS) para crear una relación de confianza de parte confiable para cada nodo de administración de tu sistema. Puedes crear relaciones de confianza de parte confiable usando comandos de PowerShell, importando metadatos SAML desde StorageGRID o introduciendo los datos manualmente.

Antes de empezar

- ${post_edited_translations.segment}
- Tienes "ha entrado en modo sandbox" en Grid Manager.
- Conoces el nombre de dominio completo (o la dirección IP) y el identificador de la parte de confianza de cada nodo de administración en tu sistema. Puedes encontrar estos valores en la tabla de detalles de los nodos de administración en la página StorageGRID Configure SSO.

  > Debes crear una relación de confianza de parte confiable para cada Admin Node en tu sistema StorageGRID. Contar con una relación de confianza de parte confiable para cada Admin Node garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier Admin Node.

- ${post_edited_translations.segment}

- Estás utilizando el complemento de administración de AD FS y perteneces al grupo Administrators.
- ${post_edited_translations.segment}

Acerca de esta tarea

Estas instrucciones se aplican a Windows Server 2016 AD FS. Si utilizas una versión diferente de AD FS, notarás ligeras diferencias en el procedimiento. Consulta la documentación de Microsoft AD FS si tienes preguntas.

Crea una relación de confianza de parte confiable usando Windows PowerShell

Puedes usar Windows PowerShell para crear rápidamente una o más relaciones de confianza con la parte de confianza.

Pasos

1. En el menú de inicio de Windows, haz clic con el botón derecho en el icono de PowerShell y selecciona **Ejecutar como administrador**.
2. En el símbolo del sistema de PowerShell, introduce el siguiente comando:

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

   - Para *`Admin_Node_Identifier`*, introduce el identificador de la parte de confianza para el Admin Node, exactamente como aparece en la página de inicio de sesión único. Por ejemplo, `SG-DC1-ADM1`.
   - Para *`Admin_Node_FQDN`*, introduce el nombre de dominio completo para ese mismo nodo de administración. (Si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces aquí una dirección IP, ten en cuenta que deberás actualizar o volver a crear esta relación de confianza entre partes si esa dirección IP llega a cambiar.)
3. En el Administrador de servidores de Windows Server, selecciona **Herramientas** > **Administración de AD FS**.

   ${post_edited_translations.segment}

4. Selecciona **AD FS** > **Relying Party Trusts**.

   ${post_edited_translations.segment}

5. Añade una política de control de acceso a la relación de confianza de parte confiable recién creada:
   a. Busca la confianza de la parte confiable que acabas de crear.
   b. Haz clic con el botón derecho del ratón sobre la confianza y selecciona **Editar política de control de acceso**.
   c. Selecciona una política de control de acceso.
   d. ${post_edited_translations.segment}
6. Agrega una directiva de emisión de declaraciones a la nueva relación de confianza de la parte confiable:
   a. Busca la confianza de la parte confiable que acabas de crear.
   b. Haz clic con el botón derecho del ratón sobre la confianza y selecciona **Editar política de emisión de reclamaciones**.
   c. Selecciona **Add rule**.
   d. En la página «Seleccionar plantilla de regla», selecciona **Enviar atributos LDAP como**

reclamaciones en la lista y selecciona **Siguiente**.

e. En la página Configurar regla, introduce un nombre para mostrar para esta regla.

   Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.

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

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

h. En la columna Outgoing Claim Type de la tabla de correspondencias, selecciona **Name ID** en la lista desplegable.

i. Selecciona **Finalizar** y, a continuación, **OK**.

7. Comprueba que los metadatos se hayan importado correctamente.

   a. Haz clic con el botón derecho del ratón sobre la confianza de la parte dependiente para abrir sus propiedades.

   b. Comprueba que los campos de las pestañas **Puntos finales**, **Identificadores** y **Firma** estén rellenados.

      ${post_edited_translations.segment}

8. Repite estos pasos para configurar una relación de confianza de parte confiable para todos los nodos de administración en tu sistema StorageGRID.

9. Cuando hayas terminado, vuelve a StorageGRID y "${post_edited_translations.segment}" para confirmar que están configurados correctamente.

Crea una relación de confianza con una parte confiable importando metadatos de federación

Puedes importar los valores de cada relación de confianza de la parte que confía accediendo a los metadatos SAML de cada Admin Node.

Pasos

1. En el Administrador de servidores de Windows Server, selecciona **Herramientas** y, a continuación, selecciona **Administración de AD FS**.
2. En Acciones, selecciona **Add Relying Party Trust**.
3. En la página de bienvenida, elige **Claims aware** y selecciona **Start**.
4. ${post_edited_translations.segment}
5. En **Dirección de metadatos de la federación (nombre de host o URL)**, escribe la ubicación de los metadatos SAML de este nodo de administración:

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

   Para *`Admin_Node_FQDN`*, introduce el nombre de dominio completo para ese mismo nodo de administración. (Si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces aquí una dirección IP, ten en cuenta que deberás actualizar o volver a crear esta relación de confianza entre partes si esa dirección IP llega a cambiar.)

6. ${post_edited_translations.segment}

Al introducir el nombre para mostrar, utiliza el identificador de la parte de confianza del nodo de administración, exactamente como aparece en la página de inicio de sesión único de Grid Manager. Por ejemplo, `SG-DC1-ADM1`.

7. Agrega una regla de reclamación:
   a. Haz clic con el botón derecho del ratón sobre la confianza y selecciona **Editar política de emisión de reclamaciones**.
   b. Selecciona **Add rule**:
   c. En la página «Seleccionar plantilla de regla», selecciona **Enviar atributos LDAP como reclamaciones** en la lista y selecciona **Siguiente**.
   d. En la página Configurar regla, introduce un nombre para mostrar para esta regla.

      Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.

   e. Para el almacén de atributos, selecciona **Active Directory**.
   f. En la columna Atributo LDAP de la tabla de asignación, escribe **objectGUID** o selecciona **User-Principal-Name**.
   g. En la columna Outgoing Claim Type de la tabla de correspondencias, selecciona **Name ID** en la lista desplegable.
   h. Selecciona **Finalizar** y, a continuación, **OK**.
8. Comprueba que los metadatos se hayan importado correctamente.
   a. Haz clic con el botón derecho del ratón sobre la confianza de la parte dependiente para abrir sus propiedades.
   b. Comprueba que los campos de las pestañas **Puntos finales**, **Identificadores** y **Firma** estén rellenados.

      ${post_edited_translations.segment}

9. Repite estos pasos para configurar una relación de confianza de parte confiable para todos los nodos de administración en tu sistema StorageGRID.
10. Cuando hayas terminado, vuelve a StorageGRID y "${post_edited_translations.segment}" para comprobar que están configurados correctamente.

Crear una relación de confianza de parte confiable manualmente

${post_edited_translations.segment}

Pasos

1. En el Administrador de servidores de Windows Server, selecciona **Herramientas** y, a continuación, selecciona **Administración de AD FS**.
2. En Acciones, selecciona **Add Relying Party Trust**.
3. En la página de bienvenida, elige **Claims aware** y selecciona **Start**.
4. Selecciona **Introducir manualmente los datos de la parte confiable** y selecciona **Siguiente**.
5. Completa el asistente de confianza de la parte que confía:

   a. ${post_edited_translations.segment}

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

b. ${post_edited_translations.segment}

c. En la página «Configurar URL», selecciona la casilla **Habilitar compatibilidad con el protocolo WebSSO de SAML 2.0**.

d. Escribe la URL del punto final del servicio SAML para el nodo de administración:

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

Para *`Admin_Node_FQDN`*, introduce el nombre de dominio completo para el Admin Node. (Si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces una dirección IP aquí, ten en cuenta que deberás actualizar o volver a crear esta relying party trust si esa dirección IP cambia en algún momento.)

e. En la página Configurar identificadores, especifica el Relying Party Identifier para el mismo Admin Node:

`Admin_Node_Identifier`

Para *`Admin_Node_Identifier`*, introduce el identificador de la parte de confianza para el Admin Node, exactamente como aparece en la página de inicio de sesión único. Por ejemplo, `SG-DC1-ADM1`.

f. ${post_edited_translations.segment}

Aparece el cuadro de diálogo «Edit Claim Issuance Policy».

> Si no aparece el cuadro de diálogo, haz clic con el botón derecho sobre la relación de confianza y selecciona **Editar política de emisión de reclamaciones**.

6. ${post_edited_translations.segment}

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

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

Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.

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

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

e. En la columna Outgoing Claim Type de la tabla de correspondencias, selecciona **Name ID** en la lista desplegable.

f. Selecciona **Finalizar** y, a continuación, **OK**.

7. Haz clic con el botón derecho del ratón sobre la confianza de la parte dependiente para abrir sus propiedades.

8. En la pestaña **Puntos finales**, configura el punto final para el cierre de sesión único (SLO):

a. Selecciona **Add SAML**.

b. ${post_edited_translations.segment}

c. Selecciona **Binding** > **Redirect**.

d. En el campo **URL de confianza**, introduce la URL utilizada para el cierre de sesión único (SLO) desde este Admin Node:

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

Para *`Admin_Node_FQDN`*, introduce el nombre de dominio completo del nodo de administración. (si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces una dirección IP aquí, ten en cuenta que deberás actualizar o volver a crear esta relación de confianza entre partes si esa dirección IP cambia en algún momento).

a. Selecciona **Aceptar**.

9. En la pestaña **Firma**, especifica el certificado de firma para esta relación de confianza de parte confiable:

a. Agrega el certificado personalizado:

- Si dispones del certificado de gestión personalizado que has subido a StorageGRID, selecciona ese certificado.
- Si no tienes el certificado personalizado, inicia sesión en el Admin Node, ve al directorio `/var/local/mgmt-api` del Admin Node y añade el archivo de certificado `custom-server.crt`.

> No se recomienda utilizar el certificado predeterminado del nodo de administración (`server.crt`). Si el nodo de administración falla, el certificado predeterminado se volverá a generar al recuperar el nodo, y será necesario actualizar la confianza de la parte que confía.

b. Selecciona **Aplicar** y selecciona **Aceptar**.

Se guardan y se cierran las propiedades de la parte que confía.

10. Repite estos pasos para configurar una relación de confianza de parte confiable para todos los nodos de administración en tu sistema StorageGRID.
11. Cuando hayas terminado, vuelve a StorageGRID y "${post_edited_translations.segment}" para comprobar que están configurados correctamente.

Crea aplicaciones empresariales en Entra ID para StorageGRID

Utiliza Entra ID para crear una aplicación empresarial para cada Admin Node en tu sistema.

Antes de empezar

- ${post_edited_translations.segment}
- Tienes "ha entrado en modo sandbox" en Grid Manager.
- Tienes el **nombre de la aplicación empresarial** para cada nodo de administración de tu sistema. Puedes copiar estos valores de la tabla de detalles del nodo de administración en la página Configurar SSO.

Debes crear una aplicación empresarial para cada nodo de administración de tu sistema StorageGRID. Contar con una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier nodo de administración.

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Tienes uno de los siguientes roles en la cuenta de Entra ID: Global Administrator, Cloud Application Administrator, Application Administrator o propietario del service principal.

Accede a Entra ID

Pasos

1. Inicia sesión en el "${post_edited_translations.segment}".
2. Accede a "Entra ID".
3. Selecciona "Aplicaciones empresariales".

${post_edited_translations.segment}

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

Pasos

1. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. Selecciona **Crear tu propia aplicación**.
   c. ${post_edited_translations.segment}
   d. Deja seleccionado el botón de opción **Integrar cualquier otra aplicación que no encuentres en la galería (fuera de la galería)**.
   e. Selecciona **Crear**.
   f. Selecciona el enlace **Empezar** en el recuadro **2. Configura el inicio de sesión único**, o selecciona el enlace **Inicio de sesión único** en el margen izquierdo.
   g. Selecciona la casilla **SAML**.
   h. ${post_edited_translations.segment}
   i. Ve a la página «Configurar SSO» y pega la URL en el campo **URL de metadatos de federación** que corresponde al **Enterprise application name** que usaste.
2. Una vez que hayas pegado la URL de metadatos de la federación para cada nodo de administración y hayas realizado todos los demás cambios necesarios en la configuración de SSO, selecciona **Guardar** en la página Configure SSO.

${post_edited_translations.segment}

Una vez guardada la configuración de SSO, puedes descargar un archivo de metadatos SAML para cada nodo de administración en tu sistema StorageGRID.

Pasos

1. ${post_edited_translations.segment}
   a. Inicia sesión en StorageGRID desde el nodo de administración.
   b. Selecciona **Configuración** > **Control de acceso** > **inicio de sesión único**.
   c. Pulsa el botón para descargar los metadatos SAML de ese nodo de administración.
   d. Guarda el archivo, que luego subirás a Entra ID.

Sube los metadatos SAML a cada aplicación empresarial

${post_edited_translations.segment}

Pasos

1. Vuelve al Portal de Azure.
2. Repite estos pasos para cada aplicación empresarial:

   > Es posible que tengas que actualizar la página de aplicaciones de Enterprise para ver en la lista las aplicaciones que añadiste anteriormente.

   a. Ve a la página Propiedades de la aplicación empresarial.
   b. Establece **Asignación obligatoria** en **No** (a menos que quieras configurar las asignaciones por separado).
   c. Accede a la página de inicio de sesión único.
   d. Completa la configuración de SAML.
   e. Pulsa el botón **Cargar archivo de metadatos** y selecciona el archivo de metadatos SAML que descargaste para el Admin Node correspondiente.
   f. Una vez que se cargue el archivo, selecciona **Guardar** y luego selecciona **X** para cerrar el panel. Regresarás a la página Configurar el inicio de sesión único con SAML.
3. "Prueba cada aplicación".

Crea conexiones de proveedores de servicios en PingFederate para StorageGRID

Utilizas PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración en tu sistema. Para agilizar el proceso, importarás los metadatos SAML desde StorageGRID.

Antes de empezar

- Has configurado el inicio de sesión único para StorageGRID y seleccionaste **Ping Federate** como tipo de SSO.
- Tienes "ha entrado en modo sandbox" en Grid Manager.
- Dispones del **ID de conexión SP** de cada nodo de administración de tu sistema. Puedes encontrar estos valores en la tabla de detalles de los nodos de administración en la página Configurar SSO.
- Has descargado los **metadatos SAML** de cada nodo de administración en tu sistema.
- Tienes experiencia creando conexiones de SP en PingFederate Server.
- Tienes el "${post_edited_translations.segment}" para PingFederate Server. La documentación de PingFederate ofrece instrucciones detalladas paso a paso y explicaciones.

- Tienes el "Permiso de administrador" para PingFederate Server.

Acerca de esta tarea

Estas instrucciones resumen cómo configurar PingFederate Server versión 10.3 como proveedor de SSO para StorageGRID. Si estás usando otra versión de PingFederate, puede que necesites adaptar estas instrucciones. Consulta la documentación de PingFederate Server para obtener instrucciones detalladas para tu versión.

Completa los requisitos previos en PingFederate

Antes de poder crear las conexiones SP que utilizarás para StorageGRID, debes completar las tareas previas en PingFederate. Utilizarás la información de estos requisitos previos cuando configures las conexiones SP.

${post_edited_translations.segment}

Si aún no lo has hecho, crea un almacén de datos para conectar PingFederate al servidor LDAP de AD FS. Utiliza los valores que usaste al "${post_edited_translations.segment}" en StorageGRID.

- ${post_edited_translations.segment}
- **Tipo de LDAP**: Active Directory
- **Nombre del atributo binario**: Introduce **objectGUID** en la pestaña de atributos binarios de LDAP exactamente como se muestra.

${post_edited_translations.segment}

Si aún no lo has hecho, crea un validador de credenciales de contraseña.

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **Filtro de búsqueda**: sAMAccountName=${username}
- ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

Pasos

1. Ve a **Autenticación** > **Integración** > **Adaptadores de IdP**.
2. Selecciona **Crear nueva instancia**.
3. En la pestaña Tipo, selecciona **HTML Form IdP Adapter**.
4. En la pestaña «Adaptador IdP», selecciona **Add a new row to 'Credential Validators'**.
5. Selecciona el ${post_edited_translations.segment} que creaste.
6. En la pestaña «Atributos del adaptador», selecciona el atributo **username** para **Pseudonym**.
7. Selecciona **Guardar**.

Crear o importar un certificado de firma

Si aún no lo has hecho, crea o importa el certificado de firma.

Pasos

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

Crea una conexión de SP en PingFederate

Al crear una conexión SP en PingFederate, debes importar los metadatos SAML que descargaste de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos que necesitas.

> Debes crear una conexión de SP para cada nodo de administración en tu sistema StorageGRID, de modo que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo. Usa estas instrucciones para crear la primera conexión de SP. Luego, ve a Crear conexiones SP adicionales para crear las conexiones adicionales que necesites.

${post_edited_translations.segment}

Pasos

1. Ve a **Aplicaciones** > **Integración** > **Conexiones SP**.
2. Selecciona **Crear conexión**.
3. ${post_edited_translations.segment}
4. Selecciona **Perfiles de SSO del navegador** y **SAML 2.0** como el protocolo.

Importar metadatos de SP

Pasos

1. En la pestaña «Importar metadatos», selecciona **File**.
2. Selecciona el archivo de metadatos SAML que descargaste desde la página Configurar SSO para el nodo de administración.
3. Revisa el resumen de metadatos y la información que aparece en la pestaña General Info.

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

4. Selecciona **Siguiente**.

Configura el inicio de sesión único (SSO) del IdP en el navegador

Pasos

1. En la pestaña SSO del navegador, selecciona **Configurar SSO del navegador**.
2. En la pestaña «Perfiles SAML», selecciona las opciones **SSO iniciado por el SP**, **SLO iniciado por el SP**, **SSO iniciado por el IdP** y **SLO iniciado por el IdP**.
3. Selecciona **Siguiente**.
4. En la pestaña «Duración de la afirmación», no hagas ningún cambio.

5. En la pestaña «Creación de aserciones», selecciona **Configurar la creación de aserciones**.
   a. En la pestaña Asignación de identidad, selecciona **Estándar**.
   b. En la pestaña «Contrato de atributos», usa **SAML_SUBJECT** como contrato de atributos y el formato de nombre no especificado que se importó.
6. Para "Extend the Contract", selecciona **Eliminar** para quitar el `urn:oid`, que no se usa.

Instancia del adaptador de mapas

Pasos

1. ${post_edited_translations.segment}
2. En la pestaña Adapter instance, selecciona el instancia del adaptador que creaste.
3. En la pestaña «Método de asignación», selecciona **Recuperar atributos adicionales de un almacén de datos**.
4. En la pestaña «Fuente de atributos y búsqueda de usuarios», selecciona **Add Attribute Source**.
5. En la pestaña Data Store, proporciona una descripción y selecciona el almacén de datos que añadiste.
6. En la pestaña «Búsqueda en el directorio LDAP»:
   - ${post_edited_translations.segment}
   - Para el Search Scope, selecciona **Subtree**.
   - En la clase de objeto raíz, busca y añade cualquiera de estos atributos: **objectGUID** o **userPrincipalName**.
7. En la pestaña «Tipos de codificación de atributos binarios LDAP», selecciona **Base64** para el atributo **objectGUID**.
8. En la pestaña «Filtro LDAP», introduce **sAMAccountName=${username}**.
9. En la pestaña «Cumplimiento del contrato de atributos», selecciona **LDAP (atributo)** en el menú desplegable «Origen» y selecciona **objectGUID** o **userPrincipalName** en el menú desplegable «Valor».
10. ${post_edited_translations.segment}
11. En la pestaña «Failsave Attribute Source», selecciona **Abort the SSO Transaction**.
12. ${post_edited_translations.segment}
13. Selecciona **Hecho**.

Configura los ajustes del protocolo

Pasos

1. ${post_edited_translations.segment}
2. En la pestaña «URL del servicio de consumidor de aserciones», acepta los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**POST** para Binding y `/api/saml-response` para Endpoint URL).
3. En la pestaña «URL de servicio SLO», acepta los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**REDIRECT** para Binding y `/api/saml-logout` para Endpoint URL.
4. En la pestaña «Enlaces SAML permitidos», desmarca **ARTIFACT** y **SOAP**. Solo son obligatorios **POST** y **REDIRECT**.
5. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}

7. Revisa el resumen y selecciona **Hecho** para guardar la configuración del protocolo.
8. Revisa el resumen y selecciona **Hecho** para guardar la configuración de SSO del navegador.

Configura credenciales

Pasos

1. ${post_edited_translations.segment}
2. En la pestaña «Credenciales», selecciona **Configurar credenciales**.
3. Selecciona el ${post_edited_translations.segment} que creaste o importaste.
4. ${post_edited_translations.segment}
   a. En la pestaña Trust Model, selecciona **Unanchored**.
   b. En la pestaña «Certificado de verificación de firma», revisa la información del certificado de firma, que se importó desde los metadatos SAML de StorageGRID.
5. Revisa las pantallas de resumen y selecciona **Guardar** para guardar la conexión SP.

Crear conexiones SP adicionales

Puedes copiar la primera conexión SP para crear las conexiones SP que necesites para cada Admin Node en tu grid. Subes nuevos metadatos para cada copia.

> Las conexiones SP para los distintos nodos de administración utilizan una configuración idéntica, salvo en lo que respecta al Partner's Entity ID, la Base URL, el Connection ID, el Connection Name, la verificación de la firma y la SLO Response URL.

Pasos

1. Selecciona **Acción** > **Copiar** para crear una copia de la conexión SP inicial para cada Admin Node adicional.
2. ${post_edited_translations.segment}
3. Selecciona el archivo de metadatos correspondiente al nodo de administración:
   a. Selecciona **Action** > **Actualizar con metadatos**.
   b. Selecciona **Elegir archivo** y sube los metadatos.
   c. Selecciona **Siguiente**.
   d. Selecciona **Guardar**.
4. Soluciona el error provocado por el atributo no utilizado:
   a. Selecciona la nueva conexión.
   b. Selecciona **Configurar SSO del navegador > Configurar la creación de aserciones > Contrato de atributos**.
   c. ${post_edited_translations.segment}
   d. Selecciona **Guardar**.

Desactiva el inicio de sesión único en StorageGRID

Puedes desactivar el inicio de sesión único (SSO) si ya no quieres usar esta funcionalidad. Debes desactivar el inicio de sesión único antes de poder desactivar la

federación de identidades.

Antes de empezar

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

Pasos

1. Selecciona **Configuración** > **Control de acceso** > **inicio de sesión único**.

   Aparece la página de inicio de sesión único.

2. Selecciona **Desactivar SSO**.
3. Selecciona **Sí**.

   Aparece un mensaje de aviso en el que se indica que los usuarios locales ahora podrán iniciar sesión.

La próxima vez que inicies sesión en StorageGRID, aparece la página de Sign in de StorageGRID y debes introducir el nombre de usuario y la contraseña de un usuario local o federado de StorageGRID.

Deshabilita temporalmente y vuelve a habilitar SSO para un nodo de administración StorageGRID

Es posible que no puedas iniciar sesión en el Grid Manager si el sistema de inicio de sesión único (SSO) deja de funcionar. En este caso, puedes desactivar y volver a activar temporalmente el SSO para un nodo de administración. Para desactivar y luego volver a activar el SSO, debes acceder al shell de comandos del nodo.

Antes de empezar

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

Acerca de esta tarea

Después de deshabilitar el SSO para un nodo de administración, puedes iniciar sesión en el Grid Manager como el usuario raíz local. Para proteger tu sistema StorageGRID, debes usar el shell de comandos del nodo para volver a habilitar el SSO en el nodo de administración tan pronto como cierres sesión.

> Desactivar el SSO en un nodo de administración no afecta la configuración del SSO de los demás nodos de administración en la grid. La casilla **Habilitar SSO** en la página de inicio de sesión único en el Grid Manager permanece seleccionada y todos los ajustes de SSO existentes se mantienen a menos que los actualices.

Pasos

1. Inicia sesión en un nodo de administración:
   a. Introduce el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
   c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
   d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

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

   Un mensaje indica que el comando solo se aplica a este Admin Node.

3. ${post_edited_translations.segment}

   Aparece un mensaje que indica que el inicio de sesión único está desactivado en el nodo.

4. Desde un navegador web, accede al Grid Manager en el mismo nodo de administración.

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

5. ${post_edited_translations.segment}
6. Si has desactivado temporalmente el SSO porque tenías que corregir la configuración del SSO:
   a. Selecciona **Configuración** > **Control de acceso** > **inicio de sesión único**.
   b. ${post_edited_translations.segment}
   c. Selecciona **Guardar**.

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

7. Si has desactivado temporalmente el SSO porque necesitabas acceder al Grid Manager por cualquier otro motivo:

   a. ${post_edited_translations.segment}
   b. Selecciona **Cerrar sesión** y cierra el Grid Manager.
   c. Vuelve a activar el SSO en el nodo de administración. Puedes seguir cualquiera de los siguientes pasos:

      - Ejecuta el siguiente comando: `enable-saml`

        Un mensaje indica que el comando solo se aplica a este Admin Node.

      Confirma que deseas activar el inicio de sesión único.

   Aparece un mensaje que indica que el inicio de sesión único está activado en el nodo.

   ◦ Reinicia el nodo de grid: `reboot`

8. ${post_edited_translations.segment}
9. Comprueba que aparece la página de Sign in de StorageGRID y que debes introducir tus credenciales de SSO para acceder a Grid Manager.

${post_edited_translations.segment}

Conoce la federación de grid de StorageGRID

Puedes utilizar la federación de grid para clonar inquilinos y replicar sus objetos entre

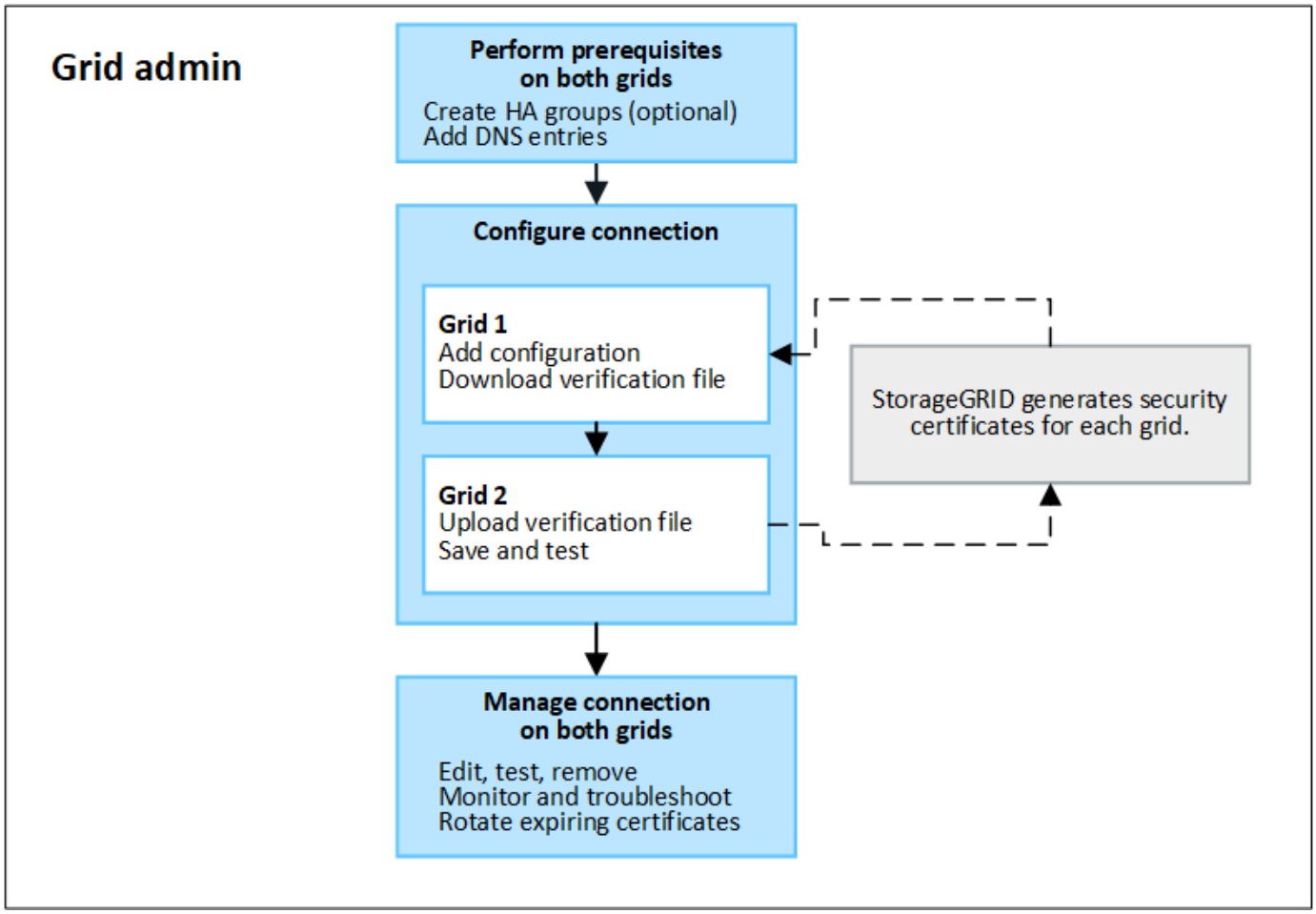
dos sistemas StorageGRID para recuperación ante desastres.

¿Qué es una conexión de federación de grid?

Una conexión de federación de grid es una conexión bidireccional, confiable y segura entre los nodos Admin y Gateway en dos sistemas StorageGRID.

Flujo de trabajo para la federación de grid

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



${post_edited_translations.segment}

- Las redes utilizadas para la federación de redes deben ejecutar versiones de StorageGRID que sean idénticas o que no tengan más de una diferencia de versión principal entre ellas.

  Para obtener más información sobre los requisitos de versión, consulta la "Notas de publicación". Debes iniciar sesión con tu cuenta de NetApp o crear una cuenta para acceder a las notas de la versión.

- Un grid puede tener una o más conexiones de federación de grid con otros 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 existe ninguna conexión implícita entre Grid 2 y Grid 3.
- Las conexiones de la federación de redes son bidireccionales. Después de que se establece la conexión, puedes supervisar y gestionar la conexión desde cualquiera de las dos redes.

- Debe existir al menos una conexión a la federación de grid para que puedas usar "clon de cuenta" o "replicación entre grids".

Requisitos de red y dirección IP

- Las conexiones de la federación de grid pueden ocurrir en la Grid Network, Admin Network o Client Network.
- Una conexión de federación de grid conecta un grid con otro grid. La configuración de cada grid especifica un endpoint de federación de grid en el otro grid, que consiste en Admin Nodes, Gateway Nodes o ambos.
- La mejor práctica es conectar "grupos de alta disponibilidad (HA)" de nodos de Gateway y de administración en cada grid. El uso de grupos de HA ayuda a garantizar que las conexiones de federación de grid permanezcan en línea si los nodos dejan de estar disponibles. Si la interfaz activa de cualquiera de los grupos de HA falla, la conexión puede usar una interfaz de respaldo.
- No se recomienda crear una conexión de federación de grid que use la dirección IP de un solo Admin Node o Gateway Node. Si el nodo deja de estar disponible, la conexión de federación de grid también dejará de estar disponible.
- "Replicación entre grids" El almacenamiento de objetos requiere que los nodos de almacenamiento de cada grid puedan acceder a los nodos de administración y Gateway configurados en el otro grid. Para cada grid, comprueba que todos los nodos de almacenamiento tengan una ruta con alto ancho de banda hacia los nodos de administración o Gateway utilizados para la conexión.

Utiliza nombres de dominio completos (FQDN) para equilibrar la carga de la conexión

En un entorno de producción, utiliza nombres de dominio completos (FQDN) para identificar cada grid en la conexión. Luego, crea las entradas DNS correspondientes, así:

- El FQDN de Grid 1 está asociado a una o varias direcciones IP virtuales (VIP) de los grupos de alta disponibilidad (HA) en Grid 1 o a la dirección IP de uno o varios nodos Admin o Gateway en Grid 1.
- El FQDN de Grid 2 asignado a una o varias direcciones VIP de Grid 2 o a la dirección IP de uno o varios nodos Admin o Gateway en Grid 2.

Cuando usas varias entradas DNS, las solicitudes para usar la conexión se distribuyen de la siguiente manera:

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

Requisitos de puertos

Al crear una conexión de federación de grid, puedes especificar cualquier número de puerto no utilizado entre 23000 y 23999. Ambos grids en esta conexión usarán el mismo puerto.

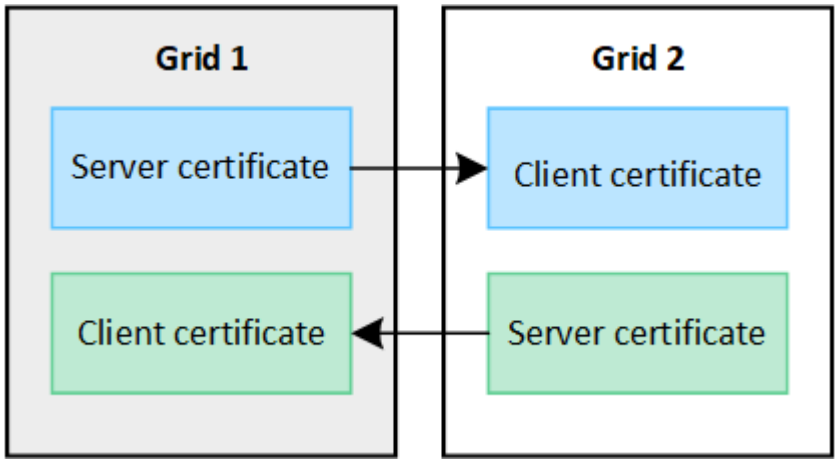
Debes asegurarte de que ningún nodo de ninguna de las dos grids utilice este puerto para otras conexiones.

Requisitos del certificado

${post_edited_translations.segment}

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

- ${post_edited_translations.segment}



De forma predeterminada, los certificados tienen una validez de 730 días (2 años). Cuando estos certificados se acercan a su fecha de caducidad, la alerta **Expiration of grid federation certificate** te recuerda que debes renovarlos, lo cual puedes hacer usando el Grid Manager.

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

Más información

- "Crear conexiones de federación de grid"
- "Gestiona las conexiones de la federación de grid"
- "${post_edited_translations.segment}"

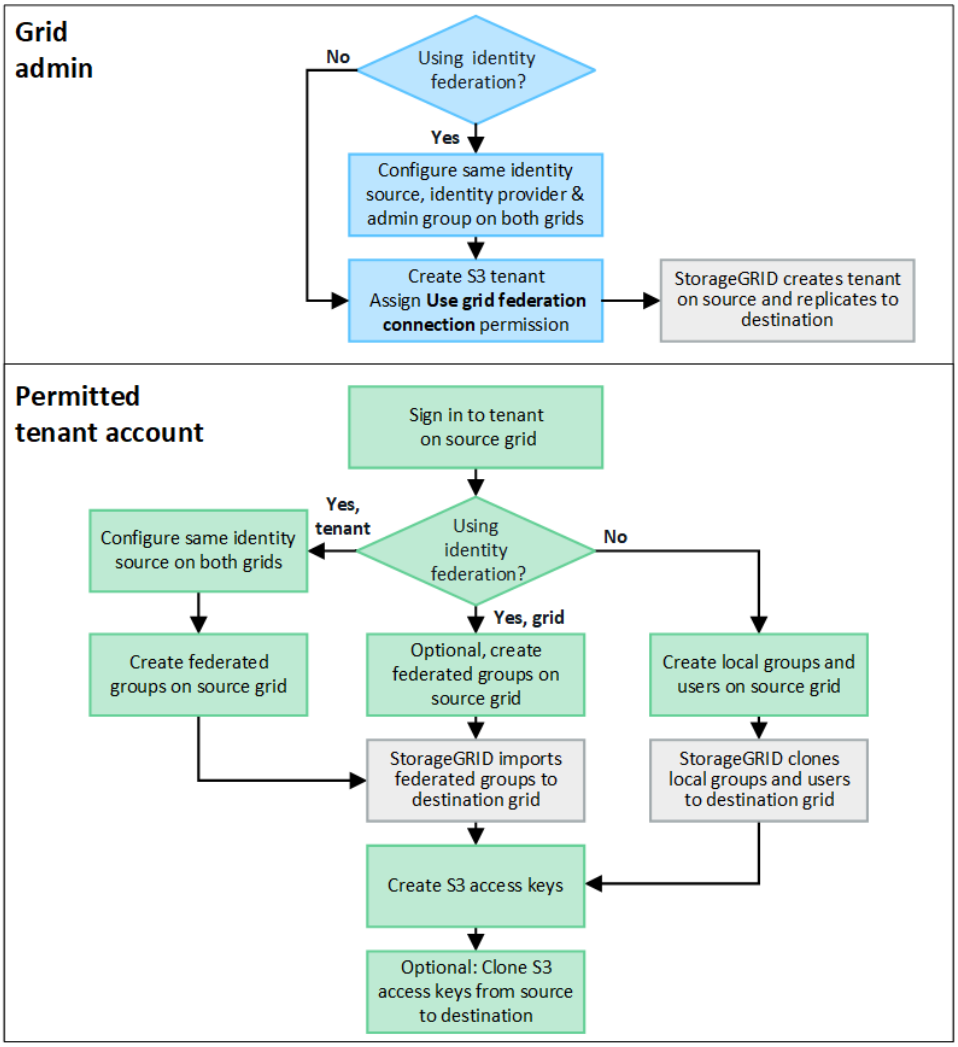
Conoce la clonación de cuentas en StorageGRID

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

Es necesario clonar la cuenta para "replicación entre grids". Clonar la información de la cuenta desde un sistema StorageGRID de origen a un sistema StorageGRID de destino garantiza que los usuarios y grupos de los inquilinos puedan acceder a los buckets y objetos correspondientes en cualquiera de las dos grids.

Flujo de trabajo para la clonación de cuentas

El diagrama de flujo muestra los pasos que los administradores de grid y los inquilinos permitidos realizarán para configurar la clonación de cuentas. Estos pasos se realizan después del "La conexión de federación de grid está configurada".



${post_edited_translations.segment}

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

${post_edited_translations.segment}

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

Pasos

1. Configura el mismo origen de identidad para ambos grids. Consulta "Usa la federación de identidades".
2. Configura el mismo proveedor de identidad de inicio de sesión único (SSO) para ambos grids. Consulta "${post_edited_translations.segment}".
3. "${post_edited_translations.segment}" en ambos grids al importar el mismo grupo federado.

   Al crear el inquilino, deberás seleccionar este grupo para que tenga el permiso de acceso a raíz inicial tanto para la cuenta de inquilino de origen como para la de destino.

Si este grupo de administradores no existe en ambas grids antes de crear el tenant, el tenant no se replica en el destino.

${post_edited_translations.segment}

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

Pasos

1. Configura el mismo origen de identidad para ambos grids. Consulta "Usa la federación de identidades".
2. Opcionalmente, si un grupo federado va a tener permiso de acceso de usuario raíz inicial tanto para las cuentas de inquilino de origen como de destino, "${post_edited_translations.segment}" en ambas grids importando el mismo grupo federado.

   Si asignas el permiso de acceso de usuario raíz a un grupo federado que no existe en ambas grids, el tenant no se replica en la grid de destino.

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

Crear cuenta de inquilino S3 permitida

Después de configurar opcionalmente SSO o federación de identidades, un administrador de grid realiza estos pasos para determinar qué tenants pueden replicar objetos de los buckets a otros sistemas StorageGRID.

Pasos

1. Determina qué grid quieres que sea el grid de origen del inquilino para las operaciones de clonación de cuentas.

   La red en la que se crea inicialmente el inquilino se conoce como la *red de origen* del inquilino. La red en la que se replica el inquilino se conoce como la *red de destino* del inquilino.

2. En esa cuadrícula, crea una nueva cuenta de inquilino de S3 o edita una cuenta existente.
3. Asigna el permiso **Usar conexión de federación de grid**.
4. ${post_edited_translations.segment}

   Si se asigna este permiso, tanto la cuenta del inquilino de origen como la de destino deben configurar la misma fuente de identidad antes de crear grupos federados. Los grupos federados añadidos al inquilino de origen no se pueden clonar en el inquilino de destino a menos que ambas grids utilicen la misma fuente de identidad.

5. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Si has seleccionado un usuario local para que tenga permiso de acceso de usuario raíz en el inquilino,

ese usuario se clona en el inquilino de destino. Sin embargo, la contraseña de ese usuario no se clona.

Para más detalles, consulta "Gestiona los inquilinos permitidos para la federación de grid".

Flujo de trabajo permitido para la cuenta de inquilino

Después de que un inquilino con el permiso **Use grid federation connection** se replica en la grid de destino, las cuentas de inquilino autorizadas pueden seguir estos pasos para clonar grupos de inquilinos, usuarios y claves de acceso S3.

Pasos

1. Inicia sesión en la cuenta del inquilino en el grid de origen del inquilino.
2. Si está permitido, configura la federación de identidad tanto en la cuenta del inquilino de origen como en la de destino.
3. Crea grupos y usuarios en el tenant 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 realiza ninguna clonación desde el inquilino de destino hacia el de origen.

4. ${post_edited_translations.segment}
5. Opcionalmente, clona las claves de acceso S3 del inquilino de origen al inquilino de destino.

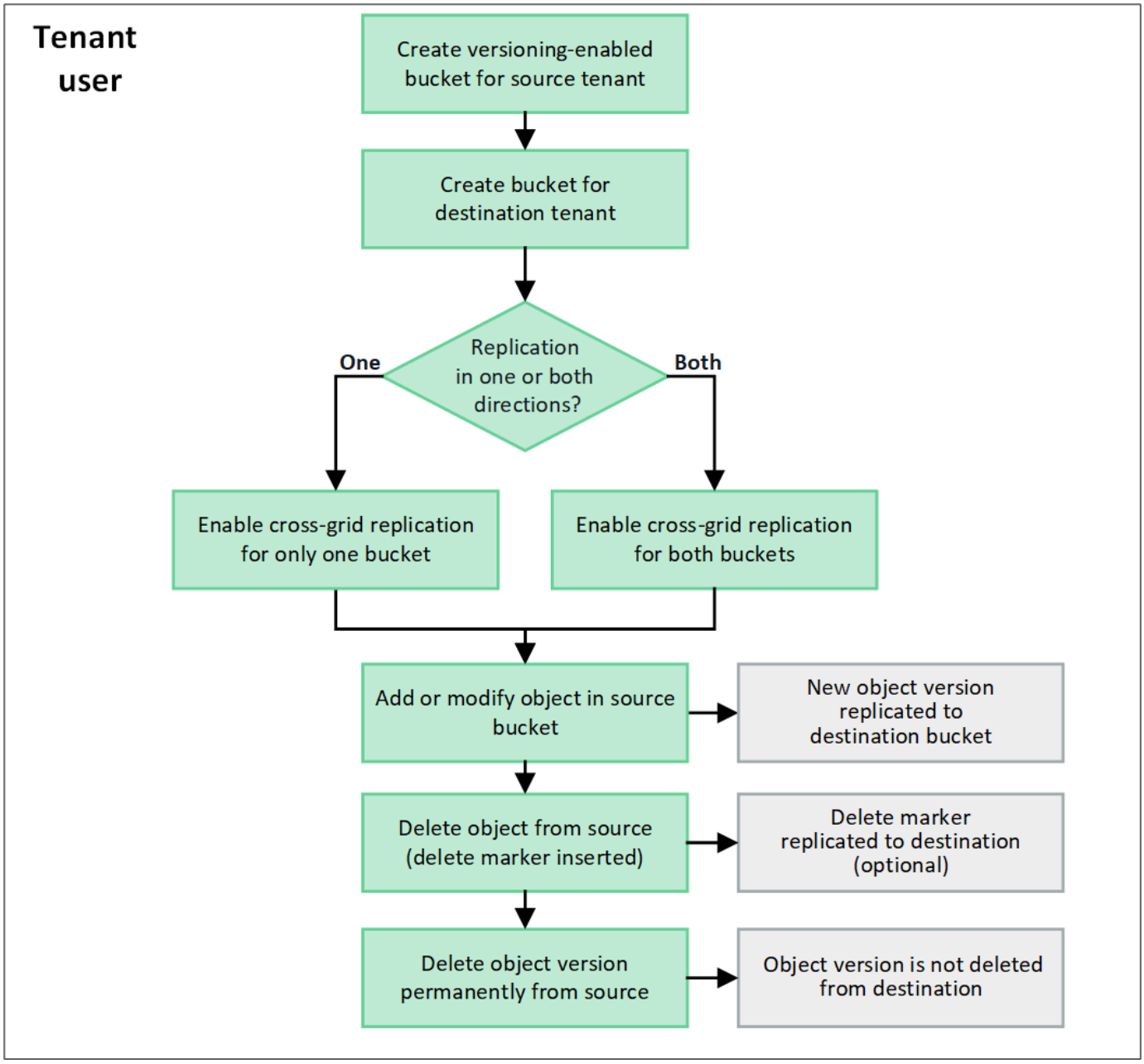
Para obtener más información sobre el flujo de trabajo permitido para las cuentas de inquilino y para saber cómo se clonan los grupos, los usuarios y las claves de acceso S3, consulta "Clonar grupos de inquilinos y usuarios" y "Clonar claves de acceso a S3 mediante la API".

Conoce la replicación entre grids en StorageGRID

La replicación entre grids es la replicación automática de objetos entre buckets S3 seleccionados en dos sistemas StorageGRID que están conectados en una "conexión de federación de grid". "${post_edited_translations.segment}" es necesario para la replicación entre grids.

${post_edited_translations.segment}

${post_edited_translations.segment}



${post_edited_translations.segment}

Si una cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** para usar una o más "${post_edited_translations.segment}", un usuario de inquilino con permiso de acceso raíz puede crear buckets en las cuentas de inquilino correspondientes de cada grid. Estos buckets:

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Debe estar vacío

${post_edited_translations.segment}

Más información

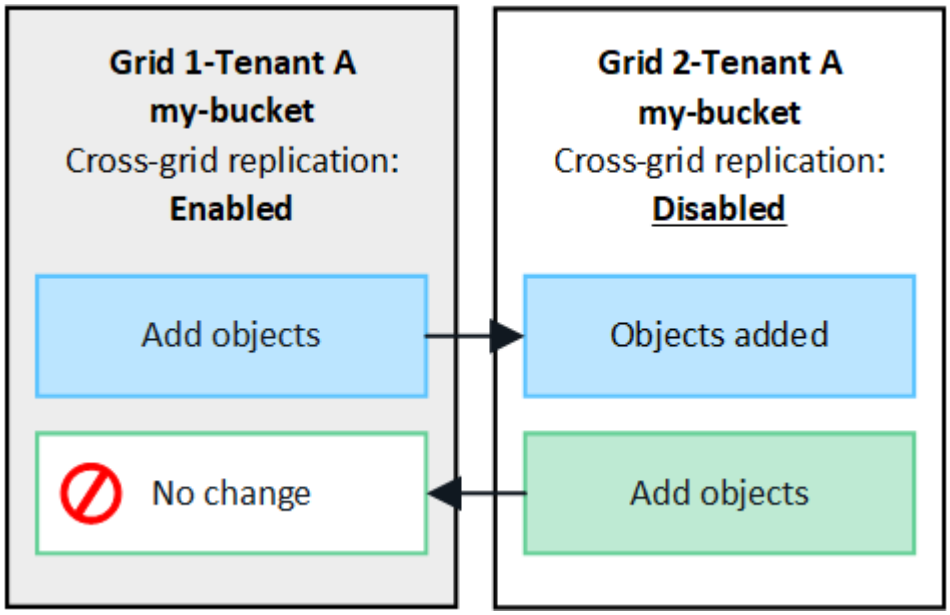
"${post_edited_translations.segment}"

${post_edited_translations.segment}

Puedes configurar la replicación entre redes para que se realice en una sola dirección o en ambas direcciones.

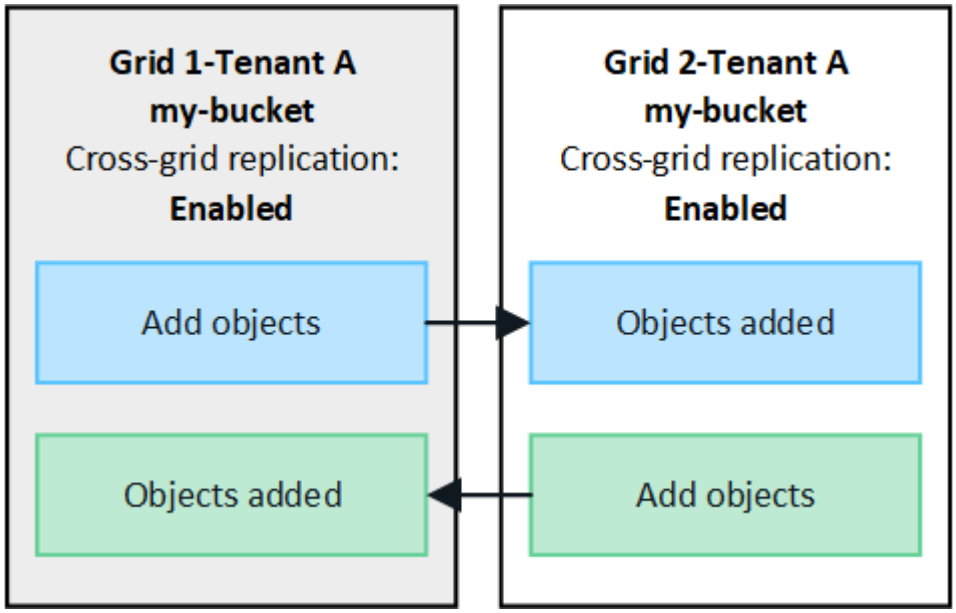
${post_edited_translations.segment}

Si habilitas la replicación entre redes para un bucket en solo una red, los objetos añadidos a ese bucket (el bucket de origen) se replican al bucket correspondiente en la otra red (el bucket de destino). Sin embargo, los objetos añadidos al bucket de destino no se replican de vuelta al de origen. En la figura, la replicación entre redes está habilitada para `my-bucket` desde Grid 1 a Grid 2, pero no está habilitada en la otra dirección.



${post_edited_translations.segment}

Si habilitas la replicación entre grids para el mismo bucket en ambos grids, los objetos añadidos a cualquiera de los buckets se replican en el otro grid. En la figura, la replicación entre grids está habilitada para `my-bucket` en ambas direcciones.



¿Qué ocurre cuando se ingieren objetos?

${post_edited_translations.segment}

1. StorageGRID replica automáticamente el objeto desde el bucket de origen al bucket de destino. El tiempo necesario para realizar esta operación de replicación en segundo plano depende de varios factores, incluido el número de otras operaciones de replicación que estén pendientes.

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

${post_edited_translations.segment}	**Estado de la replicación**
Fuente	• **FINALIZADO**: La replicación se realizó correctamente en todas las conexiones de grid. • **PENDIENTE**: El objeto no se ha replicado en al menos una conexión de grid. • **ERROR**: No hay ninguna replicación pendiente para ninguna conexión de grid y al menos una ha fallado con un error permanente. Un usuario debe resolver el error.
Destino	**RÉPLICA**: El objeto fue replicado desde la cuadrícula de origen.

   > StorageGRID no admite la cabecera `x-amz-replication-status`.

2. StorageGRID utiliza las políticas de ILM activas de cada grid para gestionar los objetos, tal como lo haría con cualquier otro objeto. Por ejemplo, el objeto A en el grid 1 se podría almacenar como dos copias replicadas y conservar para siempre, mientras que la copia del objeto A que se replicó en el grid 2 se podría almacenar mediante codificación de borrado 2+1 y eliminar después de tres años.

¿Qué ocurre cuando se eliminan objetos?

Tal y como se describe en "${post_edited_translations.segment}", StorageGRID puede eliminar un objeto por cualquiera de estas razones:

- El cliente S3 envía una solicitud de eliminación.
- Un usuario de Tenant Manager selecciona la opción "Eliminar objetos en el depósito" para eliminar todos los objetos de un bucket.
- El bucket tiene una configuración de ciclo de vida que caduca.
- Finaliza el último periodo de tiempo en la regla ILM para el objeto y no hay más ubicaciones especificadas.

Cuando StorageGRID elimina un objeto debido a una operación de Delete objects in bucket, a la expiración del ciclo de vida del bucket o a la expiración de la ubicación de ILM, el objeto replicado nunca se elimina de la otra grid en una conexión de grid federation. Sin embargo, los marcadores de eliminación añadidos al bucket de origen mediante eliminaciones del cliente S3 pueden replicarse opcionalmente al bucket de destino.

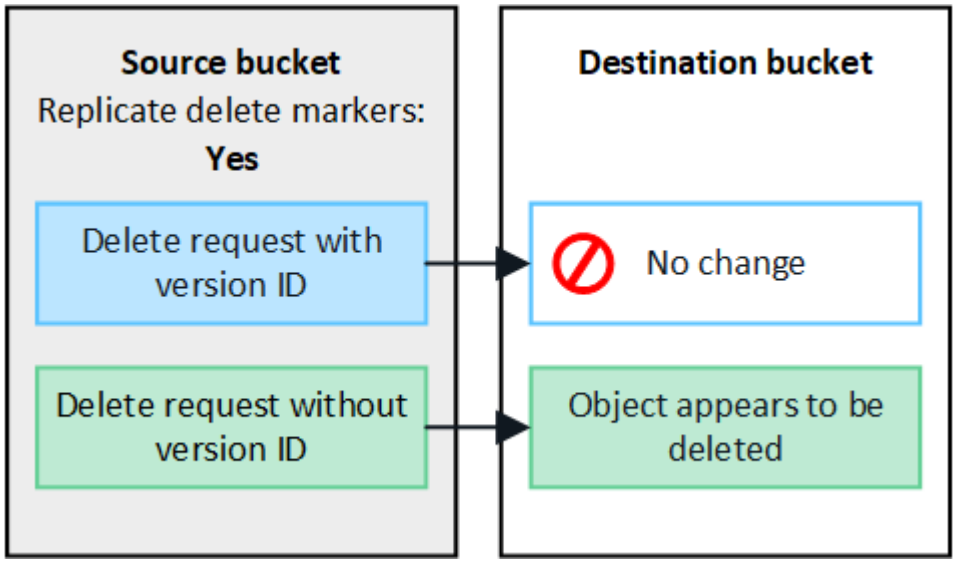
Para comprender qué ocurre cuando un cliente de S3 elimina objetos de un bucket que tiene habilitada la replicación entre grids, revisa cómo los clientes de S3 eliminan objetos de buckets que tienen habilitado el versionado, como sigue:

- Si un cliente de S3 envía una solicitud de eliminación que incluye un identificador de versión, esa versión del objeto se elimina de forma permanente. No se añade ningún marcador de eliminación al depósito.
- Si un cliente S3 emite una solicitud de eliminación que no incluye un ID de versión, StorageGRID no elimina ninguna versión del objeto. En su lugar, añade un marcador de eliminación al bucket. El marcador de eliminación hace que StorageGRID actúe como si el objeto se hubiera eliminado:
  - Una solicitud GetObject sin un ID de versión falla con `404 No Object Found`
  - Una solicitud GetObject con un ID de versión válido se realiza correctamente y devuelve la versión del objeto solicitada.

Cuando un cliente de S3 elimina un objeto de un depósito que tiene habilitada la replicación entre redes, StorageGRID determina si debe replicar la solicitud de eliminación al destino, como sigue:

- Si la solicitud de eliminación incluye un ID de versión, esa versión del objeto se elimina de forma permanente del grid de origen. Sin embargo, StorageGRID no replica las solicitudes de eliminación que incluyen un ID de versión, por lo que esa misma versión del objeto no se elimina del destino.
- Si la solicitud de eliminación no incluye un identificador de versión, StorageGRID puede, de forma opcional, replicar el marcador de eliminación, en función de cómo esté configurada la replicación entre grids para el bucket:
  - Si eliges replicar los marcadores de eliminación (predeterminado), se añade un marcador de eliminación al bucket de origen y se replica en el bucket de destino. En efecto, el objeto parece estar eliminado en ambos grids.
  - Si eliges no replicar los marcadores de eliminación, se añade un marcador de eliminación al bucket de origen, pero no se replica en el bucket de destino. En efecto, los objetos que se eliminan en el grid de origen no se eliminan en el grid de destino.

En la figura, **Replicate delete markers** se estableció en **Yes** cuando "Se habilitó la replicación entre grids". Las solicitudes de eliminación para el bucket de origen que incluyen un ID de versión no eliminan objetos del bucket de destino. Las solicitudes de eliminación para el bucket de origen que no incluyen un ID de versión parecen eliminar objetos en el bucket de destino.



Si quieres mantener sincronizadas las eliminaciones de objetos entre grids, crea "Configuraciones del ciclo de vida de S3" correspondientes para los buckets en ambos grids.

Cómo se replican los objetos cifrados

Cuando usas la replicación entre grids para replicar objetos entre grids, puedes cifrar objetos individuales, usar el cifrado de bucket predeterminado o configurar el cifrado a nivel de grid. Puedes añadir, modificar o eliminar la configuración de cifrado predeterminado de bucket o a nivel de grid antes o después de habilitar la replicación entre grids para un bucket.

Para cifrar objetos individuales, puedes usar SSE (cifrado del lado del servidor con claves gestionadas por StorageGRID) al añadir los objetos al bucket de origen. Usa la cabecera de solicitud `x-amz-server-side-encryption` y especifica `AES256`. Consulta "Utiliza el cifrado del lado 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 grids. La operación de ingesta fallará.

Para usar el cifrado predeterminado para un bucket, usa una solicitud PutBucketEncryption y establece el parámetro `SSEAlgorithm` en `AES256`. El cifrado a nivel de bucket se aplica a cualquier objeto que se ingrese sin el encabezado de solicitud `x-amz-server-side-encryption`. Consulta "Operaciones en cubos".

Para utilizar el cifrado a nivel de grid, configura la opción **Cifrado de objetos almacenados** en **AES-256**. El cifrado a nivel de grid se aplica a cualquier objeto que no esté cifrado a nivel de bucket o que se ingrese sin el encabezado de solicitud `x-amz-server-side-encryption`. Consulta "Configura las opciones de red y de objetos".

> SSE no admite AES-128. Si la opción **Stored object encryption** está habilitada para el grid de origen mediante la opción **AES-128**, el uso del algoritmo AES-128 no se propaga al objeto replicado. En su lugar, el objeto replicado utiliza la configuración de cifrado predeterminada a nivel de grid o de bucket del destino, si está disponible.

A la hora de determinar cómo cifrar los objetos de origen, StorageGRID aplica estas reglas:

1. Utiliza el encabezado de ingesta `x-amz-server-side-encryption`, si está presente.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. Si no existe una configuración para toda la grid, no cifres el objeto de origen.

A la hora de determinar cómo cifrar los objetos replicados, StorageGRID aplica estas reglas en este orden:

1. Utiliza el mismo cifrado que el objeto de origen, a menos que ese objeto use cifrado AES-128.
2. Si el objeto de origen no está cifrado o utiliza AES-128, usa la configuración de cifrado predeterminada del bucket de destino, si está configurada.
3. Si el bucket de destino no tiene una configuración de cifrado, usa la configuración de cifrado para toda la grid del destino, si está configurada.
4. Si no existe una configuración válida para toda la grid, no cifres el objeto de destino.

Replicación entre grids con S3 Object Lock

Puedes configurar la replicación entre redes de StorageGRID entre buckets de StorageGRID con S3 Object Lock habilitado en las siguientes circunstancias.

Cuando S3 Object Lock en el bucket de origen está…	Y el S3 Object Lock en el bucket de destino es…
Habilitado	Habilitado
Deshabilitado	Habilitado

Cuando S3 Object Lock está activado en el bucket de origen:

- ${post_edited_translations.segment}

  a. Los valores del encabezado de retención del objeto de origen para:

     `x-amz-object-lock-mode`

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

  b. El tiempo de retención predeterminado del bucket de origen, si se ha configurado.

  c. ${post_edited_translations.segment}

  ${post_edited_translations.segment}

- Puedes establecer el estado de retención legal del objeto de destino utilizando `x-amz-object-lock-legal-hold` al cargar el objeto.
- Se produce un error si el inquilino o el bucket de destino no admiten la configuración de S3 Object Lock del objeto de origen. Consulta "Alertas y errores de replicación entre grids."

Cuando la función S3 Object Lock del bucket de origen está desactivada:

- Puedes configurar la retención predeterminada en el bucket de destino para aplicar la configuración de retención de S3 Object Lock al objeto de destino.
- ${post_edited_translations.segment}

PutObjectTagging y DeleteObjectTagging no son compatibles

Las solicitudes PutObjectTagging y DeleteObjectTagging no son compatibles para los objetos en los buckets que tienen habilitada la replicación entre grids.

Si un cliente S3 envía 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 de buckets que tienen habilitada la replicación entre grids.

Si un cliente S3 realiza una solicitud PutObjectRetention o PutObjectLegalHold, la configuración del objeto de origen se modifica, pero los cambios no se aplican al destino.

${post_edited_translations.segment}

El tamaño máximo de segmento de la grid de origen se aplica a los objetos replicados en la grid de destino. Cuando los objetos se replican en otra grid, el parámetro **Maximum Segment Size** (**Configuration** > **System** > **Storage options**) de la grid de origen se utiliza en ambas grids. Por ejemplo, supón que el tamaño máximo de segmento de la grid de origen es de 1 GB, mientras que el tamaño máximo de segmento de la grid de destino es de 50 MB. Si ingestas un objeto de 2 GB en la grid de origen, ese objeto se guarda como dos segmentos de 1 GB. También se replica en la grid de destino como dos segmentos de 1 GB, aunque el tamaño máximo de segmento de esa grid sea de 50 MB.

Compara la replicación entre grids y la replicación CloudMirror en StorageGRID

A medida que empieces a usar la federación de grid, revisa las similitudes y diferencias entre "replicación entre grids" y "Servicio de replicación CloudMirror de StorageGRID".

No puedes usar CloudMirror en un bucket replicado por replicación entre grids, y viceversa.

	Replicación entre grids	**Servicio de replicación de CloudMirror**
${post_edited_translations.segment}	Un sistema StorageGRID actúa como sistema de recuperación ante desastres. Los objetos de un bucket pueden replicarse entre las grids en una o en ambas direcciones.	${post_edited_translations.segment} La replicación CloudMirror crea una copia independiente de un objeto en una infraestructura S3 independiente. Esta copia independiente no se utiliza como copia de backup, sino que a menudo se procesa posteriormente en la nube.
¿Cómo se configura?	1. Configura una conexión de federación de grid entre dos grids. 2. Agrega nuevas cuentas de inquilinos, que se clonan automáticamente en la otra grid. 3. Agrega nuevos grupos de inquilinos y usuarios, que también se clonan. 4. Crea los buckets correspondientes en cada grid y activa la replicación entre grids en una o ambas direcciones.	1. Un usuario inquilino configura la replicación de CloudMirror definiendo un endpoint de CloudMirror (dirección IP, credenciales, etc.) usando el Tenant Manager o la API de S3. 2. Cualquier bucket que pertenezca a esa cuenta de inquilino se puede configurar para que apunte al punto de conexión de CloudMirror.
¿Quién se encarga de configurarlo?	• Un administrador de grid configura la conexión y los tenants. • ${post_edited_translations.segment}	Normalmente, un usuario arrendatario.
${post_edited_translations.segment}	Un bucket S3 correspondiente e idéntico en el otro sistema StorageGRID en la conexión de la federación de la grid.	• Cualquier infraestructura S3 compatible (incluido Amazon S3). • ${post_edited_translations.segment}

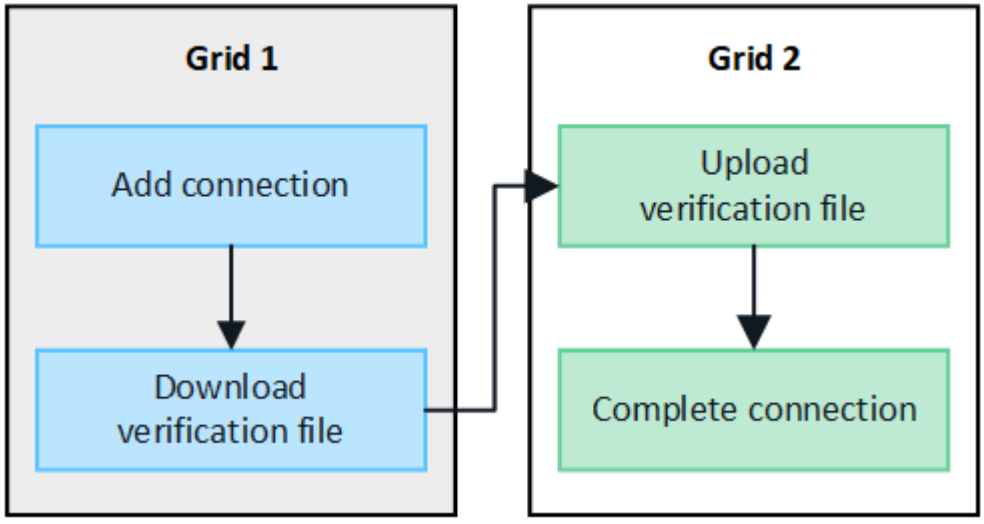
	Replicación entre grids	Servicio de replicación de CloudMirror
¿Es necesario el control de versiones de los objetos?	${post_edited_translations.segment}	No, la replicación de CloudMirror admite cualquier combinación de depósitos sin versionar y versionados, tanto en el origen como en el destino.
¿Qué hace que los objetos se trasladen al destino?	Los objetos se replican automáticamente cuando se añaden a un bucket que tiene habilitada la replicación entre grids.	Los objetos se replican automáticamente cuando se añaden a un bucket que se ha configurado con un endpoint CloudMirror. Los objetos que existían en el bucket de origen antes de que el bucket se configurara con el endpoint CloudMirror no se replican, a menos que se modifiquen.
¿Cómo se replican los objetos?	La replicación entre grids crea objetos versionados y replica el ID de versión del bucket de origen al bucket de destino. Esto permite mantener el orden de las versiones en ambas grids.	CloudMirror replication no requiere buckets con control de versiones habilitado, así que CloudMirror solo puede mantener el orden de una clave dentro de un sitio. No hay garantías de que se mantenga el orden en las solicitudes a un objeto en un sitio diferente.
¿Y si un objeto no se puede replicar?	${post_edited_translations.segment}	El objeto se ha puesto en cola para su replicación, dentro de los límites de los servicios de la plataforma (véase "Recomendaciones para usar los servicios de la plataforma").
${post_edited_translations.segment}	Sí, cuando un objeto se replica en el otro grid, sus metadatos del sistema también se replican. Los metadatos serán idénticos en ambos grids.	No, cuando un objeto se replica en el depósito externo, se actualizan sus metadatos del sistema. Los metadatos variarán entre las distintas ubicaciones, dependiendo del momento de la ingesta y del comportamiento de la infraestructura independiente de S3.
¿Cómo se recuperan los objetos?	${post_edited_translations.segment}	Las aplicaciones pueden recuperar o leer objetos enviando una solicitud a StorageGRID o al destino S3. Por ejemplo, supón que usas la replicación de CloudMirror para duplicar objetos en una organización asociada. La organización asociada puede usar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario usar StorageGRID.

	Replicación entre grids	Servicio de replicación de CloudMirror
¿Qué ocurre si se elimina un objeto?	• Las solicitudes de eliminación que incluyen un identificador de versión nunca se replican en el grid de destino. • Las solicitudes de eliminación que no incluyan un identificador de versión añaden un marcador de eliminación al bucket de origen, que opcionalmente puede replicarse en el grid de destino. • ${post_edited_translations.segment}	Los resultados variarán en función del estado de las versiones de los buckets de origen y destino (que no tienen por qué ser iguales): • Si ambos buckets tienen control de versiones, una solicitud de eliminación añadirá un marcador de eliminación en ambas ubicaciones. • Si solo el bucket de origen tiene control de versiones, una solicitud de eliminación añadirá un marcador de eliminación al origen pero no al destino. • Si ninguno de los dos buckets tiene control de versiones, una solicitud de eliminación borrará el objeto del origen pero no del destino. Del mismo modo, los objetos en el bucket de destino se pueden eliminar sin afectar al de origen.

Crear conexiones de federación de grid StorageGRID

Puedes crear una conexión de federación de grid entre dos sistemas StorageGRID si quieres clonar los detalles de los inquilinos y replicar los datos de los objetos.

Como se muestra en la figura, crear una conexión de federación de grid incluye pasos en ambos grids. Añades la conexión en un grid y la completas en el otro grid. Puedes empezar desde cualquiera de los grids.



Antes de empezar

- Has revisado "${post_edited_translations.segment}" para configurar conexiones de federación de grid.
- ${post_edited_translations.segment}

- Estás usando un "navegador web compatible".
- ${post_edited_translations.segment}

${post_edited_translations.segment}

Sigue estos pasos en cualquiera de los dos sistemas StorageGRID.

Pasos

1. ${post_edited_translations.segment}
2. Selecciona **Configuración** > **Sistema** > **Grid federation**.
3. Selecciona **Add connection**.
4. ${post_edited_translations.segment}

Campo	Descripción
${post_edited_translations.segment}	${post_edited_translations.segment}
FQDN o dirección IP de esta grid	Una de las siguientes opciones: • El nombre de dominio completo (FQDN) de la grid en la que has iniciado sesión actualmente • Una dirección VIP de un grupo HA en esta grid • Una dirección IP de un nodo de administración o de un nodo de puerta de enlace en este grid. La dirección IP puede estar en cualquier red a la que pueda acceder el grid de destino.
Puerto	El puerto que deseas utilizar para esta conexión. Puedes introducir cualquier número de puerto no utilizado comprendido entre 23000 y 23999. Ambas redes de esta conexión utilizarán el mismo puerto. Debes asegurarte de que ningún nodo de ninguna de las dos redes utilice este puerto para otras conexiones.
Días de validez del certificado para este grid	El número de días que quieres que los certificados de seguridad para este grid en la conexión sean válidos. El valor predeterminado es 730 días (2 años), pero puedes ingresar cualquier valor entre 1 y 762 días. StorageGRID genera automáticamente certificados de cliente y de servidor para cada grid cuando guardas la conexión.
Frase de contraseña de aprovisionamiento para este grid	La frase de acceso de aprovisionamiento de la grid en la que has iniciado sesión.

Campo	Descripción
${post_edited_translations.segment}	Una de las siguientes opciones: • El dominio completo (FQDN) de la grid a la que quieres conectarte • ${post_edited_translations.segment} • Una dirección IP de un nodo de administración o un nodo de puerta de enlace en la otra grid. La dirección IP puede estar en cualquier red a la que la grid de origen pueda acceder.

5. Selecciona **Guardar y continuar**.
6. En el paso «Descargar el archivo de verificación», selecciona **Descargar el archivo de verificación**.

   Después de que se complete la conexión en la otra grid, ya no podrás descargar el archivo de verificación de ninguna de las dos grids.

7. Busca el archivo descargado (*`connection-name`*`.grid-federation` y guárdalo en una ubicación segura.

   Este archivo contiene secretos (enmascarados como *****) y otros detalles confidenciales, y debes almacenarlo y transmitirlo de forma segura.

8. Selecciona **Cerrar** para volver a la página de Grid federation.
9. Comprueba que aparezca la nueva conexión y que su **Estado de la conexión** sea **Esperando a conectarse**.
10. Facilita el archivo *`connection-name`*`.grid-federation` al administrador de grid de la otra grid.

${post_edited_translations.segment}

Sigue estos pasos en el sistema StorageGRID al que te vas a conectar (la otra grid).

Pasos

1. ${post_edited_translations.segment}
2. Selecciona **Configuración** > **Sistema** > **Grid federation**.
3. Selecciona **Subir archivo de verificación** para acceder a la página de subida.
4. Selecciona **Subir archivo de verificación**. Luego, busca y selecciona el archivo que descargaste de la primera grid (*`connection-name`*`.grid-federation`).

   Se muestran los detalles de la conexión.

5. Opcionalmente, introduce un número diferente de días de validez para los certificados de seguridad de este grid. La entrada **Días de validez del certificado** toma de forma predeterminada el valor que introdujiste en el primer grid, pero cada grid puede usar diferentes fechas de caducidad.

   En general, utiliza el mismo número de días para los certificados de ambos extremos de la conexión.

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

6. ${post_edited_translations.segment}
7. ${post_edited_translations.segment}

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

   Si aparece un mensaje de error, soluciona cualquier problema. Consulta "${post_edited_translations.segment}".

8. Ve a la página Grid federation en el primer grid y actualiza el navegador. Confirma que el **Estado de la conexión** ahora es **Conectado**.
9. ${post_edited_translations.segment}

   Si editas esta conexión, se creará un nuevo archivo de verificación. El archivo original no se podrá volver a utilizar.

Después de que termines

- Consulta las consideraciones para "${post_edited_translations.segment}".
- "Crear una o varias cuentas de inquilino nuevas", asigna el permiso **Usar conexión de federación de grid** y selecciona la nueva conexión.
- "Gestiona la conexión" según sea necesario. Puedes editar los valores de conexión, comprobar una conexión, rotar los certificados de conexión o eliminar una conexión.
- "Supervisa la conexión" como parte de tus actividades habituales de supervisión de StorageGRID.
- "Soluciona los problemas de conexión", incluida la resolución de cualquier alerta o error relacionado con la clonación de cuentas y la replicación entre grids.

Administra las conexiones de la federación de grid de StorageGRID

${post_edited_translations.segment}

Antes de empezar

- Has iniciado sesión en el Grid Manager de cualquiera de las dos grids usando un "navegador web compatible".
- Tienes el "Permiso de acceso raíz" de la grid en la que has iniciado sesión.

Editar una conexión de federación de grid

Puedes editar una conexión de federación de grid iniciando sesión en el nodo Admin principal de cualquiera de los grids en la conexión. Después de hacer cambios en el primer grid, debes descargar un nuevo archivo de verificación y subirlo al otro grid.

Mientras editas la conexión, las solicitudes de clonación de cuentas o de replicación entre grids seguirán usando la configuración de conexión existente. Cualquier cambio que hagas en el primer grid se guarda localmente, pero no se utilizará hasta que se haya subido al segundo grid, guardado y probado.

Empieza a editar la conexión

Pasos

1. ${post_edited_translations.segment}
2. Selecciona **Nodos** y comprueba que todos los demás Admin Nodes de tu sistema estén online.

   Al editar una conexión de federación de grid, StorageGRID intenta guardar un archivo de "configuración candidata" en todos los nodos de administración del primer grid. Si no se puede guardar este archivo en todos los nodos de administración, aparece un mensaje de advertencia cuando seleccionas **Guardar y probar**.

3. Selecciona **Configuración** > **Sistema** > **Grid federation**.
4. Edita los datos de conexión mediante el menú **Acciones** de la página Grid federation o de la página de detalles de una conexión concreta. Consulta "Crear conexiones de federación de grid" para saber qué datos debes introducir.

   Menú de acciones

   a. ${post_edited_translations.segment}
   b. Selecciona **Acciones** > **Editar**.
   c. Introduce la nueva información.

   ${post_edited_translations.segment}

   a. Selecciona un nombre de conexión para ver sus detalles.
   b. Selecciona **Editar**.
   c. Introduce la nueva información.

5. Introduce la contraseña de aprovisionamiento de la grid en la que has iniciado sesión.
6. Selecciona **Guardar y continuar**.

   ${post_edited_translations.segment}

7. Selecciona **Descargar archivo de verificación**.

   Para descargar este archivo más adelante, ve a la página de detalles de la conexión.

8. Busca el archivo descargado (*`connection-name`*`.grid-federation` y guárdalo 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. Comprueba que el **Estado de la conexión** sea **Pendiente de edición**.

    ${post_edited_translations.segment}

11. Facilita el archivo *connection-name*`.grid-federation` al administrador de grid de la otra grid.

Termina de editar la conexión

Finaliza la edición de la conexión subiendo el archivo de verificación en la otra grid.

Pasos

1. ${post_edited_translations.segment}
2. Selecciona **Configuración** > **Sistema** > **Grid federation**.
3. Selecciona **Subir archivo de verificación** para acceder a la página de carga.
4. Selecciona **Cargar archivo de verificación**. Luego, busca y selecciona el archivo que descargaste desde el primer grid.
5. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}

   Si se puede establecer la conexión utilizando los valores modificados, aparecerá un mensaje de éxito. En caso contrario, aparecerá un mensaje de error. Revisa el mensaje y soluciona cualquier problema.

7. Cierra el asistente para volver a la página de federación de Grid.
8. Comprueba que el **Estado de la conexión** sea **Conectado**.
9. Ve a la página Grid federation en el primer grid y actualiza el navegador. Confirma que el **Estado de la conexión** ahora es **Conectado**.
10. ${post_edited_translations.segment}

Probar una conexión de federación de grid

Pasos

1. ${post_edited_translations.segment}
2. Selecciona **Configuración** > **Sistema** > **Grid federation**.
3. Prueba la conexión usando el menú **Acciones** en la página de Grid federation o en la página de detalles de una conexión específica.

   Menú de acciones

   a. ${post_edited_translations.segment}
   b. Selecciona **Acciones** > **Probar**.

   ${post_edited_translations.segment}

   a. Selecciona un nombre de conexión para ver sus detalles.
   b. Selecciona **Probar conexión**.

4. ${post_edited_translations.segment}

Estado de la conexión	Descripción
Conectado	Ambas redes 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.
${post_edited_translations.segment}	Has editado la conexión en esta grid, pero la conexión sigue utilizando la configuración existente. Para completar la edición, sube el nuevo archivo de verificación a la otra grid.
Esperando para conectarte	Has configurado la conexión en esta grid, pero la conexión no se ha completado en la otra grid. Descarga el archivo de verificación de esta grid y súbelo a la otra grid.
Desconocido	La conexión se encuentra en un estado desconocido, posiblemente debido a un problema de red o a que un nodo está desconectado.

5. Si el estado de la conexión es **Error**, soluciona cualquier problema. Luego, selecciona **Probar conexión** otra vez para confirmar que el problema se ha solucionado.

Rotar certificados de conexión

Cada conexión de federación de redes utiliza cuatro certificados SSL generados automáticamente para proteger la conexión. Cuando los dos certificados de cada red se acercan a su fecha de caducidad, la alerta **Caducidad del certificado de federación de redes** te recuerda que debes renovarlos.

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

Pasos

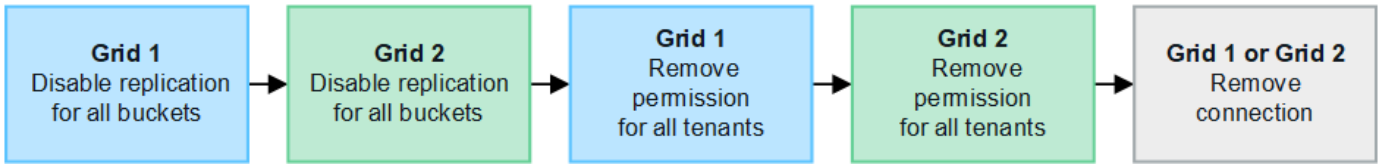
1. ${post_edited_translations.segment}
2. Selecciona **Configuración** > **Sistema** > **Grid federation**.
3. Desde cualquiera de las pestañas en la página de Grid federation, selecciona el nombre de la conexión para ver sus detalles.
4. Selecciona la pestaña **Certificados**.
5. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}
7. Introduce la contraseña de aprovisionamiento de la grid en la que has iniciado sesión.
8. ${post_edited_translations.segment}
9. ${post_edited_translations.segment}

   En general, utiliza el mismo número de días para los certificados de ambos extremos de la conexión.

Eliminar una conexión de federación de grid

Puedes eliminar una conexión de federación de grids desde cualquiera de los grids en la conexión. Como se

muestra en la figura, debes realizar los pasos previos en ambos grids para confirmar que la conexión no está siendo utilizada por ningún tenant en ninguno de los grids.



Antes de quitar una conexión, ten en cuenta lo siguiente:

- Al eliminar una conexión no se borran los elementos que ya se hayan copiado entre grids. Por ejemplo, los usuarios, grupos y objetos del tenant que existan en ambos grids no se borran de ninguno de los grids cuando se elimina el permiso del tenant. Si quieres borrar estos elementos, debes eliminarlos manualmente de ambos grids.
- ${post_edited_translations.segment}

Desactivar la replicación para todos los buckets de los inquilinos

Pasos

1. Desde cualquiera de las dos grids, inicia sesión en el Grid Manager desde el nodo de administración principal.
2. Selecciona **Configuración** > **Sistema** > **Grid federation**.
3. Selecciona el nombre de la conexión para ver sus detalles.
4. En la pestaña **Inquilinos autorizados**, determina si la conexión está siendo utilizada por algún inquilino.
5. Si aparece algún inquilino en la lista, indica a todos los inquilinos que "desactivar la replicación entre grids" para todos sus buckets en ambos grids de la conexión.

> No puedes eliminar el permiso **Usar conexión de federación entre grids** si algún bucket de un tenant tiene habilitada la replicación entre grids. Cada cuenta de tenant debe desactivar la replicación entre grids para sus buckets en ambos grids.

${post_edited_translations.segment}

${post_edited_translations.segment}

Pasos

1. Selecciona **Configuración** > **Sistema** > **Grid federation**.
2. Selecciona el nombre de la conexión para ver sus detalles.
3. Para cada inquilino en la pestaña **Inquilinos permitidos**, quita el permiso **Usar conexión de federación de grid** de cada inquilino. Consulta "${post_edited_translations.segment}".
4. Repite estos pasos para los inquilinos permitidos en la otra grid.

${post_edited_translations.segment}

Pasos

1. Cuando ningún inquilino de ninguna de las dos grids esté utilizando la conexión, selecciona **Eliminar**.
2. ${post_edited_translations.segment}
   - Si es posible eliminar la conexión, aparecerá un mensaje de éxito. La conexión de federación entre

grids ya se ha eliminado de ambos grids.

- Si no se puede eliminar la conexión (por ejemplo, porque todavía está en uso o hay un error de conexión), aparecerá un mensaje de error. Puedes hacer lo siguiente:
  - Soluciona el error (recomendado). Consulta "${post_edited_translations.segment}".
  - Elimina la conexión a la fuerza. Consulta la siguiente sección.

Eliminar una conexión de federación de grid de forma forzada

Si es necesario, puedes forzar la eliminación de una conexión que no tenga el estado **Connected**.

La eliminación forzada solo elimina la conexión del grid local. Para eliminar por completo la conexión, realiza los mismos pasos en ambos grids.

Pasos

1. ${post_edited_translations.segment}

   Aparece un mensaje de éxito. Esta conexión de federación de grid ya no se puede utilizar. Sin embargo, es posible que los buckets de inquilino aún tengan habilitada la replicación entre grids y que algunas copias de objetos ya se hayan replicado entre los grids de la conexión.

2. Desde la otra grid en la conexión, inicia sesión en el Grid Manager desde el nodo de administración principal.
3. Selecciona **Configuración** > **Sistema** > **Grid federation**.
4. Selecciona el nombre de la conexión para ver sus detalles.
5. Selecciona **Eliminar** y **Sí**.
6. Selecciona **Eliminar forzosamente** para eliminar la conexión de este grid.

Administra los inquilinos permitidos para la federación de grid de StorageGRID

Puedes permitir que las cuentas de inquilino de S3 utilicen una conexión de federación de grid entre dos sistemas StorageGRID. Cuando se permite a los inquilinos usar una conexión, se requieren pasos especiales para editar los detalles del inquilino o para eliminar de forma permanente el permiso del inquilino para usar la conexión.

Antes de empezar

- Has iniciado sesión en el Grid Manager de cualquiera de las dos grids usando un "navegador web compatible".
- Tienes el "Permiso de acceso raíz" de la grid en la que has iniciado sesión.
- Tienes "creaste una conexión de federación de grid" entre dos grids.
- Has revisado los flujos de trabajo de "clon de cuenta" y "replicación entre grids".
- Como se requiere, ya has configurado el inicio de sesión único (SSO) o la federación de identidades para ambas grids en la conexión. Consulta "¿Qué es un clon de cuenta?".

${post_edited_translations.segment}

Si quieres permitir que una cuenta de inquilino nueva o existente use una conexión de federación de grid para la clonación de cuentas y la replicación entre grids, sigue las instrucciones generales para "crear un nuevo cliente de S3" o "editar una cuenta de inquilino" y ten en cuenta lo siguiente:

- Puedes crear el inquilino desde cualquiera de las dos cuadrículas de la conexión. La cuadrícula en la que se crea un inquilino es la *cuadrícula de origen del inquilino*.
- El estado de la conexión debe ser **Conectado**.
- Cuando creas o editas el inquilino para habilitar el permiso **Usar conexión de federación de grid** y luego lo guardas en el primer grid, se replica automáticamente un inquilino idéntico en el otro grid. El grid donde se replica el inquilino es el *grid de destino del inquilino*.
- Los inquilinos de ambos grids tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos. Opcionalmente, puedes usar el campo **Descripción** para ayudarte a identificar cuál es el inquilino de origen y cuál es el de destino. Por ejemplo, esta descripción de un inquilino creado en el Grid 1 también aparecerá para el inquilino replicado en el Grid 2: "Este inquilino se creó en el Grid 1."
- Por motivos de seguridad, la contraseña del usuario raíz no se copia en la grid de destino.

  Antes de que un usuario raíz local pueda iniciar sesión en el inquilino replicado en la grid de destino, un administrador de esa grid debe "cambiar la contraseña del usuario raíz local".

- Después de que el inquilino nuevo o editado esté disponible en ambas grids, los usuarios del inquilino pueden realizar estas operaciones:
  - Desde la grid de origen del tenant, crea grupos y usuarios locales, que se clonan automáticamente en la grid de destino del tenant. Consulta "Clonar grupos de inquilinos y usuarios".
  - Crea nuevas claves de acceso de S3, que opcionalmente pueden clonarse en la grid de destino del tenant. Consulta "Clonar claves de acceso a S3 mediante la API".
  - Crea buckets idénticos en ambos grids de la conexión y habilita la replicación entre grids en una dirección o en ambas. Consulta "${post_edited_translations.segment}".

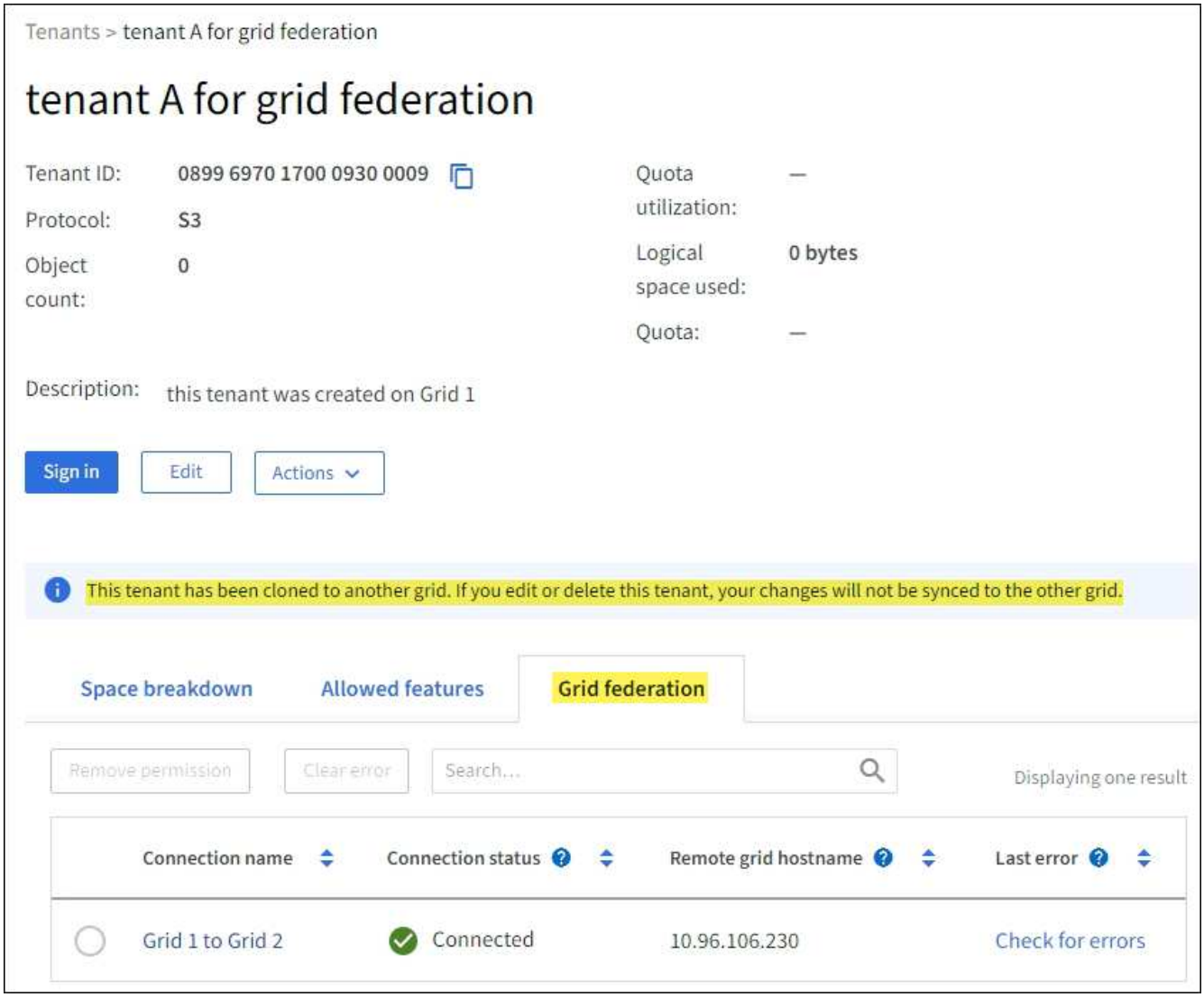
Ver un inquilino autorizado

Puedes consultar los detalles de un inquilino al que se le permite utilizar una conexión de federación de grid.

Pasos

1. Selecciona **Tenants**.
2. En la página Tenants, selecciona el nombre del tenant para ver la página de detalles del tenant.

   Si esta es la grid de origen del tenant (es decir, si el tenant se creó en esta grid), aparecerá un mensaje para recordarte que el tenant se clonó en otra grid. Si editas o eliminas este tenant, los cambios no se sincronizarán con la otra grid.



3. De forma opcional, selecciona la pestaña **Grid federation** para "${post_edited_translations.segment}".

${post_edited_translations.segment}

Si necesitas editar un inquilino que tenga el permiso **Usar conexión de federación de red**, sigue las instrucciones generales de "Editar una cuenta de inquilino" y ten en cuenta lo siguiente:

- Si un inquilino tiene el permiso **Usar conexión de federación de grid**, puedes editar los detalles del inquilino desde cualquiera de los grids de la conexión. Sin embargo, los cambios que realices no se copiarán en el otro grid. Si quieres mantener sincronizados los detalles del inquilino entre los grids, debes realizar las mismas ediciones en ambos grids.
- No puedes quitar el permiso **Utilizar conexión de federación de grid** cuando estás editando un inquilino.
- No puedes seleccionar una conexión de federación de grid diferente cuando estás editando un inquilino.

${post_edited_translations.segment}

Si necesitas eliminar un inquilino que tiene el permiso **Use grid federation connection**, sigue las instrucciones generales para "Eliminar una cuenta de inquilino" y ten en cuenta lo siguiente:

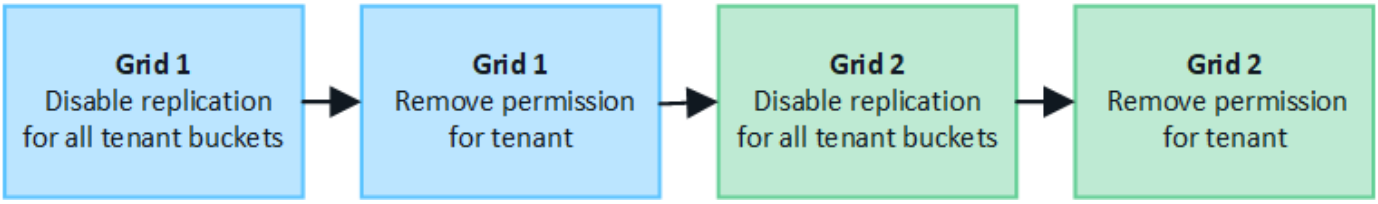
- ${post_edited_translations.segment}

- Antes de poder eliminar el inquilino clonado en la grid de destino, debes eliminar todos los buckets de la cuenta en la grid de destino.
- ${post_edited_translations.segment}
- Si eliminas el tenant original de la grid de origen, cualquier grupo de tenant, usuario o clave que se haya clonado en la grid de destino no se verá afectado. Puedes eliminar el tenant clonado o permitir que gestione sus propios grupos, usuarios, claves de acceso y buckets.
- Si vas a eliminar el inquilino clonado en la grid de destino, se producirán errores de clonación si se añaden nuevos grupos o usuarios al inquilino original.

  ${post_edited_translations.segment}

Eliminar el permiso Usar conexión de federación de grid

${post_edited_translations.segment}



Antes de retirar a un inquilino el permiso para utilizar una conexión de federación de red, ten en cuenta lo siguiente:

- No puedes eliminar el permiso **Usar conexión de federación de redes** si alguno de los buckets del inquilino tiene habilitada la replicación entre grids. La cuenta del inquilino debe desactivar la replicación entre grids en todos sus buckets primero.
- Al eliminar el permiso **Usar conexión de federación entre grids**, no se elimina ningún elemento que ya se haya replicado entre grids. Por ejemplo, cualquier usuario, grupo y objeto del tenant que exista en ambos grids no se elimina de ninguno de los grids cuando se retira el permiso del tenant. Si quieres eliminar estos elementos, debes eliminarlos manualmente de ambos grids.
- Si deseas volver a habilitar este permiso con la misma conexión de federación de grid, elimina primero este tenant en el grid de destino; de lo contrario, volver a habilitar este permiso resultará en un error.

> Al volver a habilitar el permiso **Usar conexión de federación de grid**, el grid local pasa a ser el grid de origen y se inicia la clonación en el grid remoto especificado por la conexión de federación de grid seleccionada. Si la cuenta de tenant ya existe en el grid remoto, la clonación dará lugar a un error de conflicto.

Antes de empezar

- Estás usando un "navegador web compatible".
- Tienes el "Permiso de acceso raíz" para ambas cuadrículas.

Desactivar la replicación para los buckets de los inquilinos

${post_edited_translations.segment}

Pasos

1. Desde cualquiera de las dos grids, inicia sesión en el Grid Manager desde el nodo de administración principal.

2. Selecciona **Configuración** > **Sistema** > **Grid federation**.
3. Selecciona el nombre de la conexión para ver sus detalles.
4. ${post_edited_translations.segment}
5. Si el inquilino aparece en la lista, indícale que "desactivar la replicación entre grids" para todos sus buckets en ambos grids de la conexión.

> No puedes eliminar el permiso **Usar conexión de federación de grid** si alguno de los buckets del inquilino tiene habilitada la replicación entre grids. El inquilino debe deshabilitar la replicación entre grids para sus buckets en ambos grids.

Quitar permiso para el tenant

Después de desactivar la replicación entre grids para los buckets del inquilino, puedes eliminar el permiso del inquilino para usar la conexión de federación de grids.

Pasos

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

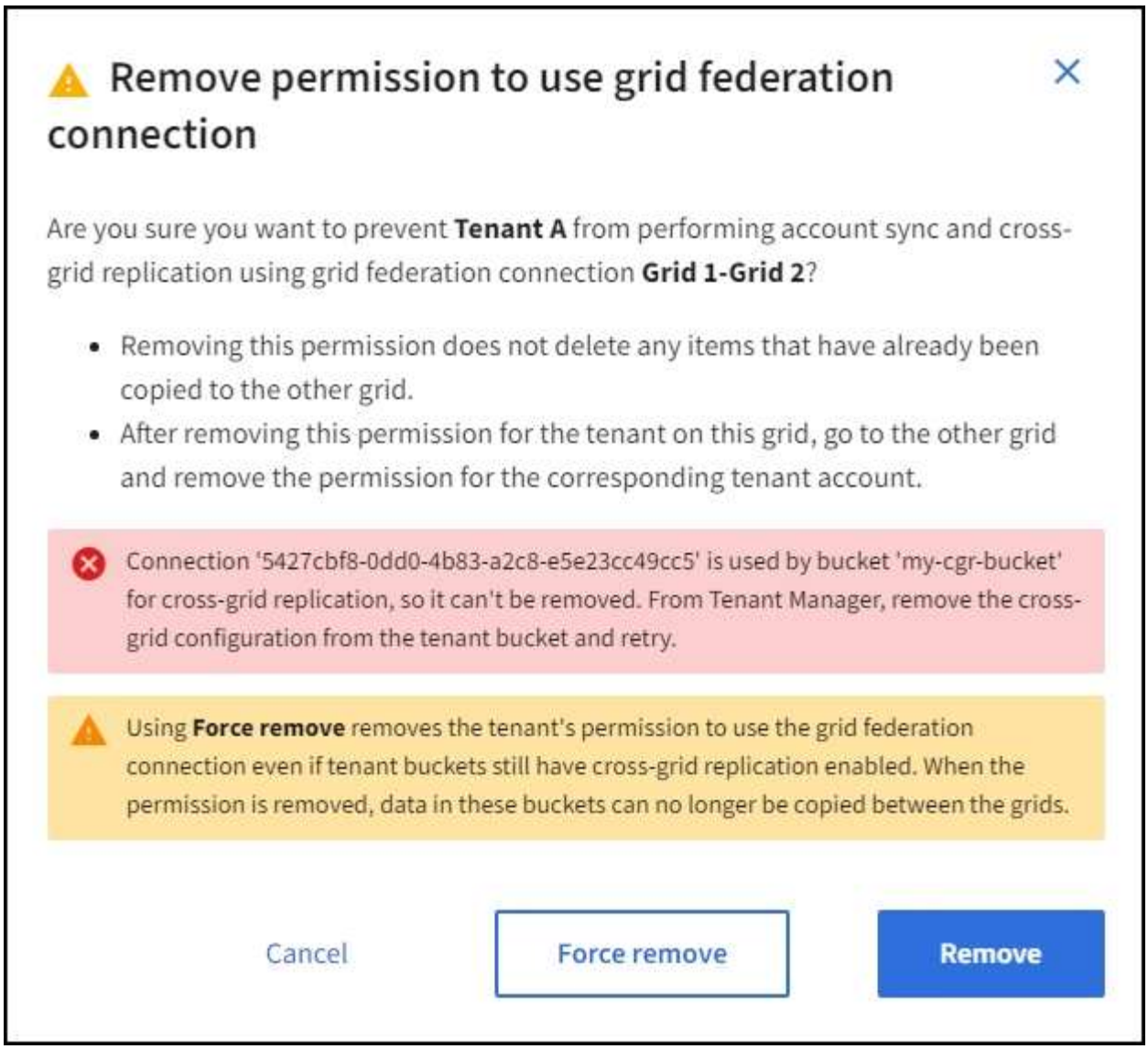
Página de federación de grid

a. Selecciona **Configuración** > **Sistema** > **Grid federation**.
b. Selecciona el nombre de la conexión para ver su página de detalles.
c. ${post_edited_translations.segment}
d. Selecciona **Eliminar permiso**.

Página de inquilinos

a. Selecciona **Tenants**.
b. Selecciona el nombre del inquilino para mostrar la página de detalles.
c. En la pestaña **Grid federation**, selecciona el botón de opción para la conexión.
d. Selecciona **Eliminar permiso**.

3. Revisa las advertencias que aparecen en el cuadro de diálogo de confirmación y selecciona **Eliminar**.
   - Si se puede eliminar el permiso, vuelves a la página de detalles y se muestra un mensaje de éxito. Este tenant ya no puede usar la conexión de grid federation.
   - Si uno o más buckets de un tenant siguen teniendo activada la replicación entre grids, se muestra un error.



${post_edited_translations.segment}

- (Recomendado.) Inicia sesión en Tenant Manager y desactiva la replicación para cada uno de los buckets del tenant. Consulta "${post_edited_translations.segment}". Luego, repite los pasos para quitar el permiso **Use grid connection**.
- Elimina el permiso a la fuerza. Consulta la siguiente sección.

4. Ve a la otra grid y repite estos pasos para eliminar el permiso del mismo tenant en la otra grid.

${post_edited_translations.segment}

${post_edited_translations.segment}

Antes de retirar por la fuerza el permiso de un inquilino, ten en cuenta las consideraciones generales para retirar el permiso así como estas consideraciones adicionales:

- Si eliminas el permiso **Usar conexión de federación de grid** por la fuerza, todos los objetos que estén pendientes de replicación en el otro grid (ingestados pero aún no replicados) se seguirán replicando. Para evitar que estos objetos en proceso lleguen al bucket de destino, también debes eliminar el permiso del tenant en el otro grid.

- ${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}
2. Selecciona **Configuración** > **Sistema** > **Grid federation**.
3. Selecciona el nombre de la conexión para ver su página de detalles.
4. ${post_edited_translations.segment}
5. Selecciona **Eliminar permiso**.
6. Lee las advertencias que aparecen en el cuadro de diálogo de confirmación y selecciona **Force remove**.

   Aparece un mensaje de éxito. Este inquilino ya no puede utilizar la conexión de federación de grid.

7. Si es necesario, ve a la otra grid y repite estos pasos para eliminar de forma forzada el permiso de la misma cuenta de tenant en la otra grid. Por ejemplo, debes repetir estos pasos en la otra grid para evitar que los objetos en proceso lleguen al bucket de destino.

Soluciona errores de federación de grid en StorageGRID

Es posible que tengas que solucionar problemas relacionados con alertas y errores sobre las conexiones de federación de grid, la clonación de cuentas y la replicación entre grids.

Alertas y errores de conexión de la federación de grid

Es posible que recibas alertas o experimentes errores con tus conexiones de federación de grid.

Después de realizar cualquier cambio para resolver un problema de conexión, prueba la conexión para asegurarte de que el estado de la conexión vuelva a ser **Conectado**. Para obtener instrucciones, consulta "Gestiona las conexiones de la federación de grid".

Alerta de fallo en la conexión de la federación de grid

Problema

Se activó la alerta **Error de conexión a la federación Grid**.

Detalles

Esta alerta indica que la conexión de la federación de grid entre los grids no está funcionando.

Medidas recomendadas

1. Revisa la configuración de la página Grid Federation para ambas grids. Confirma que todos los valores sean correctos. Consulta "Gestiona las conexiones de la federación de grid".
2. Revisa los certificados utilizados para la conexión. Asegúrate de que no haya alertas de certificados de federación de grid caducados y de que los detalles de cada certificado sean válidos. Consulta las instrucciones para rotar los certificados de conexión en "Gestiona las conexiones de la federación de grid".
3. Confirma que todos los nodos de administración y de pasarela en ambas grids estén en línea y disponibles. Resuelve cualquier alerta que pueda estar afectando a estos nodos e inténtalo de nuevo.
4. Si proporcionaste un nombre de dominio completo (FQDN) para la grid local o remota, confirma que el servidor DNS esté en línea y disponible. Consulta "${post_edited_translations.segment}" para ver los requisitos de red, dirección IP y DNS.

${post_edited_translations.segment}

Problema

Se activó la alerta **Caducidad del certificado de la federación de grid**.

Detalles

${post_edited_translations.segment}

Medidas recomendadas

Consulta las instrucciones para la rotación de los certificados de conexión en "Gestiona las conexiones de la federación de grid".

${post_edited_translations.segment}

Problema

Al editar una conexión de federación de grid, ves el siguiente mensaje de advertencia cuando seleccionas **Guardar y probar**: «No se pudo crear un archivo de configuración candidato en uno o más nodos».

Detalles

Al editar una conexión de federación de grid, StorageGRID intenta guardar un archivo de "configuración candidata" en todos los nodos de administración del primer grid. Aparece un mensaje de advertencia si este archivo no puede guardarse en todos los nodos de administración, por ejemplo, porque un nodo de administración está fuera de línea.

Medidas recomendadas

1. En la cuadrícula que estás utilizando para editar la conexión, selecciona **Nodos**.
2. Confirma que todos los nodos de administración de esa grid estén en línea.
3. Si hay algún nodo desconectado, vuelve a conectarlo e intenta editar la conexión de nuevo.

Errores al clonar cuentas

${post_edited_translations.segment}

Problema

No puedes iniciar sesión en una cuenta de inquilino clonada. El mensaje de error en la página de inicio de sesión de Tenant Manager es "Tus credenciales para esta cuenta no eran válidas. Por favor, inténtalo de nuevo."

Detalles

Por motivos de seguridad, cuando se clona una cuenta de inquilino desde la grid de origen del inquilino a la grid de destino del mismo, la contraseña que hayas establecido para el usuario raíz local del inquilino no se clona. Del mismo modo, cuando un inquilino crea usuarios locales en su grid de origen, las contraseñas de dichos usuarios locales no se clonan en la grid de destino.

Medidas recomendadas

Antes de que el usuario raíz pueda iniciar sesión en la grid de destino del tenant, un administrador de la grid debe primero "cambiar la contraseña del usuario raíz local" en la grid de destino.

Antes de que un usuario local clonado pueda iniciar sesión en la grid de destino del tenant, el usuario raíz del tenant clonado debe añadir una contraseña para el usuario en la grid de destino. Para obtener instrucciones, consulta "Gestiona usuarios" en las instrucciones para usar el Tenant Manager.

Inquilino creado sin un clon

Problema

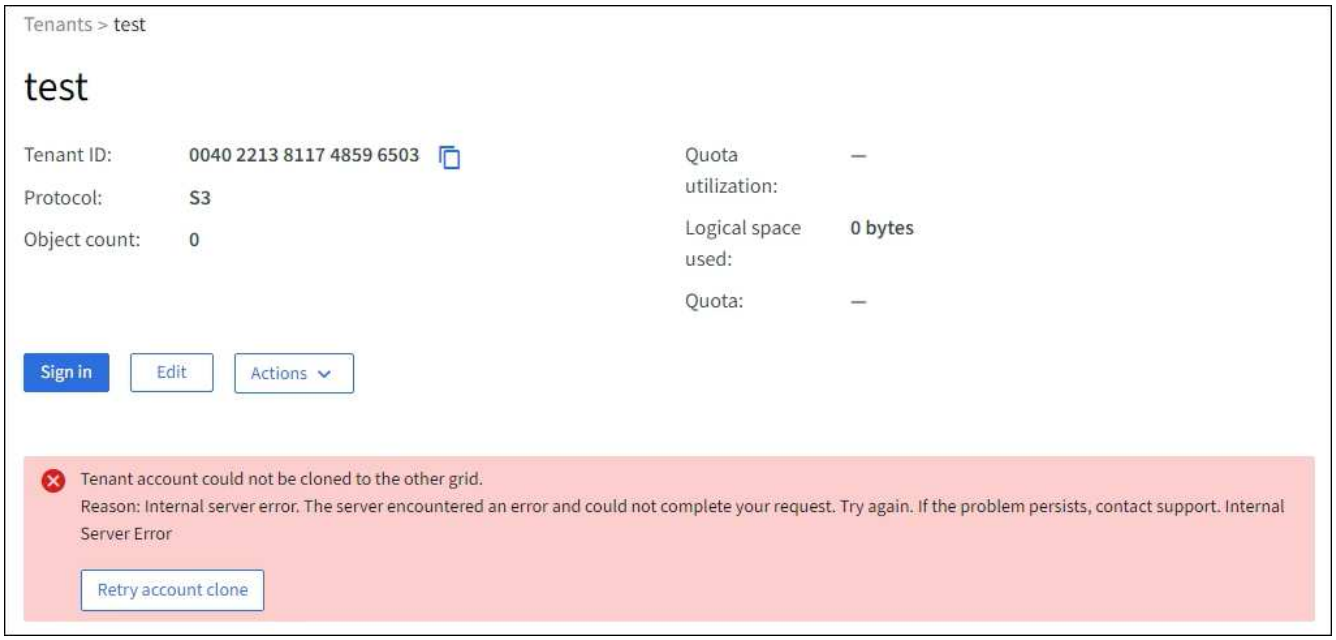
${post_edited_translations.segment}

Detalles

${post_edited_translations.segment}

Medidas recomendadas

1. Revisa el motivo indicado en el mensaje de error y resuelve cualquier problema de red o de otro tipo que pueda estar impidiendo que la conexión funcione. Consulta Alertas y errores de conexión de la federación de grid.
2. Sigue las instrucciones para probar una conexión a la federación de grid en "Gestiona las conexiones de la federación de grid" y confirma que el problema se ha solucionado.
3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
6. Selecciona **Retry account clone**.



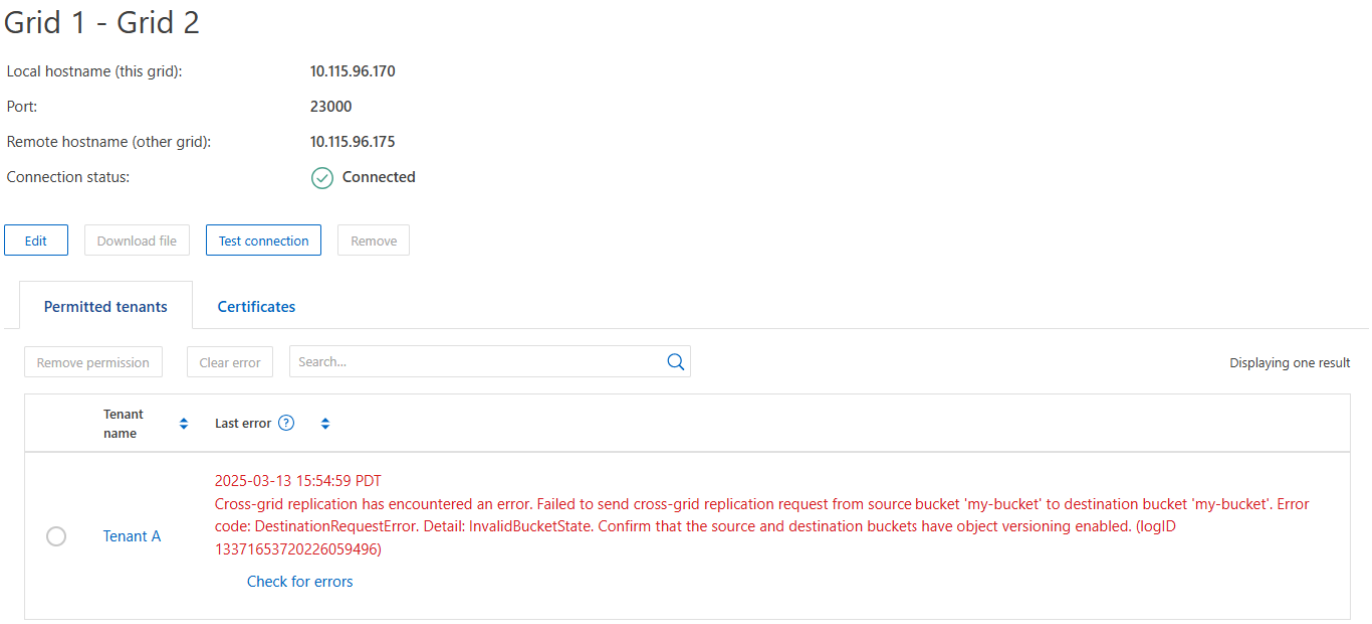
Si el error se ha solucionado, la cuenta del tenant ahora se clonará en la otra grid.

Alertas y errores de replicación entre grids

${post_edited_translations.segment}

Problema

Cuando "ver una conexión de federación de grid" (o cuando "${post_edited_translations.segment}" para una conexión), notas un error en la columna **Último error** de la página de detalles de la conexión. Por ejemplo:



Detalles

Para cada conexión de federación de redes, la columna **Último error** muestra el error más reciente que se haya producido, si lo hay, cuando se estaban replicando los datos de un inquilino a la otra red. Esta columna muestra solo el último error de replicación entre redes que se haya producido; los errores anteriores que pudieran haber ocurrido no se muestran. Un error en esta columna puede ocurrir por alguna de estas razones:

- No se encontró la versión del objeto de origen.
- ${post_edited_translations.segment}
- Se eliminó el bucket de destino.
- ${post_edited_translations.segment}
- El bucket de destino tiene el control de versiones suspendido.
- El bucket de destino fue recreado por la misma cuenta, pero ahora no tiene versiones.
- ${post_edited_translations.segment}
- El objeto de origen tiene configuraciones de S3 Object Lock y S3 Object Lock está desactivado en el depósito de destino.

Medidas recomendadas

Si aparece un mensaje de error en la columna **Último error**, sigue estos pasos:

1. Revisa el texto del mensaje.
2. Realiza las acciones recomendadas. Por ejemplo, si se suspendió el control de versiones en el bucket de destino para la replicación entre grids, vuelve a habilitar el control de versiones para ese bucket.
3. Selecciona la conexión o la cuenta de inquilino de la tabla.
4. Selecciona **Borrar error**.
5. ${post_edited_translations.segment}
6. Espera 5-6 minutos y luego ingiere un nuevo objeto en el bucket. Confirma que el mensaje de error no vuelva a aparecer.

Para asegurarte de que el mensaje de error se borre, espera al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingresar un nuevo objeto.

Después de que soluciones el error, podría aparecer un nuevo **Último error** si se ingieren objetos en un bucket diferente que también tenga un error.

7. Para determinar si algún objeto no se pudo replicar debido al error del bucket, consulta "Identifica y vuelve a intentar las operaciones de replicación que hayan fallado".

Alerta de fallo permanente en la replicación entre grids

Problema

Se activó la alerta **Cross-grid replication permanent failure**.

Detalles

Esta alerta indica que los objetos de los inquilinos no se pueden replicar entre los buckets de dos grids debido a un motivo que requiere la intervención del usuario para resolverse. Esta alerta suele deberse a un cambio en el bucket de origen o en el de destino.

Medidas recomendadas

1. Inicia sesión en la grid donde se activó la alerta.
2. Ve a **Configuración** > **Sistema** > **Grid federation** y busca el nombre de la conexión que aparece en la alerta.
3. En la pestaña **Permitted tenants**, consulta la columna **Last error** para determinar qué cuentas de tenant presentan errores.
4. Para obtener más información sobre el fallo, consulta las instrucciones de "Supervisa las conexiones de la federación de grid" para revisar las métricas de replicación entre grids.
5. Para cada cuenta de inquilino afectada:
   a. Consulta las instrucciones en "Supervisa la actividad de los inquilinos" para comprobar que el inquilino no ha superado su cuota en la grid de destino para la replicación entre grids.
   b. Según sea necesario, aumenta la cuota del inquilino en la red de destino para permitir que se guarden nuevos objetos.
6. Para cada inquilino afectado, inicia sesión en Tenant Manager en ambas grids, para que puedas comparar la lista de buckets.
7. ${post_edited_translations.segment}
   - Existe un bucket correspondiente para el mismo tenant en la otra grid (hay que utilizar el nombre exacto).
   - En ambos buckets está activado el control de versiones de objetos (el control de versiones no se puede suspender en ninguna de las dos grids).
   - Ninguno de los dos buckets se encuentra en el estado **Eliminación de objetos: solo lectura**.
8. Para confirmar que el problema se ha resuelto, consulta las instrucciones en "Supervisa las conexiones de la federación de grid" para revisar las métricas de replicación entre grids, o sigue estos pasos:
   a. Vuelve a la página de la federación Grid.
   b. Selecciona el inquilino afectado y selecciona **Borrar error** en la columna **Último error**.
   c. ${post_edited_translations.segment}

d. Espera 5-6 minutos y luego ingiere un nuevo objeto en el bucket. Confirma que el mensaje de error no vuelva a aparecer.

> Para asegurarte de que el mensaje de error se borre, espera al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingresar un nuevo objeto.

> ${post_edited_translations.segment}

a. Accede a "Identifica y vuelve a intentar las operaciones de replicación que hayan fallado" para identificar cualquier objeto o marcador de eliminación que no se haya replicado en la otra grid y volver a intentar la replicación si es necesario.

Alerta de recurso de replicación entre grids no disponible

Problema

Se activó la alerta **Cross-grid replication resource unavailable**.

Detalles

Esta alerta indica que las solicitudes de replicación entre grids están pendientes porque un recurso no está disponible. Por ejemplo, podría haber un error de red.

Medidas recomendadas

1. Supervisa la alerta para comprobar si el problema se resuelve por sí solo.
2. Si el problema persiste, determina si alguna de las grids tiene una alerta de **Grid federation connection failure** para la misma conexión o una alerta de **Unable to communicate with node** para un nodo. Esta alerta podría resolverse cuando soluciones esas alertas.
3. Para obtener más información sobre el fallo, consulta las instrucciones de "Supervisa las conexiones de la federación de grid" para revisar las métricas de replicación entre grids.
4. Si no puedes resolver la alerta, ponte en contacto con soporte técnico.

La replicación entre grids continuará con normalidad una vez que se resuelva el problema.

Identifica y vuelve a intentar las operaciones de replicación fallidas de StorageGRID

Después de resolver la alerta **Cross-grid replication permanent failure**, debes comprobar si hay algún objeto o marcador de eliminación que no se haya replicado en la otra grid. Luego puedes volver a ingresar estos objetos o usar la Grid Management API para volver a intentar la replicación.

La alerta **«Fallo permanente en la replicación entre redes»** indica que los objetos del inquilino no se pueden replicar entre los buckets de dos redes por un motivo que requiere la intervención del usuario para resolverse. Esta alerta suele deberse a un cambio en el bucket de origen o en el de destino. Para obtener más información, consulta "${post_edited_translations.segment}".

Determina si algún objeto no se replicó

Para determinar si hay algún objeto o marcador de eliminación que no se haya replicado en la otra grid, puedes buscar en el registro de auditoría los mensajes "${post_edited_translations.segment}". Este mensaje se añade al registro cuando StorageGRID no consigue replicar un objeto, un objeto multiparte o un marcador

de eliminación al bucket de destino.

Puedes usar la "${post_edited_translations.segment}" para traducir los resultados a un formato más fácil de leer.

Antes de empezar

- Tienes permiso de acceso root.
- Tienes el archivo `Passwords.txt`.
- ${post_edited_translations.segment}

Pasos

1. Inicia sesión en el nodo de administración principal:
   a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
   c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
   d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

      Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. ${post_edited_translations.segment}

   Por ejemplo, este comando busca con «grep» todos los mensajes CGRR de 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 tendrán un aspecto similar al de este ejemplo, que contiene entradas correspondientes a seis mensajes CGRR. En el ejemplo, todas las solicitudes de replicación entre grids devolvieron un error general porque no se pudo replicar el objeto. Los tres primeros errores son de operaciones de "replicate object", y los tres últimos errores son de operaciones de "replicate delete marker".

```
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 entre grids CGRR	El nombre de la solicitud
inquilino	El ID de cuenta del inquilino
${post_edited_translations.segment}	El identificador de la conexión de la federación de grid
operación	El tipo de operación de replicación que se estaba intentando realizar: • replicar objeto • replicar marcador de eliminación • replicar objeto multiparte
bucket	El nombre del bucket
objeto	El nombre del objeto
versión	El identificador de versión del objeto

Campo	Descripción
error	El tipo de error. Si la replicación entre grids falló, el error es «Error general».

Reintentar las replicaciones fallidas

${post_edited_translations.segment}

- Vuelve a introducir cada objeto en el bucket de origen.
- ${post_edited_translations.segment}

Pasos

1. En la parte superior del Grid Manager, selecciona el icono de ayuda y selecciona **API documentation**.
2. Selecciona **Ir a la documentación privada de la API**.

> Los puntos finales de la API de StorageGRID marcados como «Privados» están sujetos a cambios sin previo aviso. Los puntos finales privados de StorageGRID también ignoran la versión de la API de la solicitud.

3. ${post_edited_translations.segment}

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. ${post_edited_translations.segment}
5. En el cuadro de texto **body**, reemplaza la entrada de ejemplo de **versionID** por un identificador de versión del audit.log que corresponda a una solicitud de replicación entre grids que haya fallado.

   ${post_edited_translations.segment}

6. Selecciona **Ejecutar**.
7. ${post_edited_translations.segment}

> «Pendiente» significa que la solicitud de replicación entre grids se ha añadido a la cola interna para su procesamiento.

Supervisar los reintentos de replicación

Debes supervisar las operaciones de reintento de replicación para asegurarte de que se completan.

> Puede que la replicación de un objeto o de un marcador de eliminación en la otra grid tarde varias horas o incluso más.

Puedes supervisar las operaciones de reintento de dos formas:

- Utiliza una solicitud S3 "HeadObject" o "GetObject". La respuesta incluye el encabezado de respuesta específico de StorageGRID `x-ntap-sg-cgr-replication-status`, que tendrá uno de los siguientes valores:

${post_edited_translations.segment}	Estado de la replicación
Fuente	• ${post_edited_translations.segment} • **PENDIENTE**: El objeto aún no se ha replicado. • **ERROR**: La replicación falló debido a un error permanente. Un usuario debe solucionar el error.
Destino	**RÉPLICA**: El objeto fue replicado desde la cuadrícula de origen.

- ${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. ${post_edited_translations.segment}
3. En la sección de Parámetros, introduce el ID de versión que usaste en la solicitud `cross-grid-replication-retry-failed`.
4. Selecciona **Ejecutar**.
5. Comprueba que el código de respuesta del servidor sea **200**.
6. Comprueba el estado de la replicación, que será uno de los siguientes:
   - **PENDIENTE**: El objeto aún no se ha replicado.
   - ${post_edited_translations.segment}
   - **FALLO**: La replicación falló debido a un error permanente. Un usuario debe solucionar el error.

Gestiona la seguridad

Administra la seguridad en StorageGRID

${post_edited_translations.segment}

Gestionar el cifrado

StorageGRID ofrece varias opciones para cifrar datos. Debes "revisar los métodos de cifrado disponibles" para determinar cuáles se ajustan a tus requisitos de protección de datos.

Gestiona certificados

Puedes "configurar y gestionar los certificados del servidor" usar para las conexiones HTTP o los certificados de cliente que se emplean para autenticar la identidad de un cliente o usuario ante el servidor.

Configura servidores de gestión de claves

El uso de un "servidor de gestión de claves" te permite proteger los datos de StorageGRID incluso si se retira un dispositivo del centro de datos. Una vez cifrados los volúmenes del dispositivo, no podrás acceder a ningún

dato del mismo a menos que el nodo pueda comunicarse con el KMS.

${post_edited_translations.segment}

Gestiona la configuración del proxy

Si usas los servicios de plataforma de S3 o Cloud Storage Pools, puedes configurar un "servidor proxy de almacenamiento" entre los nodos de almacenamiento y los endpoints de S3 externos. Si envías paquetes de AutoSupport a través de HTTPS o HTTP, puedes configurar un "servidor proxy de administración" entre los nodos de administración y el soporte técnico.

Controla los cortafuegos

Para mejorar la seguridad de tu sistema, puedes controlar el acceso a los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en "cortafuegos externo". También puedes controlar el acceso de red a cada nodo configurando su "cortafuegos interno". Puedes impedir el acceso en todos los puertos excepto aquellos necesarios para tu implementación.

Revisa los métodos de cifrado de StorageGRID

StorageGRID ofrece varias opciones para cifrar datos. Debes revisar los métodos disponibles para determinar cuáles se ajustan a tus requisitos de protección de datos.

La tabla ofrece un resumen a grandes rasgos de los métodos de cifrado disponibles en StorageGRID.

Opción de cifrado	Cómo funciona	${post_edited_translations.segment}
Servidor de gestión de claves (KMS) en Grid Manager	Tú "configurar un servidor de gestión de claves" para el sitio de StorageGRID y "activar el cifrado de nodos para el dispositivo". Luego, un nodo del dispositivo se conecta al KMS para solicitar una clave de cifrado de claves (KEK). Esta clave cifra y descifra la clave de cifrado de datos (DEK) en cada volumen.	Nodos de appliance que tienen activada la opción **Cifrado de nodo** durante la instalación. Todos los datos del appliance están protegidos contra la pérdida física o la retirada del centro de datos. **Nota**: La gestión de claves de cifrado mediante un KMS solo es compatible con los Storage Nodes y los servicios appliances.

Opción de cifrado	Cómo funciona	${post_edited_translations.segment}
Página de cifrado de unidades en el instalador de StorageGRID Appliance	Si el dispositivo contiene unidades que admiten cifrado por hardware, puedes establecer una frase de contraseña para la unidad durante la instalación. Cuando estableces una frase de contraseña para la unidad, es imposible que alguien recupere datos válidos de las unidades que se hayan retirado del sistema, a menos que conozca la frase de contraseña. Antes de iniciar la instalación, ve a **Configure Hardware** > **Drive Encryption** para establecer una frase de contraseña para la unidad que se aplique a todas las unidades con autocifrado gestionadas por StorageGRID en un nodo.	Dispositivos que incorporan unidades con cifrado automático. Todos los datos en las unidades protegidas están protegidos contra la pérdida física o la extracción del centro de datos. El cifrado de unidades no se aplica a las unidades gestionadas por SANtricity. Si tienes un dispositivo de almacenamiento con unidades de autocifrado y controladoras SANtricity, puedes habilitar la seguridad de las unidades en SANtricity.
Seguridad de las unidades en SANtricity System Manager	Si la función Drive Security está habilitada para tu dispositivo StorageGRID, puedes usar "SANtricity System Manager" para crear y gestionar la clave de seguridad. La clave es necesaria para acceder a los datos de las unidades protegidas.	Appliances de almacenamiento que tienen unidades con cifrado de disco completo (FDE) o unidades de autocifrado. Todos los datos de las unidades protegidas están protegidos contra la pérdida física o la extracción del centro de datos. No se puede usar con algunos appliances de almacenamiento ni con ningún appliance de servicios.
Cifrado de objetos almacenados	Activa la opción "Cifrado de objetos almacenados" en Grid Manager. Cuando está activada, cualquier objeto nuevo que no esté cifrado a nivel de bucket o a nivel de objeto se cifra durante la ingesta.	${post_edited_translations.segment} Los objetos almacenados actualmente no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados.

Opción de cifrado	Cómo funciona	${post_edited_translations.segment}
Cifrado de buckets de S3	Envías una solicitud PutBucketEncryption para habilitar el cifrado para el bucket. Cualquier objeto nuevo que no esté cifrado a nivel de objeto se cifrará durante la ingesta.	Solo datos de objetos S3 recién ingeridos. Debes especificar el cifrado para el bucket. Los objetos existentes del bucket no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados. "Operaciones en cubos"
Cifrado del lado del servidor (SSE) de objetos S3	Envías una solicitud S3 para almacenar un objeto e incluyes el encabezado de solicitud `x-amz-server-side-encryption`.	Solo datos de objetos S3 recién ingeridos. Se debe especificar el cifrado para el objeto. Los metadatos del objeto y otros datos confidenciales no están cifrados. StorageGRID gestiona las claves. "Utiliza el cifrado del lado del servidor"
Cifrado del lado del servidor de objetos S3 con claves proporcionadas por el cliente (SSE-C)	Envías una solicitud S3 para almacenar un objeto e incluyes 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 recién ingeridos. Se debe especificar el cifrado para el objeto. Los metadatos del objeto y otros datos confidenciales no están cifrados. Las claves se gestionan fuera de StorageGRID. "Utiliza el cifrado del lado del servidor"
Cifrado de volúmenes externos o almacenes de datos	Tú usas un método de cifrado externo a StorageGRID para cifrar un volumen o un almacén de datos completo, si tu plataforma de implementación lo admite.	${post_edited_translations.segment} Un método de cifrado externo permite un control más estricto sobre los algoritmos y las claves de cifrado. Se puede combinar con los demás métodos enumerados.

Opción de cifrado	Cómo funciona	${post_edited_translations.segment}
${post_edited_translations.segment}	Tú usas un método de cifrado fuera de StorageGRID para cifrar los datos y metadatos de los objetos antes de que se incorporen a StorageGRID.	Solo datos y metadatos de objetos (los datos de configuración del sistema no están cifrados). Un método de cifrado externo permite un control más estricto sobre los algoritmos y las claves de cifrado. Se puede combinar con los demás métodos enumerados. "Amazon Simple Storage Service - Guía del usuario: protección de datos mediante el cifrado del lado del cliente"

Utiliza varios métodos de cifrado

En función de tus necesidades, puedes utilizar más de un método de cifrado a la vez. Por ejemplo:

- Puedes utilizar un KMS para proteger los nodos de los dispositivos y también usar la función de seguridad de unidades en SANtricity System Manager para "doble cifrar" los datos en las unidades con cifrado automático de esos mismos dispositivos.
- Puedes utilizar un KMS para proteger los datos en los nodos del dispositivo y también usar la opción de cifrado de objetos almacenados para cifrar todos los objetos cuando se ingieren.

Si solo una pequeña parte de tus objetos requiere cifrado, plantéate controlar el cifrado a nivel de bucket o de objeto individual. Habilitar varios niveles de cifrado tiene un coste adicional de rendimiento.

Información relacionada

"Infórmate sobre las opciones de cifrado con certificación FIPS"

Gestiona certificados

Administra certificados de seguridad en StorageGRID

Los certificados de seguridad son pequeños archivos de datos que se usan para crear conexiones seguras y confiables entre los componentes de StorageGRID y entre los componentes de StorageGRID y los sistemas externos.

${post_edited_translations.segment}

- **Los certificados de servidor** son necesarios cuando usas conexiones HTTPS. Los certificados de servidor se usan para establecer conexiones seguras entre clientes y servidores, autenticando la identidad de un servidor ante sus clientes y proporcionando una vía de comunicación segura para los datos. El servidor y el cliente tienen cada uno una copia del certificado.
- **Los certificados de cliente** autentican la identidad de un cliente o usuario ante el servidor, lo que proporciona una autenticación más segura que las contraseñas por sí solas. Los certificados de cliente no cifran los 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 que figura en su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión con el servidor utilizando la misma clave pública.

StorageGRID funciona como el servidor para algunas conexiones (como el endpoint del equilibrador de carga) o como el cliente para otras conexiones (como el servicio de replicación de CloudMirror).

Certificado CA predeterminado de Grid

StorageGRID tiene una autoridad de certificación (CA) integrada que genera un certificado de CA de Grid interno durante la instalación del sistema. El certificado de CA de Grid se usa, de forma predeterminada, para proteger el tráfico interno de StorageGRID. Una autoridad de certificación (CA) externa puede emitir certificados personalizados que cumplan plenamente con las políticas de seguridad de la información de tu organización.

Utiliza el certificado CA de Grid para entornos que no sean de producción. Para producción, utiliza certificados personalizados firmados por una autoridad de certificación externa. Se admiten las conexiones no seguras sin certificado, pero no se recomiendan.

- Los certificados CA personalizados no eliminan los certificados internos; sin embargo, los certificados personalizados deben ser los especificados para verificar las conexiones al servidor.
- Todos los certificados personalizados deben cumplir con la "Directrices para el refuerzo del sistema para certificados de servidor".
- StorageGRID admite la agrupación de certificados de una autoridad de certificación (CA) en un único archivo (lo que se conoce como paquete de certificados de CA).

> StorageGRID también incluye certificados de CA del sistema operativo que son idénticos en todas las grids. En entornos de producción, asegúrate de especificar un certificado personalizado firmado por una autoridad de certificación externa en lugar del certificado de CA del sistema operativo.

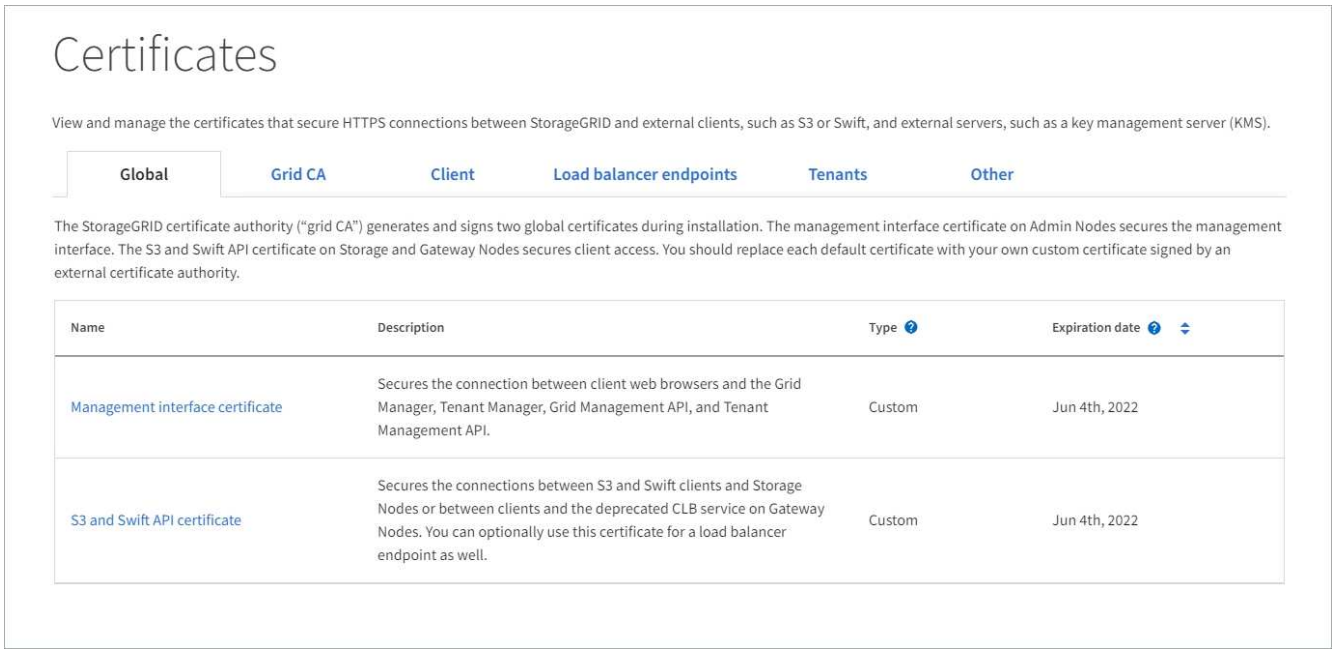
Las variantes de los tipos de certificados de servidor y de cliente se implementan de varias maneras. Debes tener listos todos los certificados necesarios para tu configuración específica de StorageGRID antes de configurar el sistema.

Accede a los certificados de seguridad

Puedes acceder a la información sobre todos los certificados de StorageGRID en un único lugar, junto con enlaces al flujo de trabajo de configuración de cada certificado.

Pasos

1. ${post_edited_translations.segment}



2. Selecciona una pestaña en la página Certificados para obtener información sobre cada categoría de certificado y acceder a la configuración de los certificados. Puedes acceder a una pestaña si tienes el "permiso correspondiente".

   - ${post_edited_translations.segment}
   - **Grid CA**: Protege el tráfico interno de StorageGRID.
   - **Cliente**: Protege las conexiones entre los clientes externos y la base de datos Prometheus de StorageGRID.
   - ${post_edited_translations.segment}
   - **Inquilinos**: Garantiza la seguridad de las conexiones con los servidores de federación de identidades o desde los endpoints de los servicios de la plataforma hasta los recursos de almacenamiento S3.
   - **Otros**: Protege las conexiones a StorageGRID que requieren certificados específicos.

     A continuación se describe cada pestaña, con enlaces a información adicional sobre los certificados.

Global

Los certificados globales protegen el acceso a StorageGRID desde navegadores web y clientes externos de la API de S3. Durante la instalación, la autoridad de certificación de StorageGRID genera inicialmente dos certificados globales. La práctica recomendada para un entorno de producción es utilizar certificados personalizados firmados por una autoridad de certificación externa.

- Certificado de interfaz de gestión: Protege las conexiones de los navegadores web de los clientes a las interfaces de gestión de StorageGRID.
- Certificado de la API de S3: Protege las conexiones de la API del cliente con los nodos de almacenamiento, los nodos de administración y los nodos de puerta de enlace, que las aplicaciones cliente de S3 utilizan para cargar y descargar datos de objetos.

${post_edited_translations.segment}

- **Nombre**: Nombre del certificado con un enlace para gestionar el certificado.
- **Descripción**
- **Tipo**: personalizado o predeterminado. + Siempre debes usar un certificado personalizado para mejorar la seguridad de la grid.
- ${post_edited_translations.segment}

Puedes:

- Sustituye los certificados predeterminados por certificados personalizados firmados por una autoridad de certificación externa para mejorar la seguridad del grid:
  - "Sustituye el certificado predeterminado de la interfaz de gestión generado por StorageGRID" se utiliza para las conexiones de Grid Manager y Tenant Manager.
  - "${post_edited_translations.segment}" se usa para las conexiones del Storage Node y del endpoint del equilibrador de carga (opcional).
- "Restaurar el certificado predeterminado de la interfaz de gestión".
- "Restablece el certificado predeterminado de la API de S3".
- "Utiliza un script para generar un nuevo certificado autofirmado de la interfaz de gestión".
- Copia o descarga el "certificado de interfaz de gestión" o "Certificado de la API de S3".

${post_edited_translations.segment}

El Certificado 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 certificado.

Puedes "${post_edited_translations.segment}", pero no puedes cambiarlo.

Cliente

Certificados de cliente, generados por una autoridad de certificación externa, protegen las conexiones entre las herramientas de monitorización externas y la base de datos StorageGRID Prometheus.

La tabla de certificados contiene una fila para cada certificado de cliente configurado e indica si el certificado puede usarse para acceder a la base de datos de Prometheus, junto con la fecha de

caducidad del certificado.

Puedes:

- "Sube o genera un nuevo certificado de cliente."
- Selecciona el nombre de un certificado para ver los detalles del certificado, donde puedes:
  - "Cambia el nombre del certificado de cliente."
  - "Configura el permiso de acceso a Prometheus."
  - "Sube y sustituye el certificado de cliente."
  - "Copia o descarga el certificado de cliente."
  - "Elimina el certificado de cliente."
- Selecciona **Acciones** para "editar", "${post_edited_translations.segment}" o "eliminar" rápidamente un certificado de cliente. Puedes seleccionar hasta 10 certificados de cliente y eliminarlos de una sola vez usando **Acciones** > **Eliminar**.

${post_edited_translations.segment}

${post_edited_translations.segment} protege las conexiones entre los clientes S3 y el servicio de equilibrador de carga de StorageGRID en los nodos de puerta de enlace y los nodos de administración.

La tabla de puntos de conexión del equilibrador de carga contiene una fila para cada punto de conexión configurado e indica si se está utilizando el certificado global de la API S3 o un certificado personalizado del punto de conexión del equilibrador de carga para dicho punto de conexión. También se muestra la fecha de caducidad de cada certificado.

> Los cambios en el certificado de un endpoint pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Puedes:

- "${post_edited_translations.segment}", incluidos los datos de su certificado.
- "Especifica un certificado de endpoint del equilibrador de carga para FabricPool."
- "Utiliza el certificado global de la API de S3" en lugar de generar un nuevo certificado para el endpoint del balanceador de carga.

Inquilinos

Los usuarios pueden utilizar certificados del servidor de federación de identidades o certificados de los endpoints de servicio de la plataforma para asegurar sus conexiones con StorageGRID.

La tabla de inquilinos tiene una fila para cada inquilino e indica si cada inquilino tiene permiso para usar su propia fuente de identidad o los servicios de la plataforma.

Puedes:

- "Selecciona un nombre de inquilino para iniciar sesión en el Tenant Manager"
- "Selecciona el nombre de un inquilino para ver los detalles de la federación de identidades del inquilino"
- "Selecciona un nombre de cliente para ver los detalles de los servicios de la plataforma de ese cliente"

- "Especifica un certificado de endpoint de servicio de plataforma durante la creación del endpoint"

Otros

StorageGRID utiliza otros certificados de seguridad para fines específicos. Estos certificados se enumeran según su nombre funcional. Otros certificados de seguridad incluyen:

- Certificados de Cloud Storage Pool
- Certificados de notificación por correo electrónico
- Certificados del servidor syslog externo
- Certificados de conexión de la federación de grid
- Certificados de federación de identidades
- <<${post_edited_translations.segment},Certificados del servidor de gestión de claves (KMS)>>
- <<${post_edited_translations.segment},Certificados de inicio de sesión único>>

La información indica el tipo de certificado que utiliza una función y las fechas de caducidad de los certificados del servidor y del cliente, según corresponda. Si seleccionas el nombre de una función, se abre una pestaña del navegador donde puedes ver y editar los detalles del certificado.

> Solo podrás ver y acceder a la información de otros certificados si dispones del "permiso correspondiente".

Puedes:

- "Especifica un certificado de Cloud Storage Pool para S3, C2S S3 o Azure"
- "Especifica un certificado para las notificaciones de alerta por correo electrónico"
- "Usa un certificado para un servidor syslog externo"
- "Rotar los certificados de conexión de la federación de grid"
- "Ver y editar un certificado de federación de identidades"
- "Sube los certificados del servidor y del cliente del servidor de gestión de claves (KMS)"
- "Especificar manualmente un certificado de SSO para una relación de confianza de parte confiable"

Detalles del certificado de seguridad

A continuación se describe cada tipo de certificado de seguridad, 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 navegadores web de los clientes y la interfaz de gestión de StorageGRID, permitiendo que los usuarios accedan a Grid Manager y Tenant Manager sin avisos de seguridad. Este certificado también autentica las conexiones a la Grid Management API y a la Tenant Management API. Puedes utilizar el certificado predeterminado creado durante la instalación o subir un certificado personalizado.	**Configuración** > **Seguridad** > **Certificados**, selecciona la pestaña **Global** y luego selecciona **Management interface certificate**	"Configura los certificados de la interfaz de gestión"

Certificado de la API de S3

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica las conexiones seguras de los clientes S3 a un nodo de almacenamiento y a los puntos de conexión del equilibrador de carga (opcional).	**Configuración** > **Seguridad** > **Certificados**, selecciona la pestaña **Global** y luego selecciona **S3 API certificate**	"Configura los certificados de la API de S3"

Certificado CA de Grid

Consulta el Descripción predeterminada del certificado CA de la grid.

Certificado de cliente de administrador

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Cliente	Instalado en cada cliente, permitiendo que StorageGRID autentique el acceso de clientes externos. • Permite a los clientes externos autorizados acceder a la base de datos de StorageGRID Prometheus. • Permite supervisar de forma segura StorageGRID mediante herramientas externas.	**Configuración** > **Seguridad** > **Certificados** y luego selecciona la pestaña **Cliente**	"Configurar certificados de cliente"

Certificado del endpoint del balanceador de carga

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los clientes de S3 y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace y los nodos de administración. Puedes cargar o generar un certificado del equilibrador de carga cuando configuras un punto de conexión del equilibrador de carga. Las aplicaciones cliente usan el certificado del equilibrador de carga al conectarse a StorageGRID para guardar y recuperar datos de objetos. También puedes utilizar una versión personalizada del certificado global Certificado de la API de S3 para autenticar las conexiones al servicio de equilibrador de carga. Si se utiliza el certificado global para autenticar las conexiones del equilibrador de carga, no necesitas cargar ni generar un certificado independiente para cada endpoint del equilibrador de carga. **Nota:** El certificado utilizado para la autenticación del equilibrador de carga es el que más se utiliza durante el funcionamiento normal de StorageGRID.	**Configuración** > **Red** > **Puntos de conexión del equilibrador de carga**	• "Configura los puntos de conexión del equilibrador de carga" • "Crear un punto de conexión del equilibrador de carga para FabricPool"

Certificado del endpoint de Cloud Storage Pool

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión desde un StorageGRID Cloud Storage Pool a una ubicación de almacenamiento externa, como S3 Glacier o Microsoft Azure Blob storage. Se requiere un certificado diferente para cada tipo de proveedor de nube.	**ILM** > **Grupos de almacenamiento**	"Crear un grupo de almacenamiento en la nube"

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 StorageGRID que se usa para las notificaciones de alertas. • Si la comunicación con el servidor SMTP requiere Transport Layer Security (TLS), debes especificar el certificado de la autoridad de certificación (CA) del servidor de correo electrónico. • Especifica un certificado de cliente solo si el servidor de correo electrónico SMTP requiere certificados de cliente para la autenticación.	**Alertas** > **Email setup**	"Configura notificaciones por correo electrónico para las alertas"

Certificado del servidor 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 las conexiones TCP, RELP/TCP y UDP a un servidor syslog externo.	**Configuración** > **Supervisión** > **Servidor de auditoría y syslog**	"Utiliza un servidor syslog externo"

Certificado de conexión de Grid federation

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica y cifra la información enviada entre el sistema StorageGRID actual y otra grid en una conexión de federación de grids.	**Configuración** > **Sistema** > **Federación de redes**	• "Crear conexiones de federación de grid" • "Rotar los 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 un sistema externo gestione los grupos de administradores y los usuarios.	**Configuración** > **Control de acceso** > **Federación de identidades**	"Usa la federación de identidades"

${post_edited_translations.segment}

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre StorageGRID y un servidor externo de gestión de claves (KMS), que proporciona claves de cifrado a los nodos del dispositivo StorageGRID.	**Configuración** > **Seguridad** > **Servidor de gestión de claves**	"Agregar servidor de gestión de claves (KMS)"

Certificado del endpoint de los servicios de plataforma

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	${post_edited_translations.segment}	**Tenant Manager** > **STORAGE (S3)** > **Puntos de conexión de los servicios de la plataforma**	"Crear un endpoint de servicios de plataforma" "Editar el endpoint de los servicios de plataforma"

${post_edited_translations.segment}

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 las solicitudes de inicio de sesión único (SSO).	**Configuración** > **Control de acceso** > **Inicio de sesión único**	"${post_edited_translations.segment}"

${post_edited_translations.segment}

Ejemplo 1: servicio de equilibrado de carga

En este ejemplo, StorageGRID actúa como servidor.

1. Configuras un punto final del equilibrador de carga y subes o generas un certificado de servidor en StorageGRID.
2. Configuras una conexión de cliente S3 al endpoint del balanceador de carga y subes el mismo certificado al cliente.
3. Cuando el cliente desea guardar o recuperar datos, se conecta al punto de acceso del equilibrador de carga mediante HTTPS.

4. StorageGRID responde con el certificado del servidor, que contiene una clave pública, y con una firma basada en la clave privada.
5. El cliente compara la firma del servidor con la firma que figura en su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión usando la misma clave pública.
6. ${post_edited_translations.segment}

Ejemplo 2: Servidor externo de gestión de claves (KMS)

${post_edited_translations.segment}

1. Mediante un software externo de servidor de gestión de claves (KMS), configuras StorageGRID como cliente KMS y obtienes un certificado de servidor firmado por una autoridad de certificación (CA), un certificado público de cliente y la clave privada correspondiente a dicho certificado de cliente.
2. Usando el Grid Manager, configuras un servidor KMS y subes los certificados del servidor y del cliente, además de la clave privada del cliente.
3. ${post_edited_translations.segment}
4. El servidor KMS valida la firma del certificado y decide que puede confiar en StorageGRID.
5. El servidor KMS responde utilizando la conexión validada.

Tipos de certificados de servidor compatibles en StorageGRID

${post_edited_translations.segment}

> 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. Consulta "Gestiona certificados de seguridad". Si configuras una política de seguridad personalizada que no sea compatible con el certificado del servidor, puedes "volver temporalmente a la política de seguridad predeterminada".

Para obtener más información sobre cómo StorageGRID protege las conexiones de los clientes, consulta "${post_edited_translations.segment}".

Configura certificados de la interfaz de gestión en StorageGRID

Puedes sustituir el certificado predeterminado de la interfaz de gestión por un único certificado personalizado que permita a los usuarios acceder a Grid Manager y a Tenant Manager sin que aparezcan advertencias de seguridad. También puedes volver al certificado predeterminado de la interfaz de gestión o generar uno nuevo.

Acerca de esta tarea

De forma predeterminada, cada nodo de administración recibe un certificado firmado por la CA del grid. Puedes sustituir estos certificados firmados por la CA por un único certificado de interfaz de gestión personalizado común y su clave privada correspondiente.

Como se usa un único certificado de interfaz de gestión personalizado para todos los nodos de administración, debes especificar el certificado como un certificado comodín o multidominio si los clientes necesitan verificar el nombre de host al conectarse a Grid Manager y Tenant Manager. Define el certificado personalizado de manera que coincida con todos los nodos de administración del grid.

Debes completar la configuración en el servidor y, dependiendo de la autoridad de certificación (CA) raíz que

utilices, es posible que los usuarios también tengan que instalar el certificado de la CA de Grid en el navegador web que vayan a utilizar para acceder al Grid Manager y al Tenant Manager.

Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor caducado, se activa la alerta **Caducidad del certificado de servidor para la interfaz de gestión** cuando dicho certificado está a punto de caducar. Cuando lo necesites, puedes ver cuándo caduca el certificado actual seleccionando **Configuración** > **Seguridad** > **Certificados** y revisando la fecha de caducidad del certificado de la interfaz de gestión en la pestaña Global.

${post_edited_translations.segment}

- El certificado de tu interfaz de gestión personalizada caduca.
- Tú Volver de un certificado personalizado de la interfaz de gestión al certificado predeterminado del servidor.

Agrega un certificado personalizado para la interfaz de gestión

Para añadir un certificado personalizado para la interfaz de gestión, puedes proporcionar tu propio certificado o generar uno usando Grid Manager.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, selecciona **Certificado de la interfaz de gestión**.
3. Selecciona **Usar certificado personalizado**.
4. Sube o genera el certificado.

Subir certificado

Sube los archivos de certificados del servidor necesarios.

a. Selecciona **Cargar certificado**.

b. ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - **Clave privada del certificado**: El archivo de la 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 de CA**: Un único archivo opcional que contiene los certificados de cada autoridad de certificación (CA) emisora intermedia. El archivo debe contener cada uno de los archivos de certificados de CA codificados en formato PEM, concatenados en el orden de la cadena de certificados.

c. Despliega **Detalles del certificado** para ver los metadatos de cada certificado que subiste. Si subiste un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

   - ${post_edited_translations.segment}

     Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Selecciona **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Selecciona **Guardar**. + El certificado de la interfaz de gestión personalizada se utiliza para todas las nuevas conexiones posteriores a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

Generar certificado

${post_edited_translations.segment}

> ${post_edited_translations.segment}

a. Selecciona **Generar certificado**.

b. ${post_edited_translations.segment}

Campo	Descripción
Nombre de dominio	Uno o más dominios completos para incluir en el certificado. Usa un * como comodín para representar varios nombres de dominio.
${post_edited_translations.segment}	Una o varias direcciones IP para incluir en el certificado.

Campo	Descripción
${post_edited_translations.segment}	${post_edited_translations.segment} Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la primera dirección IP como nombre común (CN) del sujeto.
Días de validez	Número de días después de la creación en los que caduca el certificado.
${post_edited_translations.segment}	${post_edited_translations.segment} ${post_edited_translations.segment} **Nota**: Deja esta casilla marcada a menos que tengas problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

c. Selecciona **Generar**.

d. Selecciona **Detalles del certificado** para ver los metadatos del certificado generado.

- ${post_edited_translations.segment}

  Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Selecciona **Guardar**. + El certificado de la interfaz de gestión personalizada se utiliza para todas las nuevas conexiones posteriores a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

5. Actualiza la página para asegurarte de que el navegador web esté actualizado.

> Después de subir o generar un nuevo certificado, espera hasta un día para que se borren las alertas relacionadas con la caducidad del certificado.

6. Después de que añades un certificado personalizado de la interfaz de gestión, la página de certificado de la interfaz de gestión muestra información detallada sobre los certificados que están en uso. + Puedes descargar o copiar el certificado PEM según lo necesites.

Restaurar el certificado predeterminado de la interfaz de gestión

Puedes volver a utilizar el certificado predeterminado de la interfaz de administración para las conexiones a Grid Manager y Tenant Manager.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, selecciona **Certificado de la interfaz de gestión**.
3. Selecciona **Usar certificado predeterminado**.

   Cuando restauras el certificado predeterminado de la interfaz de gestión, los archivos de certificado de servidor personalizados que configuraste se eliminan y no se pueden recuperar del sistema. El certificado predeterminado de la interfaz de gestión se utiliza para todas las nuevas conexiones de cliente posteriores.

4. Actualiza la página para asegurarte de que el navegador web esté actualizado.

Utiliza un script para generar un nuevo certificado autofirmado de la interfaz de gestión

Si se requiere una validación estricta del nombre de host, puedes utilizar un script para generar el certificado de la interfaz de gestión.

Antes de empezar

- Tienes "permisos de acceso específicos".
- Tienes el archivo `Passwords.txt`.

Acerca de esta tarea

La mejor práctica para un entorno de producción es utilizar un certificado firmado por una autoridad de certificación externa.

Pasos

1. Obtén el nombre de dominio completo (FQDN) de cada Admin Node.
2. Inicia sesión en el nodo de administración principal:
   a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
   c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
   d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

      Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

3. Configura StorageGRID con un nuevo certificado autofirmado.

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

   - En el caso de `--domains`, utiliza caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración. Por ejemplo, `*.ui.storagegrid.example.com` utiliza el carácter comodín * para representar `admin1.ui.storagegrid.example.com` y `admin2.ui.storagegrid.example.com`.
   - Establece `--type` en `management` para configurar el certificado de la interfaz de gestión, que usan Grid Manager y Tenant Manager.
   - Por defecto, los certificados generados tienen una validez de un año (365 días) y deben volver a generarse antes de que caduquen. Puedes usar el argumento `--days` para cambiar el periodo de validez predeterminado.

El periodo de validez de un certificado comienza cuando se ejecuta `make-certificate`. Debes asegurarte de que el cliente de gestión esté sincronizado con la misma fuente de tiempo que StorageGRID; de lo contrario, el cliente podría rechazar el certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

${post_edited_translations.segment}

4. Selecciona y copia el certificado.

   ${post_edited_translations.segment}

5. Cierra sesión en la línea de comandos. `$ exit`
6. Confirma que el certificado se configuró:
   a. ${post_edited_translations.segment}
   b. Selecciona **Configuración** > **Seguridad** > **Certificados**
   c. En la pestaña **Global**, selecciona **Certificado de la interfaz de gestión**.
7. Configura tu cliente de gestión para que use el certificado público que copiaste. Incluye las etiquetas BEGIN y END.

Descarga o copia el certificado de la interfaz de administración

Puedes guardar o copiar el contenido del certificado de la interfaz de administración para utilizarlo en otro lugar.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, selecciona **Certificado de la interfaz de gestión**.
3. Selecciona la pestaña **Servidor** o **Paquete de CA** y luego descarga o copia el certificado.

${post_edited_translations.segment}

Descarga el certificado o el paquete de CA `.pem`. Si utilizas un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Selecciona **Descargar certificado** o **Descargar paquete de CA**.

   Si estás descargando un paquete de CA, todos los certificados de las pestañas secundarias del paquete de CA se descargan en un único archivo.

b. Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado o paquete PEM de CA

Copia el texto del certificado para pegarlo en otro lugar. Si utilizas un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. ${post_edited_translations.segment}

   Si estás copiando un paquete de CA, todos los certificados de las pestañas secundarias del paquete de CA se copian juntos.

b. ${post_edited_translations.segment}

c. Guarda el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Configura certificados de la API S3 en StorageGRID

Puedes sustituir o restaurar el certificado de servidor que se utiliza para las conexiones de los clientes S3 a los nodos de almacenamiento o a los endpoints del balanceador de carga. El certificado de servidor personalizado de sustitución es específico de tu organización.

Hemos eliminado los detalles de Swift de esta versión del sitio de documentación. Consulta "StorageGRID 11.8: configura los certificados de las API de S3 y Swift".

Acerca de esta tarea

De forma predeterminada, a cada nodo de almacenamiento se le asigna un certificado de servidor X.509 firmado por la CA de la grid. Estos certificados firmados por la CA pueden sustituirse por un único certificado de servidor personalizado común y la clave privada correspondiente.

Se utiliza un único certificado de servidor personalizado para todos los nodos de almacenamiento, por lo que debes especificar el certificado como certificado comodín o multidominio si los clientes necesitan verificar el nombre de host al conectarse al endpoint de almacenamiento. Define el certificado personalizado de manera que coincida con todos los nodos de almacenamiento en el grid.

${post_edited_translations.segment}

Para asegurarte de que las operaciones no se interrumpan por un fallo en el certificado del servidor, la alerta **Vencimiento del certificado de servidor global para la API de S3** se activa cuando el certificado de servidor raíz está a punto de caducar. Si lo necesitas, puedes ver cuándo caduca el certificado actual seleccionando **Configuración** > **Seguridad** > **Certificados** y consultando la fecha de caducidad del certificado de la API de S3 en la pestaña Global.

Puedes subir o generar un certificado de API de S3 personalizado.

Agrega un certificado personalizado de la API de S3

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, selecciona **S3 API certificate**.
3. Selecciona **Usar certificado personalizado**.
4. Sube o genera el certificado.

Subir certificado

Sube los archivos de certificados del servidor necesarios.

a. Selecciona **Cargar certificado**.

b. ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - **Clave privada del certificado**: El archivo de la 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 de CA**: Un único archivo opcional que contiene los certificados de cada autoridad de certificación emisora intermedia. El archivo debe contener cada uno de los archivos de certificados de CA codificados en formato PEM, concatenados en el orden de la cadena de certificados.

c. Selecciona los detalles del certificado para ver los metadatos y el PEM de cada certificado personalizado de la API de S3 que hayas subido. Si subiste un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

   - ${post_edited_translations.segment}

     Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Selecciona **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Selecciona **Guardar**.

   El certificado de servidor personalizado se usa para las siguientes nuevas conexiones de clientes S3.

Generar certificado

${post_edited_translations.segment}

a. Selecciona **Generar certificado**.

b. ${post_edited_translations.segment}

Campo	Descripción
Nombre de dominio	Uno o más dominios completos para incluir en el certificado. Usa un * como comodín para representar varios nombres de dominio.
${post_edited_translations.segment}	Una o varias direcciones IP para incluir en el certificado.

Campo	Descripción
${post_edited_translations.segment}	${post_edited_translations.segment} Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la primera dirección IP como nombre común (CN) del sujeto.
Días de validez	Número de días después de la creación en los que caduca el certificado.
${post_edited_translations.segment}	${post_edited_translations.segment} ${post_edited_translations.segment} **Nota**: Deja esta casilla marcada a menos que tengas problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

c. Selecciona **Generar**.

d. Selecciona **Detalles del certificado** para mostrar los metadatos y el PEM del certificado personalizado de la API de S3 que se generó.

- ${post_edited_translations.segment}

  Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Selecciona **Guardar**.

El certificado de servidor personalizado se usa para las siguientes nuevas conexiones de clientes S3.

5. Selecciona una pestaña para mostrar los metadatos del certificado predeterminado del servidor StorageGRID, de un certificado firmado por una autoridad de certificación (CA) que se haya cargado o de un certificado personalizado que se haya generado.

> Después de subir o generar un nuevo certificado, espera hasta un día para que se borren las alertas relacionadas con la caducidad del certificado.

6. Actualiza la página para asegurarte de que el navegador web esté actualizado.
7. Después de añadir un certificado de la API de S3 personalizado, la página del certificado de la API de S3 muestra información detallada sobre el certificado de la API de S3 personalizado que está en uso. + Puedes descargar o copiar el PEM del certificado según sea necesario.

Restablece el certificado predeterminado de la API de S3

Puedes volver a utilizar el certificado predeterminado de la API de S3 para las conexiones de los clientes de S3 a los nodos de almacenamiento. Sin embargo, no puedes utilizar el certificado predeterminado de la API de S3 para un endpoint de un load balancer.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, selecciona **S3 API certificate**.
3. Selecciona **Usar certificado predeterminado**.

   Al restaurar la versión predeterminada del certificado global de la API de S3, los archivos de certificados de servidor personalizados que hayas configurado se eliminan y no pueden recuperarse del sistema. El certificado predeterminado de la API de S3 se usará para las siguientes nuevas conexiones de clientes S3 a Storage Nodes.

4. Selecciona **OK** para confirmar la advertencia y restablecer el certificado predeterminado de la API de S3.

   Si tienes permiso de acceso Root y se ha utilizado un certificado personalizado de la API de S3 para las conexiones al endpoint del balanceador de carga, se muestra una lista de endpoints del balanceador de carga a los que ya no podrás acceder usando el certificado predeterminado de la API de S3. Ve a "Configura los puntos de conexión del equilibrador de carga" para editar o eliminar los endpoints afectados.

5. Actualiza la página para asegurarte de que el navegador web esté actualizado.

Descarga o copia el certificado de la API de S3

${post_edited_translations.segment}

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Certificados**.
2. En la pestaña **Global**, selecciona **S3 API certificate**.
3. Selecciona la pestaña **Servidor** o **Paquete de CA** y luego descarga o copia el certificado.

${post_edited_translations.segment}

Descarga el certificado o el paquete de CA `.pem`. Si utilizas un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Selecciona **Descargar certificado** o **Descargar paquete de CA**.

   Si estás descargando un paquete de CA, todos los certificados de las pestañas secundarias del paquete de CA se descargan en un único archivo.

b. Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado o paquete PEM de CA

Copia el texto del certificado para pegarlo en otro lugar. Si utilizas un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. ${post_edited_translations.segment}

   Si estás copiando un paquete de CA, todos los certificados de las pestañas secundarias del paquete de CA se copian juntos.

b. ${post_edited_translations.segment}

c. Guarda el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Información relacionada

- "Usa la API de REST de S3"
- "${post_edited_translations.segment}"

Copia el certificado StorageGRID Grid CA

StorageGRID utiliza una autoridad de certificación (CA) interna para proteger el tráfico interno. Este certificado no cambia aunque subas tus propios certificados.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "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 utilizando el certificado de servidor personalizado. No deben copiar el certificado de la CA del sistema StorageGRID.

Pasos

1. ${post_edited_translations.segment}

2. En la sección **Certificado PEM**, descarga o copia el certificado.

${post_edited_translations.segment}

Descarga el archivo de certificado `.pem`.

a. Selecciona **Descargar certificado**.

b. Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

${post_edited_translations.segment}

Copia el texto del certificado para pegarlo en otro sitio.

a. ${post_edited_translations.segment}

b. ${post_edited_translations.segment}

c. Guarda el archivo de texto con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

Configura los certificados de StorageGRID para FabricPool

Para los clientes S3 que realizan una validación estricta de nombres de host y no admiten desactivarla, como los clientes ONTAP que usan FabricPool, puedes generar o cargar un certificado de servidor al configurar el endpoint del equilibrador de carga.

Antes de empezar

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

Acerca de esta tarea

Cuando creas un endpoint de equilibrador de carga, puedes generar un certificado de servidor autofirmado o subir un certificado firmado por una autoridad de certificación (CA) conocida. En entornos de producción, deberías usar un certificado firmado por una CA conocida. Los certificados firmados por una CA se pueden rotar sin interrupciones. También son más seguros porque ofrecen una mejor protección contra ataques de tipo man-in-the-middle.

Los siguientes pasos ofrecen directrices generales para los clientes de S3 que utilizan FabricPool. Para obtener información y procedimientos más detallados, consulta "Configura StorageGRID para FabricPool".

Pasos

1. Si lo deseas, configura un grupo de alta disponibilidad (HA) para que lo use FabricPool.
2. Crea un punto de conexión del equilibrador de carga de S3 para que lo use FabricPool.

   Al crear un punto final de equilibrador de carga HTTPS, se te pedirá que subas tu certificado de servidor, la clave privada del certificado y, opcionalmente, el paquete de la autoridad de certificación (CA bundle).

3. ${post_edited_translations.segment}

   Especifica el puerto del extremo del balanceador de carga y el nombre de dominio completo utilizado en el certificado de CA que cargaste. A continuación, proporciona el certificado de CA.

   > Si una CA intermedia emitió el certificado de StorageGRID, debes proporcionar el certificado de la CA intermedia. Si la CA raíz emitió directamente el certificado de StorageGRID, debes proporcionar el certificado de la CA raíz.

Configura certificados de cliente en StorageGRID

Los certificados de cliente permiten a los clientes externos autorizados acceder a la base de datos de StorageGRID Prometheus, lo que ofrece una forma segura para que las herramientas externas supervisen StorageGRID.

Si necesitas acceder a StorageGRID usando una herramienta de monitoreo externa, debes cargar o generar un certificado de cliente usando Grid Manager y copiar la información del certificado en la herramienta externa.

Consulta "Gestiona certificados de seguridad" y "Configura certificados de servidor personalizados".

> Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor caducado, se activa la alerta **Caducidad de los certificados de cliente configurados en la página Certificados** cuando este certificado de servidor está a punto de caducar. Según sea necesario, puedes ver cuándo caduca el certificado actual seleccionando **Configuración** > **Seguridad** > **Certificados** y consultando la fecha de caducidad del certificado de cliente en la pestaña Cliente.

> Si utilizas un servidor de gestión de claves (KMS) para proteger los datos en nodos de dispositivos configurados de forma especial, consulta la información específica sobre "subir un certificado de cliente KMS".

Antes de empezar

- Tienes permiso de acceso root.
- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Para configurar un certificado de cliente:
  - Tienes la dirección IP o el nombre de dominio del Admin Node.
  - Si has configurado el certificado de la interfaz de gestión de StorageGRID, tienes la CA, el certificado de cliente y la clave privada que se usaron para configurar el certificado de la interfaz de gestión.
  - Para cargar tu propio certificado, la clave privada del certificado está disponible en tu ordenador local.
  - La clave privada debe haberse guardado o anotado en el momento de su creación. Si no tienes la clave privada original, debes crear una nueva.
- Para editar un certificado de cliente:
  - Tienes la dirección IP o el nombre de dominio del Admin Node.
  - Para cargar tu propio certificado o un certificado nuevo, la clave privada, el certificado de cliente y la CA (si se utiliza) están disponibles en tu ordenador local.

Agregar certificados de cliente

Para añadir el certificado de cliente, sigue uno de estos procedimientos:

- El certificado de la interfaz de gestión ya está configurado
- Certificado de cliente emitido por una CA
- Certificado generado desde Grid Manager

El certificado de la interfaz de gestión ya está configurado

Sigue este procedimiento para añadir un certificado de cliente si ya se ha configurado un certificado de interfaz de gestión utilizando una CA, un certificado de cliente y una clave privada proporcionados por el cliente.

Pasos

1. En el Grid Manager, selecciona **Configuración** > **Seguridad** > **Certificados** y luego selecciona la pestaña **Cliente**.
2. Selecciona **Add**.
3. Introduce un nombre para el certificado.
4. Para acceder a las métricas de Prometheus mediante tu herramienta de monitorización externa, selecciona **Allow prometheus**.
5. Selecciona **Continuar**.
6. En el paso **Adjuntar certificados**, sube el certificado de la interfaz de gestión.
   a. Selecciona **Cargar certificado**.
   b. Selecciona **Examinar** y elige el archivo del certificado de la interfaz de gestión (`.pem`).
      - Selecciona **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el certificado PEM.
      - Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
   c. Selecciona **Crear** para guardar el certificado en Grid Manager.

      El nuevo certificado aparece en la pestaña Cliente.
7. Configura una herramienta de supervisión externa, como Grafana.

Certificado de cliente emitido por una CA

Sigue este procedimiento para añadir un certificado de cliente de administrador si no se ha configurado ningún certificado de interfaz de gestión y tienes previsto añadir un certificado de cliente para Prometheus que utilice un certificado de cliente y una clave privada emitidos por una autoridad de certificación (CA).

Pasos

1. Sigue los pasos para "configurar un certificado de la interfaz de gestión".
2. En el Grid Manager, selecciona **Configuración** > **Seguridad** > **Certificados** y luego selecciona la pestaña **Cliente**.
3. Selecciona **Add**.
4. Introduce un nombre para el certificado.

5. Para acceder a las métricas de Prometheus mediante tu herramienta de monitorización externa, selecciona **Allow prometheus**.
6. Selecciona **Continuar**.
7. ${post_edited_translations.segment}
   a. Selecciona **Cargar certificado**.
   b. Selecciona **Examinar** y elige los archivos del certificado de cliente, la clave privada y el paquete de CA (`.pem`).
      - Selecciona **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el certificado PEM.
      - Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
   c. Selecciona **Crear** para guardar el certificado en Grid Manager.

      ${post_edited_translations.segment}
8. Configura una herramienta de supervisión externa, como Grafana.

Certificado generado desde Grid Manager

Sigue este procedimiento para añadir un certificado de cliente de administrador si no se ha configurado ningún certificado de interfaz de gestión y tienes previsto añadir un certificado de cliente para Prometheus que utiliza la función de generar certificados en Grid Manager.

Pasos

1. En el Grid Manager, selecciona **Configuración** > **Seguridad** > **Certificados** y luego selecciona la pestaña **Cliente**.
2. Selecciona **Add**.
3. Introduce un nombre para el certificado.
4. Para acceder a las métricas de Prometheus mediante tu herramienta de monitorización externa, selecciona **Allow prometheus**.
5. Selecciona **Continuar**.
6. ${post_edited_translations.segment}
7. ${post_edited_translations.segment}

   - **Sujeto** (opcional): sujeto X.509 o nombre distintivo (DN) del titular del certificado.
   - **Días de validez**: el número de días durante los que el certificado generado es válido, a partir del momento en que se genera.
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

     Deja esta casilla marcada a menos que tengas problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.
8. Selecciona **Generar**.
9. Selecciona **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el

certificado PEM.

> No podrás ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copia o descarga la clave en una ubicación segura.

- Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
- ${post_edited_translations.segment}

  Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

  Indica el nombre del archivo de la clave privada y la ubicación de descarga.

10. Selecciona **Crear** para guardar el certificado en Grid Manager.

    El nuevo certificado aparece en la pestaña Cliente.

11. ${post_edited_translations.segment}
12. ${post_edited_translations.segment}
13. Selecciona **Usar certificado personalizado**.
14. Sube los archivos certificate.pem y private_key.pem del paso ${post_edited_translations.segment}. No es necesario subir el paquete de CA.
    a. Selecciona **Cargar certificado** y luego selecciona **Continuar**.
    b. Sube cada archivo de certificado (`.pem`).
    c. ${post_edited_translations.segment}

       El nuevo certificado aparece en la página de certificados de la interfaz de administración.
15. Configura una herramienta de supervisión externa, como Grafana.

${post_edited_translations.segment}

Pasos

1. Configura los siguientes ajustes en tu herramienta de monitorización externa, como Grafana.
   a. **Nombre**: Introduce un nombre para la conexión.

      StorageGRID no requiere esta información, pero debes introducir un nombre para comprobar la conexión.

   b. **URL**: introduce el nombre de dominio o la dirección IP del nodo de administración. Especifica HTTPS y el puerto 9091.

      Por ejemplo: `https://admin-node.example.com:9091`

   c. Activa **Autenticación de cliente TLS** y **Con certificado de CA**.

d. En «Detalles de autenticación TLS/SSL», copia y pega:
   - ${post_edited_translations.segment}
   - El certificado de cliente en **Client Cert**
   - La clave privada de **Client Key**
e. **ServerName**: introduce el nombre de dominio del nodo de administración.

   ServerName debe coincidir con el nombre de dominio tal como aparece en el certificado de la interfaz de gestión.

2. ${post_edited_translations.segment}

   Ahora puedes acceder a las métricas de Prometheus desde StorageGRID con tu herramienta de monitorización externa.

   Para obtener información sobre las métricas, consulta "Instrucciones para monitorear StorageGRID".

Editar certificados de cliente

Puedes editar el certificado de cliente de un administrador para cambiar su nombre, habilitar o deshabilitar el acceso a Prometheus, o subir un nuevo certificado cuando el actual haya caducado.

Pasos

1. ${post_edited_translations.segment}

   En la tabla se indican las fechas de caducidad de los certificados y los permisos de acceso a Prometheus. Si un certificado está a punto de caducar o ya ha caducado, aparece un mensaje en la tabla y se activa una alerta.

2. Selecciona el certificado que deseas editar.
3. Selecciona **Editar** y luego selecciona **Editar nombre y permisos**
4. Introduce un nombre para el certificado.
5. Para acceder a las métricas de Prometheus mediante tu herramienta de monitorización externa, selecciona **Allow prometheus**.
6. Selecciona **Continuar** para guardar el certificado en Grid Manager.

   El certificado actualizado aparece en la pestaña Cliente.

Adjuntar nuevo certificado de cliente

${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}

   En la tabla se indican las fechas de caducidad de los certificados y los permisos de acceso a Prometheus. Si un certificado está a punto de caducar o ya ha caducado, aparece un mensaje en la tabla y se activa una alerta.

2. Selecciona el certificado que deseas editar.

3. ${post_edited_translations.segment}

Subir certificado

Copia el texto del certificado para pegarlo en otro sitio.

a. Selecciona **Cargar certificado** y luego selecciona **Continuar**.

b. Sube el nombre del certificado de cliente (`.pem`).

   Selecciona **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el certificado PEM.

   - ${post_edited_translations.segment}

     Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

c. Selecciona **Crear** para guardar el certificado en Grid Manager.

   El certificado actualizado aparece en la pestaña Cliente.

Generar certificado

Genera el texto del certificado para pegarlo en otro sitio.

a. Selecciona **Generar certificado**.

b. ${post_edited_translations.segment}

   - **Sujeto** (opcional): sujeto X.509 o nombre distintivo (DN) del titular del certificado.
   - **Días de validez**: el número de días durante los que el certificado generado es válido, a partir del momento en que se genera.
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

     Deja esta casilla marcada a menos que tengas problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

c. Selecciona **Generar**.

d. Selecciona **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el certificado PEM.

   No podrás ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copia o descarga la clave en una ubicación segura.

   - Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
   - ${post_edited_translations.segment}

Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Indica el nombre del archivo de la clave privada y la ubicación de descarga.

e. Selecciona **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la pestaña Cliente.

${post_edited_translations.segment}

${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Descarga o copia el certificado.

${post_edited_translations.segment}

Descarga el archivo de certificado `.pem`.

a. Selecciona **Descargar certificado**.

b. Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

${post_edited_translations.segment}

Copia el texto del certificado para pegarlo en otro sitio.

a. ${post_edited_translations.segment}

b. ${post_edited_translations.segment}

c. Guarda el archivo de texto con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

Eliminar certificados de cliente

${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}
2. Selecciona el certificado que deseas eliminar.
3. Selecciona **Eliminar** y luego confirma.

> ${post_edited_translations.segment}

Después de que se elimina un certificado, los clientes que usaban ese certificado deben especificar un nuevo certificado de cliente para acceder a la base de datos de StorageGRID Prometheus.

Configura los ajustes de seguridad

Administra la política TLS y SSH en StorageGRID

${post_edited_translations.segment}

La política de seguridad controla cómo TLS y SSH cifran los datos en tránsito. En general, utiliza la política «Compatibilidad moderna» (predeterminada), a menos que tu sistema deba cumplir con Common Criteria o que necesites usar otros cifrados.

> Algunos servicios de StorageGRID no se han actualizado para usar los cifrados en estas políticas.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".

Selecciona una política de seguridad

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Ajustes de seguridad**.

   La pestaña **Políticas de TLS y SSH** muestra las políticas disponibles. La política activa actualmente se identifica con una marca de verificación verde en el mosaico de la política.

2. ${post_edited_translations.segment}

Compatibilidad moderna (predeterminada)

Usa la política predeterminada si necesitas un cifrado robusto y no tienes requisitos especiales. Esta política es compatible con la mayoría de los clientes TLS y SSH.

Compatibilidad con versiones anteriores

Utiliza la política de compatibilidad Legacy si necesitas opciones de compatibilidad adicionales para clientes más antiguos. Las opciones adicionales de esta política pueden hacer que sea menos segura que la política de compatibilidad Modern.

Criterios Comunes

Utiliza la política de Common Criteria si necesitas la certificación de Common Criteria.

FIPS estricto

Usa la política estricta de FIPS si necesitas la certificación Common Criteria y tienes que usar el módulo NetApp Cryptographic Security Module (NCSM) 3.0.8 o el módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 para las conexiones de clientes externos con los endpoints del equilibrador de carga, Tenant Manager y Grid Manager. El uso de esta política podría reducir el rendimiento.

El módulo NCSM 3.0.8 y el módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 se usan en las siguientes operaciones:

- NCSM
  - ${post_edited_translations.segment}
  - Conexiones TLS entre los clientes y el servicio nginx-gw (puntos finales del equilibrador de carga)
  - Conexiones TLS entre los clientes y el servicio LDR
  - Cifrado del contenido de objetos para SSE-S3, SSE-C y la configuración de cifrado de objetos almacenados
  - Conexiones SSH

  Para obtener más información, consulta el NIST Cryptographic Algorithm Validation Program "Certificado n.º 4838".

- NetApp Módulo Kernel Crypto API de StorageGRID

  El módulo NetApp StorageGRID Kernel Crypto API solo está presente en plataformas de máquinas virtuales (VM) y dispositivos StorageGRID.

  - Recolección de entropía
  - ${post_edited_translations.segment}

  Para obtener más información, consulta el Programa de Validación de Algoritmos Criptográficos de NIST "${post_edited_translations.segment}" y "${post_edited_translations.segment}".

Nota: Después de seleccionar esta política, "realizar un reinicio progresivo" en todos los nodos para activar el NCSM. Usa **Mantenimiento** > **Reinicio progresivo** para iniciar y monitorear los reinicios.

Personalizado

Crea una política personalizada si necesitas aplicar tus propios cifrados.

Opcionalmente, si tu StorageGRID tiene requisitos de criptografía FIPS 140, activa la función de modo FIPS para usar el módulo NCSM 3.0.8 y el módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64:

a. Establece el parámetro `fipsMode` en `true`.

b. Cuando se te solicite, "realizar un reinicio progresivo" en todos los nodos para activar los módulos de criptografía. Usa **Mantenimiento** > **Reinicio progresivo** para iniciar y supervisar los reinicios.

c. Selecciona **Soporte** > **Diagnóstico** para ver las versiones activas de los módulos FIPS.

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}

   Aparece una marca de verificación verde junto a **Current policy** en el mosaico de la política.

Crear una política de seguridad personalizada

Puedes crear una política personalizada si necesitas aplicar tus propios cifrados.

Pasos

1. En la ficha de la política que más se parezca a la política personalizada que quieres crear, selecciona **Ver detalles**.
2. ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. Pega el JSON que copiaste y haz los cambios que sean necesarios.
5. Selecciona **Usar política**.

   ${post_edited_translations.segment}

6. Si lo deseas, selecciona **Editar configuración** para realizar más cambios en la nueva política personalizada.

Volver temporalmente a la política de seguridad predeterminada

Si has configurado una política de seguridad personalizada, puede que no puedas iniciar sesión en Grid Manager si la política TLS configurada es incompatible con "certificado de servidor configurado".

Puedes volver temporalmente a la política de seguridad predeterminada.

Pasos

1. Inicia sesión en un nodo de administración:
   a. Introduce el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
   c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
   d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

   Cuando inicias sesión como root, el indicador cambia de `$` a `#`.
2. Ejecuta el siguiente comando:

   ```
   restore-default-cipher-configurations
   ```
3. Desde un navegador web, accede al Grid Manager en el mismo nodo de administración.
4. Sigue los pasos de Selecciona una política de seguridad para volver a configurar la política.

Configura la red StorageGRID y la seguridad de objetos

Puedes configurar la seguridad de la red y de los objetos para cifrar los objetos almacenados, impedir determinadas solicitudes S3 o permitir que las conexiones de los clientes a los Storage Nodes utilicen HTTP en lugar de HTTPS.

Cifrado de objetos almacenados

El cifrado de objetos almacenados permite cifrar todos los datos de los objetos a medida que se importan a través de S3. De forma predeterminada, los objetos almacenados no están cifrados, pero puedes optar por cifrarlos utilizando el algoritmo de cifrado AES-128 o AES-256. Al habilitar esta configuración, todos los objetos recién importados se cifran, pero no se produce ningún cambio en los objetos ya almacenados. Si deshabilitas el cifrado, los objetos que ya están cifrados permanecen así, pero los objetos recién importados no se cifran.

La configuración de cifrado de objetos almacenados solo se aplica a los objetos de S3 que no hayan sido cifrados mediante el cifrado a nivel de bucket o a nivel de objeto.

Para obtener más información sobre los métodos de cifrado de StorageGRID, consulta "Revisa los métodos de cifrado de StorageGRID".

Impedir que el cliente realice modificaciones

Impedir la modificación por parte del cliente es una configuración válida para todo el sistema. Cuando se selecciona la opción **Impedir la modificación por parte del cliente**, se rechazan las siguientes solicitudes.

API de REST de S3

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

Habilita HTTP para las conexiones del nodo de almacenamiento

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para cualquier conexión directa con los nodos de almacenamiento. Si lo deseas, puedes habilitar HTTP para estas conexiones, por ejemplo, al realizar pruebas en una red que no sea de producción.

Utiliza HTTP para las conexiones con los nodos de almacenamiento únicamente si los clientes S3 necesitan establecer conexiones HTTP directamente con los nodos de almacenamiento. No necesitas usar esta opción para los clientes que solo usan conexiones HTTPS o para los clientes que se conectan al servicio de Load Balancer (porque puedes "${post_edited_translations.segment}" usar tanto HTTP como HTTPS).

Consulta "${post_edited_translations.segment}" para saber qué puertos usan los clientes S3 al conectarse a los nodos de almacenamiento mediante HTTP o HTTPS.

Selecciona opciones

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes permiso de acceso root.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Ajustes de seguridad**.
2. Selecciona la pestaña **Red y objetos**.
3. ${post_edited_translations.segment}
4. Si lo deseas, selecciona **Impedir la modificación por parte del cliente** si quieres evitar que los clientes de S3 realicen solicitudes específicas.

   > Si modificas esta configuración, la nueva configuración tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para mejorar el rendimiento y la escalabilidad.

5. Opcionalmente, selecciona **Habilitar HTTP para las conexiones a los nodos de almacenamiento** si los clientes se conectan directamente a los nodos de almacenamiento y quieres usar conexiones HTTP.

   > Ten cuidado al habilitar HTTP en una red de producción porque las solicitudes se enviarán sin cifrar.

6. Selecciona **Guardar**.

Cambiar la configuración de seguridad de la interfaz StorageGRID

${post_edited_translations.segment}

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".

- Tienes "Permiso de acceso raíz".

Acerca de esta tarea

La página **Configuración de seguridad** incluye los parámetros **Tiempo de espera por inactividad del navegador** y **Rastreo de pila de la Management API**.

Tiempo de espera por inactividad del navegador

Indica cuánto tiempo puede estar inactivo el navegador de un usuario antes de que se cierre su sesión. El valor predeterminado es de 15 minutos.

El tiempo de espera por inactividad del navegador también se controla mediante lo siguiente:

- Un temporizador independiente de StorageGRID, no configurable, que se incluye por motivos de 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 desconecta automáticamente, incluso si el tiempo de espera por inactividad del navegador está desactivado o no se ha alcanzado el valor para el tiempo de espera del navegador. Para renovar el token, el usuario debe volver a iniciar sesión.
- Configuración del tiempo de espera para el proveedor de identidad, suponiendo que el inicio de sesión único (SSO) esté habilitado para StorageGRID.

  Si el SSO está habilitado y se agota el tiempo de espera del navegador de un usuario, el usuario debe volver a introducir sus credenciales de SSO para acceder de nuevo a StorageGRID. Consulta "Cómo funciona el SSO".

Traza de la pila de la Management API

Controla si se devuelve un seguimiento de la pila en las respuestas de error de la API de Grid Manager y Tenant Manager.

Esta opción está desactivada por defecto, pero es posible que quieras activar esta funcionalidad en un entorno de prueba. En general, deberías dejar desactivado el seguimiento de la pila en los entornos de producción para evitar revelar detalles internos del software cuando ocurren errores en la API.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Ajustes de seguridad**.
2. Selecciona la pestaña **Interfaz**.
3. Para cambiar la configuración del tiempo de espera de inactividad del navegador:
   a. Despliega el acordeón.
   b. Para cambiar el tiempo de espera, especifica un valor comprendido entre 60 segundos y 7 días. El tiempo de espera predeterminado es de 15 minutos.
   c. Para desactivar esta función, desmarca la casilla.
   d. Selecciona **Guardar**.

      La nueva configuración no afecta a los usuarios que ya hayan iniciado sesión. Los usuarios deben volver a iniciar sesión o actualizar su navegador para que la nueva configuración del tiempo de espera surta efecto.
4. Para cambiar la configuración del seguimiento de la pila de la Management API:
   a. Despliega el acordeón.

b. Marca la casilla de verificación para devolver un seguimiento de la pila en las respuestas de error de la API de Grid Manager y Tenant Manager.

> Mantén desactivada la traza de pila en los entornos de producción para evitar revelar detalles internos del software cuando ocurran errores en la API.

c. Selecciona **Guardar**.

Administra el acceso SSH externo en StorageGRID

Gestiona el acceso SSH para el tráfico entrante en el grid bloqueando o permitiendo el acceso externo. Gestionar el acceso externo por SSH no afecta al tráfico entre nodos en el grid.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "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 necesitas realizar tareas que requieran acceso SSH entrante, como la resolución de problemas, permite temporalmente el acceso externo. Cuando hayas terminado la tarea, bloquea el acceso externo.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Ajustes de seguridad**.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
   a. Marca la casilla para bloquear el acceso (predeterminado).
   b. Desmarca la casilla para permitir el acceso.

> Requiere acceso en el puerto 22 entre el portátil de servicio y todos los demás nodos de grid. Elimina el acceso en el puerto 22 cuando completes la tarea de mantenimiento.

4. Selecciona **Guardar**.

Configura servidores de gestión de claves

Conoce los servidores de gestión de claves en StorageGRID

${post_edited_translations.segment}

StorageGRID solo admite determinados servidores de gestión de claves. Para obtener una lista de los productos y versiones compatibles, usa la "Herramienta de matriz de interoperabilidad (IMT) de NetApp".

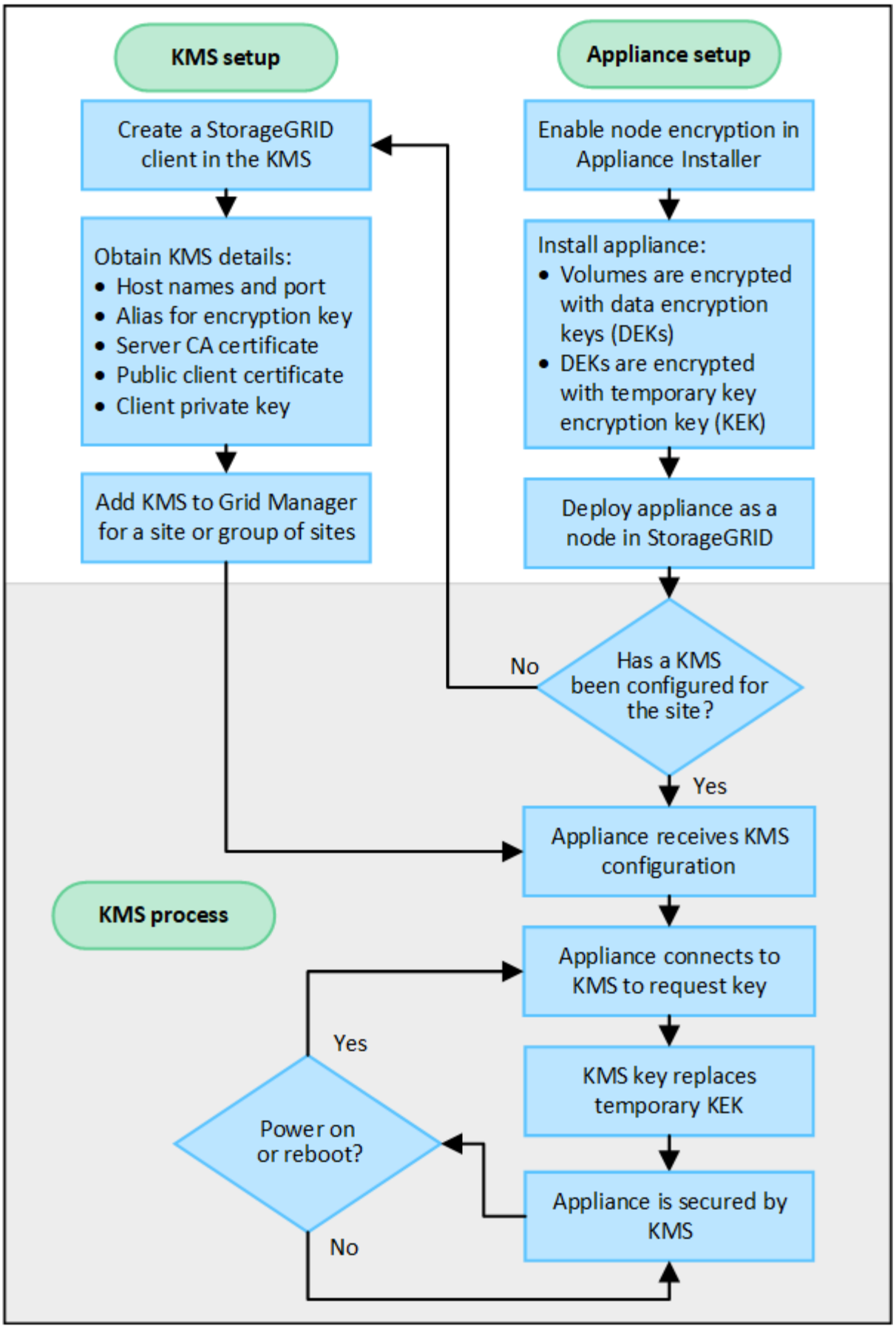
Puedes usar uno o varios servidores de gestión de claves para gestionar las claves de cifrado de los nodos de cualquier dispositivo StorageGRID que tenga habilitada la opción **Node Encryption** durante la instalación. Usar servidores de gestión de claves con estos nodos de dispositivo te permite proteger tus datos incluso si se retira un dispositivo del centro de datos. Después de que los volúmenes del dispositivo estén cifrados, no puedes acceder a ningún dato en el dispositivo a menos que el nodo pueda comunicarse con el KMS.

StorageGRID no crea ni gestiona las claves externas utilizadas para cifrar y descifrar los nodos del appliance. Si tienes pensado utilizar un servidor de gestión de claves externo para proteger los datos de StorageGRID, debes comprender cómo configurar ese servidor y cómo gestionar las claves de cifrado. Realizar las tareas de gestión de claves queda fuera del alcance de estas instrucciones. Si necesitas ayuda, consulta la documentación de tu servidor de gestión de claves o ponte en contacto con el soporte técnico.

Configuración del servidor de gestión de claves StorageGRID y de los dispositivos

Antes de que puedas usar un servidor de gestión de claves (KMS) para proteger los datos de StorageGRID en los nodos del dispositivo, debes completar dos tareas de configuración: configurar uno o más servidores KMS y habilitar el cifrado de los nodos del dispositivo. Cuando estas dos tareas de configuración estén completas, el proceso de gestión de claves ocurre automáticamente.

El diagrama de flujo muestra los pasos a grandes rasgos para usar un KMS y proteger los datos de StorageGRID en los nodos de los dispositivos.



${post_edited_translations.segment}

Configura el servidor de gestión de claves (KMS)

La configuración de un servidor de gestión de claves incluye los siguientes pasos a grandes rasgos.

Paso	Consulta
${post_edited_translations.segment}	"Configura StorageGRID como cliente en el KMS"
${post_edited_translations.segment}	"Configura StorageGRID como cliente en el KMS"
Agrega el KMS al Grid Manager, asígnalo a un solo sitio o a un grupo predeterminado de sitios, sube los certificados requeridos y guarda la configuración del KMS.	"Agrega un servidor de gestión de claves (KMS)"

Configura el appliance

${post_edited_translations.segment}

1. ${post_edited_translations.segment}

> No puedes activar la opción **Cifrado de nodos** después de añadir un appliance a la grid, y no puedes usar la gestión externa de claves para appliances que no tengan activado el cifrado de nodos.

2. Ejecuta el StorageGRID Appliance Installer. Durante la instalación, se asigna una clave de cifrado de datos (DEK) aleatoria a cada volumen del dispositivo, de la siguiente manera:
   - Las DEK se usan para cifrar los datos de cada volumen. Estas claves se generan mediante el cifrado de disco Linux Unified Key Setup (LUKS) en el SO del appliance y no se pueden cambiar.
   - Cada DEK individual se cifra mediante una clave maestra de cifrado (KEK). La KEK inicial es una clave temporal que cifra las DEK hasta que el dispositivo pueda conectarse al KMS.
3. Agrega el nodo del dispositivo a StorageGRID.

Consulta "Habilitar el cifrado de nodos" para más detalles.

${post_edited_translations.segment}

El cifrado con gestión de claves incluye los siguientes pasos a grandes rasgos que se llevan a cabo de forma automática.

1. Al instalar en la red un dispositivo que tiene activado el cifrado de nodos, StorageGRID comprueba si existe una configuración de KMS para el sitio que contiene el nuevo nodo.
   - Si ya se ha configurado un KMS para el sitio, el dispositivo recibe la configuración del KMS.
   - ${post_edited_translations.segment}
2. El dispositivo utiliza la configuración de 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 a la KEK temporal y ahora se utiliza para cifrar y descifrar las DEK de los volúmenes del dispositivo.

Cualquier dato que exista antes de que el nodo del dispositivo cifrado se conecte al KMS configurado se cifra con una clave temporal. Sin embargo, no debes considerar que los volúmenes del dispositivo estén protegidos frente a su retirada del centro de datos hasta que la clave de cifrado de KMS sustituya a la clave temporal.

4. Si el dispositivo se enciende o se reinicia, se vuelve a conectar al KMS para solicitar la clave. La clave, que se guarda en la memoria volátil, no sobrevive a una pérdida de alimentación o a un reinicio.

Requisitos y consideraciones del servidor de gestión de claves StorageGRID

Antes de configurar un servidor externo de gestión de claves (KMS), debes conocer las consideraciones y los requisitos.

${post_edited_translations.segment}

${post_edited_translations.segment}

"Especificación del Protocolo de Interoperabilidad para la Gestión de Claves versión 1.4"

¿Cuáles son las consideraciones de red?

La configuración del cortafuegos de red debe permitir que cada nodo del dispositivo se comunique a través del puerto utilizado para las comunicaciones del Protocolo de Interoperabilidad de Gestión de Claves (KMIP). El puerto KMIP predeterminado es 5696.

Debes asegurarte de que cada nodo de dispositivo que utilice el cifrado de nodos tenga acceso de red al KMS o al clúster de KMS que configuraste 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 KMS o clúster de KMS, según lo que admita el KMS y qué "Política de TLS y SSH" estés utilizando.

StorageGRID negocia el protocolo y el cifrado (TLS 1.2) o el conjunto de cifrados (TLS 1.3) con el KMS al establecer la conexión. Para ver qué versiones de protocolo y cifrados o conjuntos de cifrado están disponibles, revisa la sección `tlsOutbound` de la política activa de TLS y SSH del grid (**Configuration** > **Security Security settings**).

¿Qué dispositivos son compatibles?

Puedes utilizar un servidor de gestión de claves (KMS) para gestionar las claves de cifrado de cualquier dispositivo StorageGRID de tu grid que tenga activada la opción **Node Encryption**. Esta opción solo se puede activar durante la etapa de configuración del hardware de la instalación del dispositivo usando el StorageGRID Appliance Installer.

${post_edited_translations.segment}

Puedes utilizar el KMS configurado para los dispositivos StorageGRID y los nodos de los dispositivos.

${post_edited_translations.segment}

- Nodos implementados como máquinas virtuales (VM)

- ${post_edited_translations.segment}

Los nodos implementados en estas otras plataformas pueden usar el cifrado fuera de StorageGRID a nivel de almacén de datos o de disco.

¿Cuándo debo configurar los servidores de gestión de claves?

En una nueva instalación, lo habitual es configurar uno o varios servidores de gestión de claves en Grid Manager antes de crear inquilinos. Este orden garantiza que los nodos estén protegidos antes de que se almacene cualquier dato de objeto en ellos.

Puedes configurar los servidores de gestión de claves en Grid Manager antes o después de instalar los nodos del appliance.

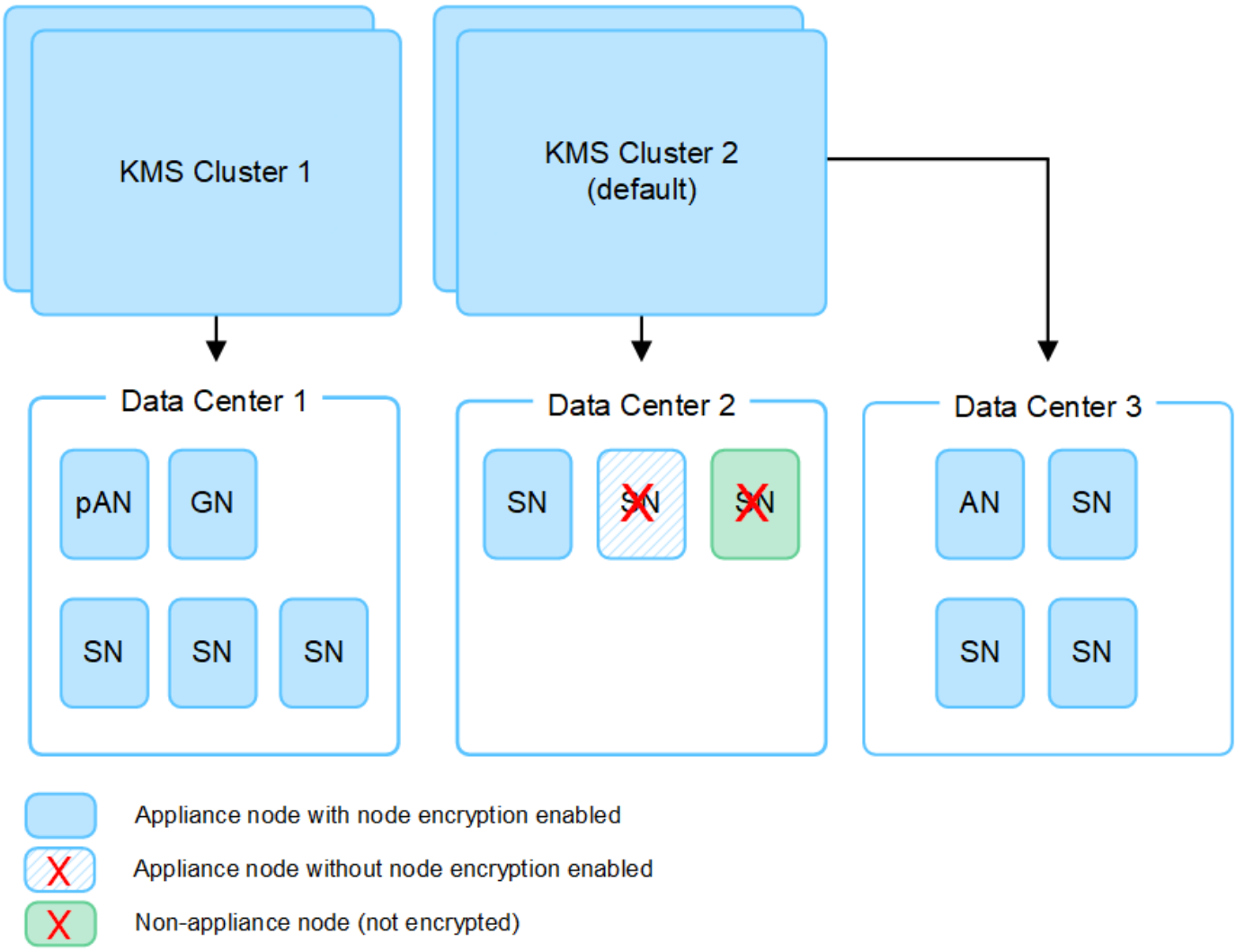
${post_edited_translations.segment}

Puedes configurar uno o varios servidores de gestión de claves externos para proporcionar claves de cifrado a los nodos de appliance en tu sistema StorageGRID. Cada KMS proporciona una única clave de cifrado a los nodos de appliance de StorageGRID en un solo sitio o en un grupo de sitios.

StorageGRID admite el uso de clústeres de KMS. Cada clúster de KMS contiene varios servidores de gestión de claves replicados que comparten los ajustes de configuración y las claves de cifrado. Se recomienda usar clústeres de KMS para la gestión de claves, ya que mejora las capacidades de conmutación por error de una configuración de alta disponibilidad.

Por ejemplo, supón que tu sistema StorageGRID tiene tres centros de datos. Podrías configurar un clúster KMS para proporcionar una clave a todos los nodos de los dispositivos en el Data Center 1 y un segundo clúster KMS para proporcionar una clave a todos los nodos de los dispositivos en los demás sitios. Cuando añades el segundo clúster KMS, puedes configurar un KMS predeterminado para Data Center 2 y Data Center 3.

Ten en cuenta que no puedes utilizar un KMS para nodos que no sean de appliance ni para ningún nodo de appliance que no tuviera activada la configuración **Cifrado de nodo** durante la instalación.



${post_edited_translations.segment}

Como práctica recomendada de seguridad, deberías "rotar la clave de cifrado" periódicamente que usa cada KMS configurado.

${post_edited_translations.segment}

- Se distribuye automáticamente a los nodos de los dispositivos cifrados en el sitio o sitios asociados con el KMS. La distribución debería ocurrir dentro de una hora desde que se rota la clave.
- ${post_edited_translations.segment}
- Si por cualquier motivo la nueva versión de la clave no se puede usar para cifrar los volúmenes del dispositivo, se activará la alerta **Error en la rotación de la clave de cifrado de KMS** para el nodo del dispositivo. Es posible que necesites ponerte en contacto con el soporte técnico para obtener ayuda para resolver esta alerta.

¿Puedo volver a utilizar un nodo de appliance después de que haya sido cifrado?

Si necesitas instalar un dispositivo cifrado en otro sistema StorageGRID, primero debes decomisionar el nodo de grid para mover los datos de objetos a otro nodo. Después, puedes usar el StorageGRID Appliance Installer para "borrar la configuración de KMS". Al borrar la configuración de KMS, se desactiva el ajuste **Node Encryption** y se elimina la asociación entre el nodo del dispositivo y la configuración de KMS para el sitio de

StorageGRID.

${post_edited_translations.segment}

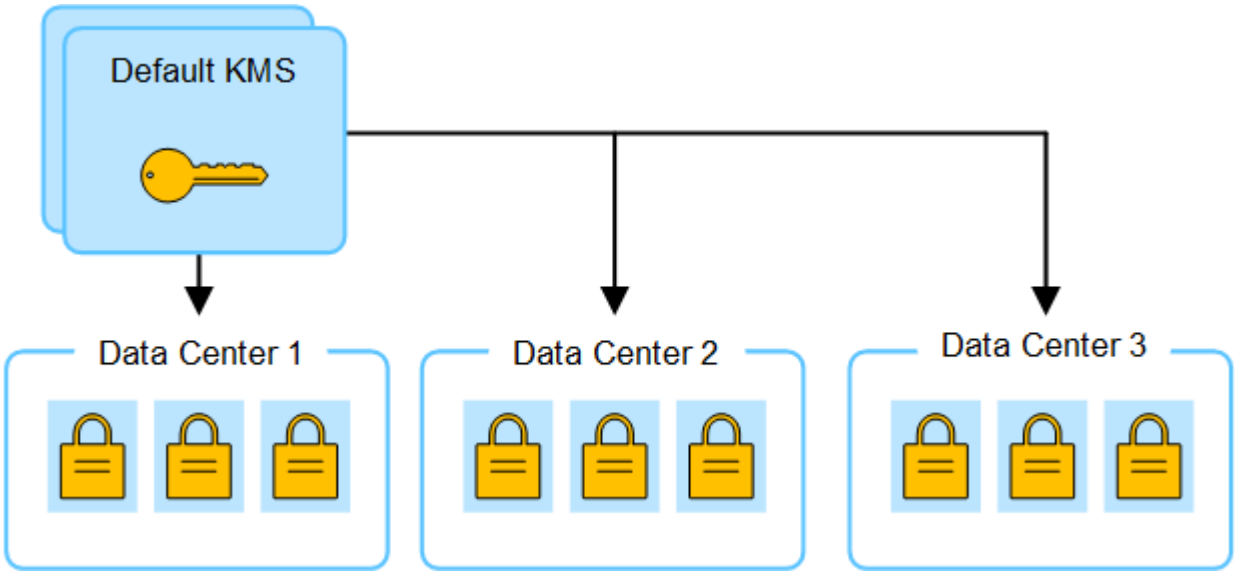
Consideraciones para cambiar el KMS de un sitio StorageGRID

Cada servidor de gestión de claves (KMS) o clúster de KMS proporciona una clave de cifrado a todos los nodos del appliance en una única sede o en un grupo de sedes. Si necesitas cambiar qué KMS se utiliza para una sede, es posible que tengas que copiar la clave de cifrado de un KMS a otro.

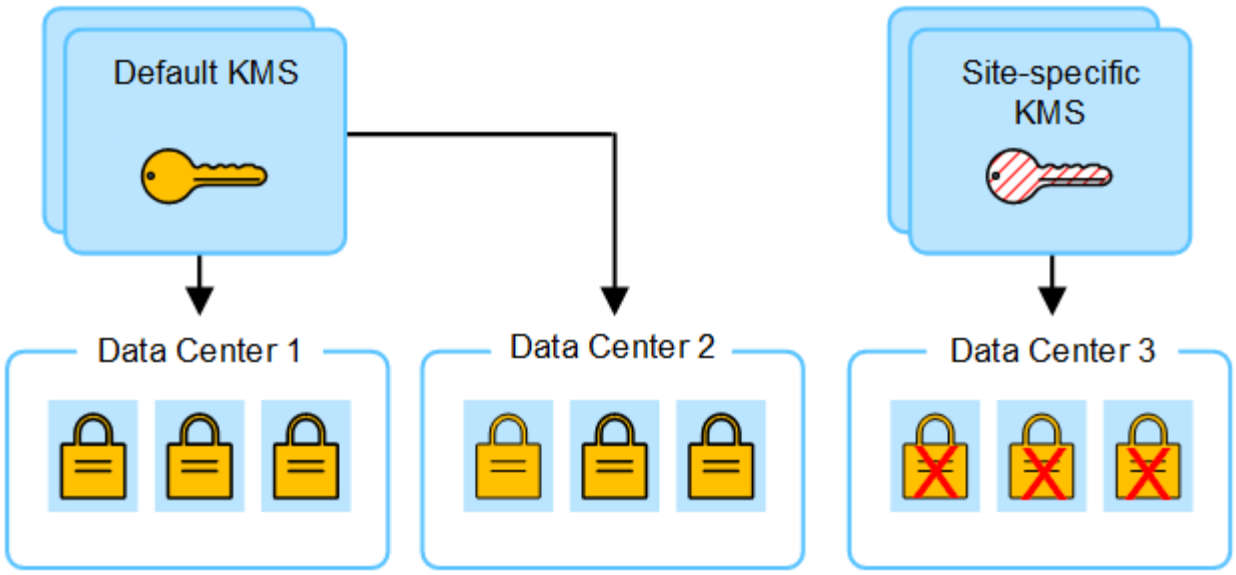
Si cambias el KMS utilizado para un sitio, debes asegurarte de que los nodos del dispositivo previamente cifrados en ese sitio puedan descifrarse usando la clave almacenada en el nuevo KMS. En algunos casos, podrías necesitar copiar la versión actual de la clave de cifrado del KMS original al nuevo KMS. Debes asegurarte de que el KMS tenga la clave correcta para descifrar los nodos del dispositivo cifrados en el sitio.

Por ejemplo:

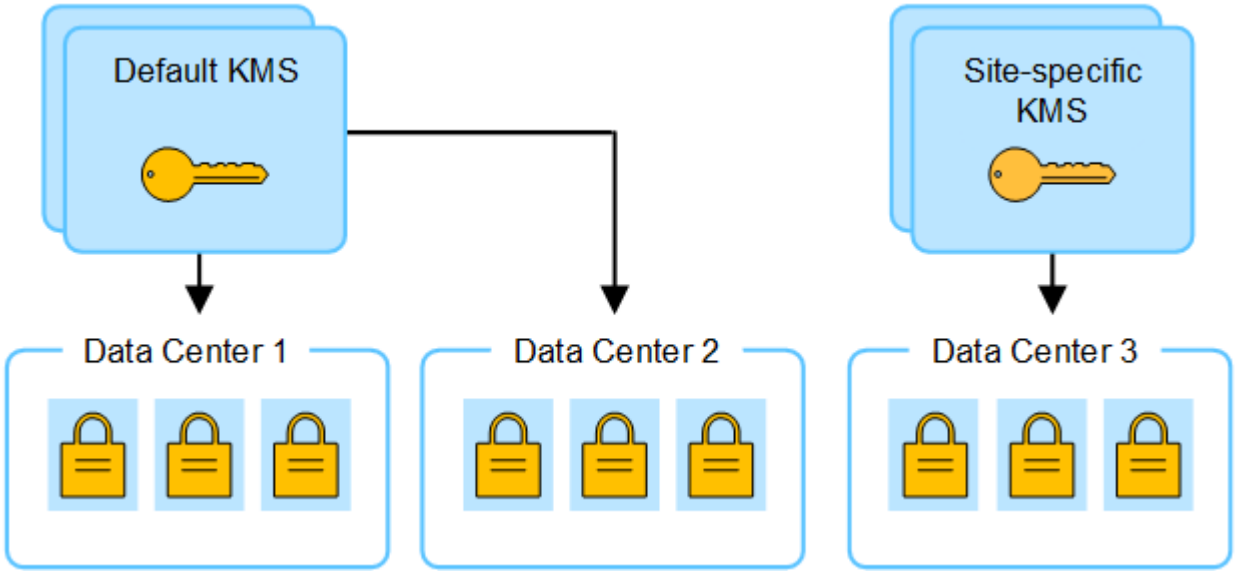
1. Inicialmente configuras un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos de appliance que tienen habilitada la configuración **Cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se utiliza para cifrar los nodos de appliance en todos los sitios. Esta misma clave también se debe utilizar para descifrar esos appliances.



3. Decides añadir un KMS específico para un sitio (el Data Center 3 de la figura). Sin embargo, porque los nodos del appliance ya están cifrados, ocurre un error de validación cuando intentas guardar la configuración para el KMS específico del sitio. El error ocurre porque el KMS específico del sitio no tiene la clave correcta para descifrar los nodos de ese sitio.



4. Para solucionar el problema, copias la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. (Técnicamente, copias la clave original a una nueva clave con el mismo alias. La clave original pasa a ser una versión anterior de la nueva clave.) El KMS específico del sitio ahora tiene la clave correcta para descifrar los nodos del dispositivo en Data Center 3, así que puede guardarse en StorageGRID.



${post_edited_translations.segment}

${post_edited_translations.segment}

Caso de uso para cambiar el KMS de un sitio	Pasos necesarios
${post_edited_translations.segment}	Edita el KMS específico del sitio. En el campo **Gestiona claves para**, selecciona **Sitios no gestionados por otro KMS (KMS predeterminado)**. El KMS específico del sitio se usará ahora como el KMS predeterminado. Se aplicará a cualquier sitio que no tenga un KMS dedicado. "Editar un servidor de gestión de claves (KMS)"
Tienes un KMS predeterminado y añades un nuevo sitio en una ampliación. No quieres utilizar el KMS predeterminado para el nuevo sitio.	1. Si los nodos de los dispositivos de la nueva ubicación ya han sido cifrados mediante el KMS predeterminado, utiliza el software del KMS para copiar la versión actual de la clave de cifrado del KMS predeterminado a un nuevo KMS. 2. Usando el Grid Manager, añade el nuevo KMS y selecciona el sitio. "Agrega un servidor de gestión de claves (KMS)"
Quieres que el KMS de un sitio use un servidor diferente.	1. Si los nodos de los dispositivos de la sede ya han sido cifrados por el KMS existente, utiliza el software del KMS para copiar la versión actual de la clave de cifrado del KMS existente al nuevo KMS. 2. Mediante el Grid Manager, edita la configuración actual de KMS e introduce el nuevo nombre de host o la nueva dirección IP. "Agrega un servidor de gestión de claves (KMS)"

Configura StorageGRID como cliente en el KMS

Debes configurar StorageGRID como cliente para cada servidor externo de gestión de claves o clúster KMS antes de poder añadir el KMS a StorageGRID.

Estas instrucciones se aplican a Thales CipherTrust Manager y Hashicorp Vault. Para ver la lista de productos y versiones compatibles, usa el "Herramienta de matriz de interoperabilidad (IMT) de NetApp".

Pasos

1. ${post_edited_translations.segment}

   Cada KMS gestiona una única clave de cifrado para los nodos de los dispositivos StorageGRID de un único sitio o de un grupo de sitios.

2. Crea una clave utilizando uno de los dos métodos siguientes:
   - Utiliza la página de gestión de claves de tu producto KMS. Crea una clave de cifrado AES para cada KMS o clúster de KMS.

     ${post_edited_translations.segment}

   - Haz que StorageGRID cree la clave. Se te pedirá cuando pruebes y guardes después de "carga de certificados de cliente".

3. ${post_edited_translations.segment}

   Necesitarás esta información cuando añadas el KMS a StorageGRID:

   - Nombre de host o dirección IP de cada servidor.
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

4. Para cada KMS o clúster de KMS, obtén un certificado de servidor firmado por una autoridad de certificación (CA) o un paquete de certificados que contenga cada uno de los archivos de certificados de CA codificados en formato PEM, concatenados en el orden de la cadena de certificados.

   El certificado del servidor permite que el KMS externo se autentique en StorageGRID.

   - El certificado debe usar el formato X.509 codificado en Base-64 Privacy Enhanced Mail (PEM).
   - El campo «Nombre alternativo del sujeto» (SAN) de cada certificado de servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP a la que StorageGRID se conectará.

     > Al configurar el KMS en StorageGRID, debes introducir los mismos FQDN o direcciones IP en el campo **Hostname**.

   - ${post_edited_translations.segment}

5. Obtén el certificado público de cliente emitido para StorageGRID por el KMS externo y la clave privada para el certificado de cliente.

   El certificado de cliente permite a StorageGRID autenticarse ante el KMS.

Agrega un servidor de gestión de claves en StorageGRID

Usas el asistente de StorageGRID Key Management Server para añadir cada KMS o clúster KMS.

Antes de empezar

- Has revisado la "Consideraciones y requisitos para usar un servidor de gestión de claves".
- Tienes "${post_edited_translations.segment}" y dispones de la información necesaria para cada KMS o clúster de KMS.
- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".

Acerca de esta tarea

Si es posible, configura cualquier servidor de gestión de claves específico de un sitio antes de configurar un KMS predeterminado que se aplique a todos los sitios no gestionados por otro KMS. Si creas primero el KMS predeterminado, todos los dispositivos cifrados por nodo de la grid se cifrarán mediante el KMS predeterminado. Si quieres crear un KMS específico de un sitio más adelante, primero debes copiar la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. Consulta "Aspectos a tener en cuenta al cambiar el KMS de un sitio" para más detalles.

${post_edited_translations.segment}

En el paso 1 (Datos del KMS) del asistente para añadir un servidor de gestión de claves, tú proporcionas los

datos del KMS o del clúster de KMS.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Servidor de gestión de claves**.

   Aparece la página del servidor de gestión de claves con la pestaña Detalles de configuración seleccionada.

2. Selecciona **Crear**.

   Aparece el paso 1 (detalles del KMS) del asistente Add a Key Management Server.

3. Introduce la siguiente información para el KMS y el cliente de StorageGRID que configuraste en ese KMS.

Campo	Descripción
Nombre de la KMS	Un nombre descriptivo que te ayude a identificar este KMS. Debe tener entre 1 y 64 caracteres.
${post_edited_translations.segment}	El alias exacto de la clave para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. **Nota**: Si aún no has creado una clave usando tu producto KMS, se te pedirá que StorageGRID cree la clave.
${post_edited_translations.segment}	El sitio de StorageGRID que se asociará a este KMS. Si es posible, deberías configurar cualquier servidor de gestión de claves específico del sitio antes de configurar un KMS predeterminado que se aplique a todos los sitios no gestionados por otro KMS. • Selecciona una sede si este KMS va a gestionar las claves de cifrado de los nodos del appliance en una sede concreta. • Selecciona **Sitios no gestionados por otro KMS (KMS predeterminado)** para configurar un KMS predeterminado que se aplicará a cualquier sitio que no tenga un KMS dedicado y a cualquier sitio que añadas en ampliaciones posteriores. ${post_edited_translations.segment}
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de Interoperabilidad de Gestión de Claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar de KMIP.
Nombre de host	El nombre de dominio completo o la dirección IP del KMS. **Nota:** El campo «Nombre alternativo del sujeto» (SAN) del certificado del servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP que introduzcas aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si estás configurando un clúster KMS, selecciona **Add another hostname** para añadir un nombre de host para cada servidor del clúster.

5. Selecciona **Continuar**.

Paso 2: Subir el certificado del servidor

En el paso 2 (Cargar certificado del servidor) del asistente Añadir un servidor de gestión de claves, subes el certificado del servidor (o el paquete de certificados) para el KMS. El certificado del servidor permite que el KMS externo se autentique ante StorageGRID.

Pasos

1. En el **Paso 2 (Cargar el certificado del servidor)**, busca la ubicación donde guardaste el certificado del servidor o el paquete de certificados.
2. Sube el archivo del certificado.

   Aparecen los metadatos del certificado del servidor.

   ${post_edited_translations.segment}

3. Selecciona **Continuar**.

${post_edited_translations.segment}

En el paso 3 (Subir certificados de cliente) del asistente Agregar un servidor de gestión de claves, subes el certificado de cliente y la clave privada del certificado de cliente. El certificado de cliente permite que StorageGRID se autentique ante el KMS.

Pasos

1. En el **Paso 3 (Cargar certificados de cliente)**, busca la ubicación del certificado de cliente.
2. Sube el archivo del certificado de cliente.

   Aparecen los metadatos del certificado de cliente.

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. Selecciona **Probar y guardar**.

   Si una clave no existe, se te pedirá que StorageGRID cree una.

   Se comprueban 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 nuevo servidor de gestión de claves se añade a la tabla en la página Key Management Server.

   Inmediatamente después de añadir un KMS, el estado del certificado en la página Key Management Server aparece como Unknown. StorageGRID puede tardar hasta 30 minutos en obtener el estado real de cada certificado. Debes actualizar tu navegador web para ver el estado actual.

6. Si aparece un mensaje de error al seleccionar **Probar y guardar**, revisa los detalles del mensaje y luego selecciona **OK**.

   Por ejemplo, es posible que recibas un error 422: entidad no procesable si falla una prueba de conexión.

7. Si necesitas guardar la configuración actual sin comprobar la conexión externa, selecciona **Force save**.

Al seleccionar **Force save**, se guarda la configuración del KMS, pero no se comprueba la conexión externa desde cada appliance a ese KMS. Si hay algún problema con la configuración, podrías no poder reiniciar los nodos de appliance que tengan habilitado el cifrado de nodos en el sitio afectado. Podrías perder el acceso a tus datos hasta que se resuelvan los problemas.

8. Revisa el mensaje de confirmación y selecciona **OK** si estás seguro de que quieres guardar la configuración de forma forzada.

   ${post_edited_translations.segment}

Administra un servidor de gestión de claves en StorageGRID

Gestionar un servidor de gestión de claves (KMS) implica ver o editar detalles, gestionar certificados, ver los nodos cifrados y eliminar un KMS cuando ya no lo necesites.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "permiso de acceso necesario".

Ver detalles de KMS

Puedes consultar información sobre cada servidor de gestión de claves (KMS) en tu sistema StorageGRID, incluidos los detalles de las claves y el estado actual de los certificados del servidor y del cliente.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Servidor de gestión de claves**.

   Aparece la página del servidor de gestión de claves y muestra la siguiente información:

   - La pestaña Detalles de configuración muestra cualquier servidor de gestión de claves que esté configurado.
   - La pestaña «Nodos cifrados» muestra cualquier nodo que tenga activado el cifrado de nodos.

2. Para ver los detalles de un KMS específico y realizar operaciones en él, selecciona el nombre del KMS. La página de detalles del KMS muestra la siguiente información:

Campo	Descripción
${post_edited_translations.segment}	${post_edited_translations.segment} Este campo muestra el nombre de un sitio específico de StorageGRID o **sitios no gestionados por otro KMS (KMS predeterminado)**.

Campo	Descripción
Nombre de host	El dominio completo o la dirección IP del KMS. Si hay un clúster de dos servidores de gestión de claves, se muestra 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, se muestra el nombre de dominio completo o la dirección IP del primer KMS, junto con el número de servidores de gestión de claves adicionales que hay 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, selecciona un KMS y selecciona **Editar** o **Acciones** > **Editar**.

3. Selecciona una pestaña en la página de detalles del KMS para ver la siguiente información:

Pestaña	Campo	Descripción
${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment}
UID clave	${post_edited_translations.segment}	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 PEM del certificado.	${post_edited_translations.segment}	${post_edited_translations.segment}
Certificado de cliente	Metadatos	Los metadatos del certificado, como el número de serie, la fecha y la hora de caducidad, y el PEM del certificado.

4. ${post_edited_translations.segment}

   Cuando la rotación de claves se realiza correctamente, se actualizan los campos Key UID y Last modified.

Si renuevas la clave de cifrado mediante el software KMS, hazlo pasando de la última versión utilizada de la clave a una nueva versión de la misma clave. No la renueves por una clave completamente diferente.

Nunca intentes rotar una clave cambiando el nombre de la clave (alias) en el KMS. StorageGRID requiere que todas las versiones de clave utilizadas anteriormente (así como las futuras) sean accesibles desde el KMS con el mismo alias de clave. Si cambias el alias de la clave de un KMS configurado, es posible que StorageGRID no pueda descifrar tus datos.

Gestiona certificados

Soluciona rápidamente cualquier problema con los certificados de servidor o de cliente. Si es posible, reemplaza los certificados antes de que caduquen.

Debes resolver cualquier problema relacionado con los certificados lo antes posible para mantener el acceso a los datos.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Servidor de gestión de claves**.
2. En la tabla, fíjate en el valor de caducidad del certificado de cada KMS.
3. Si la fecha de caducidad del certificado de cualquier KMS es Unknown, espera hasta 30 minutos y luego actualiza tu navegador web.
4. ${post_edited_translations.segment}
   a. Selecciona **Server certificate** y comprueba el valor del campo "Expires on".
   b. Para sustituir el certificado, selecciona **Editar certificado** para subir un certificado nuevo.
   c. Repite estos pasos secundarios y selecciona **Certificado de cliente** en lugar de **Certificado de servidor**.
5. Cuando se activen las alertas **Caducidad del certificado de la CA de KMS**, **Caducidad del certificado de cliente de KMS** y **Caducidad del certificado de servidor de KMS**, toma nota de la descripción de cada alerta y realiza las acciones recomendadas.

   StorageGRID puede tardar hasta 30 minutos en obtener las actualizaciones de la caducidad del certificado. Actualiza tu navegador web para ver los valores actuales.

Si aparece el mensaje «**El estado del certificado del servidor es desconocido**», asegúrate de que tu KMS permita obtener un certificado de servidor sin requerir un certificado de cliente.

${post_edited_translations.segment}

${post_edited_translations.segment}

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Servidor de gestión de claves**.

   Aparece la página «Servidor de gestión de claves». La pestaña «Detalles de configuración» muestra los servidores de gestión de claves que se hayan configurado.

2. En la parte superior de la página, selecciona la pestaña **Nodos cifrados**.

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

Columna	Descripción
Nombre de nodo	El nombre del nodo del dispositivo.
Tipo de nodo	${post_edited_translations.segment}
${post_edited_translations.segment}	El nombre del sitio de StorageGRID en el que está instalado el nodo.
Nombre de la KMS	El nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS en la lista, selecciona la pestaña Detalles de configuración para añadir un KMS. "Agrega un servidor de gestión de claves (KMS)"
UID clave	El ID único de la clave de cifrado que se utiliza para cifrar y descifrar datos en el nodo del dispositivo. Para ver el UID completo de una clave, selecciona el texto. Un guión (--) indica que se desconoce el UID de la clave, posiblemente porque hay un problema de conexión entre el nodo del appliance y el KMS.
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. Puede tardar varios minutos en actualizarse el estado de la conexión después de los cambios en la configuración del KMS. **Nota:** Actualiza tu navegador web para ver los nuevos valores.

4. Si en la columna Estado aparece un problema relacionado con el KMS, resuélvelo de inmediato.

   Durante el funcionamiento normal de KMS, el estado será **Conectado a KMS**. Si un nodo se desconecta de la grid, se muestra el estado de conexión del nodo (Administratively Down o Unknown).

   ${post_edited_translations.segment}

   - No se ha podido cargar la configuración de KMS
   - Error de conectividad con 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
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

Lleva a cabo las acciones recomendadas para estas alertas.

${post_edited_translations.segment}

${post_edited_translations.segment}

Es posible que tengas que modificar la configuración de un servidor de gestión de claves, por ejemplo, si un certificado está a punto de caducar.

Antes de empezar

- Si planeas actualizar el sitio seleccionado para un KMS, has revisado "Consideraciones para cambiar el KMS de un sitio".
- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Servidor de gestión de claves**.

   Aparece la página «Key management server» y muestra todos los key management servers que se han configurado.

2. Selecciona el KMS que quieras editar y selecciona **Acciones** > **Editar**.

   También puedes editar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Editar** en la página de detalles del KMS.

3. Opcionalmente, actualiza los detalles en **Step 1 (KMS details)** del asistente Edit a Key Management Server.

Campo	Descripción
Nombre de la KMS	Un nombre descriptivo que te ayude a identificar este KMS. Debe tener entre 1 y 64 caracteres.
${post_edited_translations.segment}	El alias exacto de la clave para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Solo necesitas modificar el nombre de la clave en casos excepcionales. Por ejemplo, debes modificar el nombre de la clave si se cambia el nombre del alias en el KMS o si todas las versiones de la clave anterior se han copiado al historial de versiones del nuevo alias.

Campo	Descripción
${post_edited_translations.segment}	Si estás editando un KMS específico de un sitio y aún no tienes un KMS predeterminado, puedes seleccionar opcionalmente **Sitios no gestionados por otro KMS (KMS predeterminado)**. Esta selección convierte un KMS específico de un sitio en el KMS predeterminado, que se aplicará a todos los sitios que no tengan un KMS dedicado y a cualquier sitio añadido en una expansión. **Nota:** Si estás editando un KMS específico de un sitio, no puedes seleccionar otro sitio. Si estás editando el KMS predeterminado, no puedes seleccionar un sitio específico.
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de Interoperabilidad de Gestión de Claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar de KMIP.
Nombre de host	El nombre de dominio completo o la dirección IP del KMS. **Nota:** El campo «Nombre alternativo del sujeto» (SAN) del certificado del servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP que introduzcas aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si estás configurando un clúster KMS, selecciona **Add another hostname** para añadir un nombre de host para cada servidor del clúster.
5. Selecciona **Continuar**.

   ${post_edited_translations.segment}

6. ${post_edited_translations.segment}
7. Selecciona **Continuar**.

   ${post_edited_translations.segment}

8. Si necesitas sustituir el certificado de cliente y la clave privada del certificado de cliente, selecciona **Examinar** y sube los nuevos archivos.
9. Selecciona **Probar y guardar**.

   Se prueban las conexiones entre el servidor de gestión de claves y todos los nodos de appliance con cifrado de nodos en los sitios afectados. Si todas las conexiones de los nodos son válidas y se encuentra la clave correcta en el KMS, el servidor de gestión de claves se añade a la tabla de la página Key Management Server.

10. Si aparece un mensaje de error, revisa los detalles del mensaje y selecciona **OK**.

    Por ejemplo, es posible que recibas un error 422: entidad no procesable si el sitio que has seleccionado para este KMS ya está gestionado por otro KMS, o si ha fallado una prueba de conexión.

11. Si necesitas guardar la configuración actual antes de solucionar los errores de conexión, selecciona **Force save**.

Al seleccionar **Force save**, se guarda la configuración del KMS, pero no se comprueba la conexión externa desde cada appliance a ese KMS. Si hay algún problema con la configuración, podrías no poder reiniciar los nodos de appliance que tengan habilitado el cifrado de nodos en el sitio afectado. Podrías perder el acceso a tus datos hasta que se resuelvan los problemas.

${post_edited_translations.segment}

12. Revisa el mensaje de confirmación y selecciona **OK** si estás seguro de que quieres guardar la configuración de forma forzada.

    La configuración del KMS se guarda, pero no se prueba la conexión con el KMS.

Eliminar un servidor de gestión de claves (KMS)

Es posible que, en algunos casos, desees eliminar un servidor de gestión de claves. Por ejemplo, es posible que desees eliminar un KMS específico de un sitio si has decomisionado dicho sitio.

Antes de empezar

- Has revisado la "Consideraciones y requisitos para usar un servidor de gestión de claves".
- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".

Acerca de esta tarea

Puedes eliminar un KMS en estos casos:

- Puedes eliminar un KMS específico de un sitio si dicho sitio ha sido decomisionado o si el sitio no incluye ningún nodo de dispositivo con el cifrado de nodos activado.
- ${post_edited_translations.segment}

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Servidor de gestión de claves**.

   Aparece la página «Key management server» y muestra todos los key management servers que se han configurado.

2. Selecciona el KMS que quieras eliminar y selecciona **Actions** > **Remove**.

   También puedes eliminar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Eliminar** en la página de detalles del KMS.

3. Confirma que lo siguiente es cierto:
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
4. Selecciona **Sí**.

   ${post_edited_translations.segment}

Gestiona la configuración del proxy

Configura un proxy de almacenamiento StorageGRID

Si estás utilizando servicios de plataforma o Cloud Storage Pools, puedes configurar un proxy no transparente entre los nodos de almacenamiento y los endpoints de S3 externos. Por ejemplo, es posible que necesites un proxy no transparente para permitir que los mensajes de los servicios de plataforma se envíen a endpoints externos, como un endpoint en internet.

${post_edited_translations.segment}

Antes de empezar

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

Acerca de esta tarea

${post_edited_translations.segment}

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Proxy settings**.
2. ${post_edited_translations.segment}
3. Selecciona el protocolo para el proxy de almacenamiento.
4. Introduce el nombre de host o la dirección IP del servidor proxy.
5. ${post_edited_translations.segment}

   Deja este campo en blanco para utilizar el puerto predeterminado del protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Selecciona **Guardar**.

   Después de guardar el proxy de almacenamiento, puedes configurar y probar nuevos endpoints para los servicios de plataforma o Cloud Storage Pools.

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

7. ${post_edited_translations.segment}
8. Si necesitas desactivar un proxy de almacenamiento, desmarca la casilla de selección y selecciona **Guardar**.

Configura los ajustes del proxy de administración en StorageGRID

Si envías paquetes AutoSupport usando HTTP o HTTPS, puedes configurar un proxy no transparente entre los nodos de administración y el soporte técnico (AutoSupport).

Para obtener más información sobre AutoSupport, consulta "Configura AutoSupport".

Antes de empezar

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

Acerca de esta tarea

Puedes configurar los ajustes de un único proxy de administrador.

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Proxy settings**.

   Aparece la página «Configuración del proxy». De forma predeterminada, la opción «Almacenamiento» está seleccionada en el menú de pestañas.

2. Selecciona la pestaña **Admin**.
3. Marca la casilla **Habilitar proxy de administrador**.
4. Introduce el nombre de host o la dirección IP del servidor proxy.
5. Introduce el puerto que se utiliza para conectarte al servidor proxy.
6. Si lo deseas, introduce un nombre de usuario y una contraseña para el servidor proxy.

   Deja estos campos en blanco si tu servidor proxy no requiere un nombre de usuario o una contraseña.

7. Selecciona una de las siguientes:

   - Si deseas proteger la conexión con el proxy de administración, selecciona **Verificar certificado del proxy**. Sube un paquete de CA para verificar la autenticidad de los certificados SSL presentados por el servidor proxy de administración.

     > AutoSupport on Demand, E-Series AutoSupport a través de StorageGRID y la determinación de la ruta de actualización en la página de actualización de StorageGRID no funcionarán si se verifica un certificado de proxy.

     Después de que subas el paquete de CA, aparecen sus metadatos.

   - Si no deseas validar los certificados al comunicarte con el servidor proxy de administración, selecciona **No verificar el certificado del proxy**.

8. Selecciona **Guardar**.

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

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

9. Si necesitas desactivar el proxy de administrador, desmarca la casilla **Habilitar proxy de administrador** y luego selecciona **Guardar**.

Controla los cortafuegos

Controla el acceso a StorageGRID en un firewall externo

Puedes abrir o cerrar puertos específicos en el firewall externo.

Puedes controlar el acceso a las interfaces de usuario y a las API en los Admin Nodes de StorageGRID abriendo o cerrando puertos específicos en el firewall externo. Por ejemplo, es posible que quieras evitar que los inquilinos puedan conectarse al Grid Manager en el firewall, además de utilizar otros métodos para controlar el acceso al sistema.

Si quieres configurar el firewall interno de StorageGRID, consulta "Configura el cortafuegos interno".

Puerto	Descripción	${post_edited_translations.segment}
443	${post_edited_translations.segment}	Los navegadores web y los clientes de la API de gestión pueden acceder al Grid Manager, a la Grid Management API, al Tenant Manager y a la Tenant Management API. **Nota:** El puerto 443 también se utiliza para parte del tráfico interno.
8443	Puerto restringido de Grid Manager en los nodos de administración	• Los navegadores web y los clientes de la API de gestión pueden acceder al Grid Manager y a la Grid Management API mediante HTTPS. • ${post_edited_translations.segment} • Se rechazarán las solicitudes de contenido interno.
9443	Puerto restringido de Tenant Manager en los nodos de administración	• Los navegadores web y los clientes de la API de gestión pueden acceder al Tenant Manager y a la Tenant Management API mediante HTTPS. • Los navegadores web y los clientes de la API de gestión no pueden acceder al Grid Manager ni a la Grid Management API. • Se rechazarán las solicitudes de contenido interno.

El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debes utilizar el puerto HTTPS predeterminado (443) si quieres que los usuarios se autentiquen con el inicio de sesión único.

Información relacionada

- "Inicia sesión en Grid Manager"
- "Crear cuenta de inquilino"
- "Comunicaciones externas"

Administra los controles internos de firewall en StorageGRID

StorageGRID incluye un cortafuegos interno en cada nodo que mejora la seguridad de tu grid al permitirte controlar el acceso de red al nodo. Usa el cortafuegos para evitar el acceso de red en todos los puertos excepto en los necesarios para tu implementación específica de grid. Los cambios de configuración que hagas en la página de control del

cortafuegos se aplican a cada nodo.

${post_edited_translations.segment}

- **Lista de direcciones con privilegios**: utiliza esta pestaña para permitir el acceso seleccionado a los puertos cerrados. Puedes añadir direcciones IP o subredes en notación CIDR que puedan acceder a los puertos cerrados mediante la pestaña Gestionar acceso externo.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

  La configuración de esta pestaña prevalece sobre la de la pestaña Gestionar acceso externo.

  - Un nodo con una red de clientes no fiable solo aceptará conexiones en los puertos de los puntos finales del equilibrador de carga configurados en dicho nodo (puntos finales globales, de interfaz de nodo y vinculados al tipo de nodo).
  - ${post_edited_translations.segment}
  - Cuando se consideran de confianza, se puede acceder a todos los puertos abiertos en la pestaña Gestionar acceso externo, así como a cualquier endpoint del equilibrador de carga abierto en la Client Network.

> La configuración que realices en una pestaña puede afectar a los cambios de acceso que realices en otra pestaña. Asegúrate de comprobar la configuración de todas las pestañas para garantizar que tu red funcione tal y como esperas.

Para configurar los controles del cortafuegos interno, consulta "Configura los controles del cortafuegos".

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulta "Controla el acceso en el cortafuegos externo".

${post_edited_translations.segment}

La pestaña Privileged address list te permite registrar una o más direcciones IP para permitirles el acceso a los puertos de la grid que están cerrados. La pestaña Manage external access te permite cerrar el acceso externo a los puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son aquellos a los que pueden acceder los nodos que no pertenecen a la grid de forma predeterminada). A menudo puedes utilizar estas dos pestañas juntas para personalizar el acceso exacto a la red que necesitas permitir para tu grid.

> ${post_edited_translations.segment}

Ejemplo 1: usa un servidor de enlace para tareas de mantenimiento

Supón que quieres usar un jump host (un host con seguridad reforzada) para la administración de la red. Podrías seguir estos pasos generales:

1. Utiliza la pestaña «Lista de direcciones privilegiadas» para añadir la dirección IP del jump host.
2. ${post_edited_translations.segment}

> Añade la dirección IP privilegiada antes de bloquear los puertos 443 y 8443. Cualquier usuario que esté conectado actualmente a un puerto bloqueado, incluido tú, perderá el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas.

Después de guardar tu configuración, todos los puertos externos del Admin Node de tu grid se bloquearán para todos los hosts, excepto para el jump host. Luego puedes usar el jump host para realizar tareas de mantenimiento en tu grid de forma más segura.

${post_edited_translations.segment}

Supongamos que quieres bloquear los puertos sensibles y el servicio en ese puerto. Podrías seguir estos pasos generales:

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

> Añade la dirección IP privilegiada antes de bloquear el acceso a cualquier puerto asignado para acceder a Grid Manager y Tenant Manager (los puertos preestablecidos son 443 y 8443). Cualquier usuario que esté conectado actualmente a un puerto bloqueado, incluido tú, perderá el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas.

Después de que guardes tu 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 negará el acceso al servicio sin importar desde qué interfaz provenga la solicitud.

Ejemplo 3: desactivar el acceso a los servicios que no se utilizan

A nivel de red, puedes desactivar algunos servicios que no tengas previsto utilizar. Por ejemplo, para bloquear el tráfico de clientes HTTP S3, usarías el interruptor de la pestaña Manage external access para bloquear el puerto 18084.

${post_edited_translations.segment}

Si utilizas una red de clientes, puedes ayudar a proteger StorageGRID de ataques hostiles aceptando el tráfico entrante de clientes solo en los endpoints configurados explícitamente.

De forma predeterminada, la red de clientes de cada nodo de grid es de *confianza*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de grid en todos los "puertos externos disponibles".

Puedes reducir la amenaza de ataques hostiles contra tu sistema StorageGRID especificando que la Client Network de cada nodo sea *untrusted*. Si la Client Network de un nodo es untrusted, el nodo solo acepta conexiones entrantes en los puertos configurados explícitamente como endpoints del load balancer. Consulta "Configura los puntos de conexión del equilibrador de carga" y "Configura los controles del cortafuegos".

Ejemplo 1: el nodo de puerta de enlace solo acepta solicitudes HTTPS S3

Supongamos que quieres que un nodo de puerta de enlace rechace todo el tráfico entrante en la red del cliente, excepto las solicitudes HTTPS S3. Para ello, deberías seguir estos pasos generales:

1. Desde la página "${post_edited_translations.segment}", configura un endpoint del equilibrador de carga para S3 sobre HTTPS en el puerto 443.
2. En la página de control del cortafuegos, selecciona No fiable para indicar que la Client Network en el Gateway Node no es fiable.

${post_edited_translations.segment}

${post_edited_translations.segment}

Supongamos que quieres habilitar el tráfico saliente de los servicios de la plataforma S3 desde un nodo de almacenamiento, pero quieres impedir cualquier conexión entrante a ese nodo de almacenamiento desde la red del cliente. Realizarías este paso general:

- ${post_edited_translations.segment}

${post_edited_translations.segment}

Ejemplo 3: limitar el acceso a Grid Manager a una subred

Supongamos que quieres permitir el acceso a Grid Manager únicamente en una subred concreta. Realiza los siguientes pasos:

1. Conecta la red de clientes de tus nodos de administración a la subred.
2. Utiliza la pestaña Untrusted Client Network para configurar la Client Network como no fiable.
3. Cuando creas un punto de conexión del equilibrador de carga de la interfaz de gestión, introduce el puerto y selecciona la interfaz de gestión a la que accederá el puerto.
4. ${post_edited_translations.segment}
5. Utiliza la pestaña «Gestionar acceso externo» para bloquear todos los puertos externos (con o sin direcciones IP privilegiadas configuradas para los hosts fuera de esa subred).

Una vez que guardes tu configuración, solo los hosts de la subred que especificaste podrán acceder al Grid Manager. Todos los demás hosts quedarán bloqueados.

Configura el firewall interno de StorageGRID

Puedes configurar el firewall de StorageGRID para controlar el acceso de red a puertos específicos en tus nodos de StorageGRID.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Has revisado la información en "Gestiona los controles del cortafuegos" y "${post_edited_translations.segment}".
- ${post_edited_translations.segment}

> ${post_edited_translations.segment}

Acerca de esta tarea

StorageGRID incluye un cortafuegos interno en cada nodo que te permite abrir o cerrar algunos de los puertos de los nodos de tu grid. Puedes usar las pestañas de control del cortafuegos para abrir o cerrar los puertos que están abiertos por defecto en la Grid Network, Admin Network y Client Network. También puedes crear una lista de direcciones IP privilegiadas que pueden acceder a los puertos del grid que estén cerrados. Si estás usando una Client Network, puedes especificar si un nodo confía en el tráfico entrante de la Client Network y puedes configurar el acceso a puertos específicos en la Client Network.

Limitar el número de puertos abiertos a direcciones IP fuera de tu grid a solo aquellos que sean absolutamente necesarios mejora la seguridad de tu grid. Usas la configuración de cada una de las tres

pestañas de control del Firewall para asegurarte de que solo estén abiertos los puertos necesarios.

Para obtener más información sobre el uso de los controles del firewall, incluidos algunos ejemplos, consulta "Gestiona los controles del cortafuegos".

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulta "Controla el acceso en el cortafuegos externo".

Accede a los controles del cortafuegos

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Control del cortafuegos**.

   Las tres pestañas de esta página se describen en "Gestiona los controles del cortafuegos".

2. Selecciona cualquier pestaña para configurar los controles del cortafuegos.

   Puedes utilizar estas pestañas en cualquier orden. Las configuraciones que establezcas en una pestaña no limitan lo que puedes hacer en las demás; sin embargo, los cambios de configuración que realices en una pestaña podrían modificar el comportamiento de los puertos configurados en otras pestañas.

Lista de direcciones privilegiadas

La pestaña «Lista de direcciones privilegiadas» sirve para conceder a los hosts acceso a los puertos que están cerrados por defecto o que se han cerrado mediante la configuración de la pestaña «Manage external access».

Las direcciones IP y subredes con privilegios no tienen acceso al grid interno de forma predeterminada. Además, los endpoints del equilibrador de carga y los puertos adicionales que abras en la pestaña Lista de direcciones con privilegios seguirán estando accesibles aunque los bloquees en la pestaña Administrar acceso externo.

> La configuración de la pestaña «Lista de direcciones privilegiadas» no puede anular la configuración de la pestaña «Red de clientes no fiables».

Pasos

1. En la pestaña «Lista de direcciones privilegiadas», introduce la dirección o la subred IP a la que quieres conceder acceso a los puertos cerrados.
2. Si lo deseas, selecciona **Add another IP address or subnet in CIDR notation** para añadir clientes con privilegios adicionales.

   > Agrega la menor cantidad posible de direcciones a la lista de direcciones privilegiadas.

3. Si lo deseas, selecciona **Permitir que las direcciones IP con privilegios accedan a los puertos internos de StorageGRID**. Consulta "Puertos internos de StorageGRID".

   > Esta opción elimina algunas protecciones para los servicios internos. Si es posible, déjala desactivada.

4. Selecciona **Guardar**.

Gestiona el acceso externo

Cuando se cierra un puerto en la pestaña Gestionar acceso externo, el puerto no puede ser accedido por ninguna dirección IP que no sea de la grid, a menos que añadas la dirección IP a la lista de direcciones privilegiadas. Solo puedes cerrar los puertos que están abiertos por defecto, y solo puedes abrir los puertos que hayas cerrado.

> La configuración de la pestaña Manage external access no puede anular la configuración de la pestaña Untrusted Client Network. Por ejemplo, si un nodo no es de confianza, el puerto SSH/22 se bloquea en la Client Network aunque esté abierto en la pestaña Manage external access. La configuración de la pestaña Untrusted Client Network anula los puertos cerrados (como 443, 8443, 9443) en la Client Network.

Pasos

1. Selecciona **Gestionar acceso externo**. La pestaña muestra una tabla con todos los puertos externos (puertos a los que pueden acceder por defecto los nodos que no forman parte del grid) de los nodos de tu grid.
2. Configura los puertos que quieras abrir y cerrar utilizando las siguientes opciones:
   - ${post_edited_translations.segment}
   - Selecciona **Abrir todos los puertos mostrados** para abrir todos los puertos que aparecen en la tabla.
   - ${post_edited_translations.segment}

> Si cierras los puertos 443 u 8443 de Grid Manager, cualquier usuario que esté conectado en ese momento a un puerto bloqueado, incluido tú, perderá el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas.

> Utiliza la barra de desplazamiento situada a la derecha de la tabla para asegurarte de que has visto todos los puertos disponibles. Utiliza el campo de búsqueda para encontrar la configuración de cualquier puerto externo introduciendo un número de puerto. Puedes introducir un número de puerto parcial. Por ejemplo, si introduces **2**, se mostrarán todos los puertos que tengan la cadena "2" como parte de su nombre.

3. Selecciona **Guardar**

${post_edited_translations.segment}

Si la red de cliente de un nodo no es de confianza, el nodo solo acepta tráfico entrante en los puertos configurados como puntos finales del equilibrador de carga y, opcionalmente, en los puertos adicionales que selecciones en esta pestaña. También puedes utilizar esta pestaña para especificar la configuración predeterminada para los nuevos nodos añadidos en una ampliación.

> Las conexiones de los clientes existentes podrían fallar si no se han configurado los endpoints del equilibrador de carga.

${post_edited_translations.segment}

Pasos

1. Selecciona **Red de cliente no fiable**.

2. En la sección «Establecer valor predeterminado para nuevos nodos», especifica cuál debe ser la configuración predeterminada cuando se añadan nuevos nodos a la grid en un procedimiento de ampliación.

   - **De confianza** (por defecto): Cuando se añade un nodo en una ampliación, su Client Network es de confianza.
   - **No fiable**: Cuando se añade un nodo en una ampliación, su red de cliente no es fiable.

     Si lo necesitas, puedes volver a esta pestaña para cambiar la configuración de un nodo nuevo concreto.

   ${post_edited_translations.segment}

3. Utiliza las siguientes opciones para seleccionar los nodos que solo deben permitir conexiones de clientes en los puntos finales del equilibrador de carga configurados explícitamente o en puertos adicionales seleccionados:

   - Selecciona **Marcar como no fiable los nodos mostrados** para añadir todos los nodos que aparecen en la tabla a la lista de Red de clientes no fiables.
   - Selecciona **Confiar en los nodos mostrados** para eliminar todos los nodos que aparecen en la tabla de la lista de Untrusted Client Network.
   - Utiliza el botón de alternancia situado junto a cada nodo para configurar la red del cliente como de confianza o no de confianza para el nodo seleccionado.

     ${post_edited_translations.segment}

   Utiliza la barra de desplazamiento situada a la derecha de la tabla para asegurarte de que has visto todos los nodos disponibles. Utiliza el campo de búsqueda para encontrar la configuración de cualquier nodo introduciendo el nombre de nodo. Puedes introducir un nombre parcial. Por ejemplo, si introduces **GW**, se mostrarán todos los nodos que tengan la cadena "GW" como parte de su nombre.

4. Selecciona **Guardar**.

   La nueva configuración del cortafuegos se aplica y se hace efectiva de forma inmediata. Las conexiones de los clientes existentes podrían fallar si no se han configurado los endpoints del balanceador de carga.

Gestiona inquilinos

Cuentas de tenant en StorageGRID

Una cuenta de inquilino te permite utilizar la API de REST del Servicio de Almacenamiento Sencillo (S3) para almacenar y recuperar objetos en un sistema StorageGRID.

Se han eliminado los detalles sobre Swift de esta versión del sitio de documentación. Consulta "StorageGRID 11.8: administra inquilinos".

Como administrador de la grid, creas y gestionas las cuentas de inquilino que los clientes de S3 usan para almacenar y recuperar objetos.

${post_edited_translations.segment}

Puedes usar las cuentas de inquilino para segregar los objetos almacenados por diferentes entidades. Por ejemplo, puedes usar varias cuentas de inquilino para cualquiera de estos casos de uso:

- **Caso de uso empresarial:** Si administras un sistema StorageGRID en una aplicación empresarial, es posible que desees segregar el almacenamiento de objetos de la red según los distintos departamentos de tu organización. En este caso, podrías crear cuentas de inquilino para el departamento de Marketing, el departamento de Customer Support, el departamento de Human Resources, etc.

> Si utilizas el protocolo de cliente S3, puedes emplear los buckets de S3 y las políticas de bucket para segregar los objetos entre los departamentos de una empresa. No necesitas usar cuentas de inquilino. Consulta las instrucciones para implementar "${post_edited_translations.segment}" para más información.

- **Caso de uso de proveedor de servicios:** Si administras un sistema StorageGRID como proveedor de servicios, puedes segregar el almacenamiento de objetos del grid por las diferentes entidades que alquilarán el almacenamiento en tu grid. En este caso, crearías cuentas de inquilino para Company A, Company B, Company C, y así sucesivamente.

Para más información, consulta "Utiliza una cuenta de inquilino".

${post_edited_translations.segment}

Utiliza el Grid manager para crear una cuenta de inquilino. Al crear una cuenta de inquilino, debes especificar la siguiente información:

- ${post_edited_translations.segment}
- Permisos de la cuenta de inquilino, como si la cuenta de inquilino puede usar los servicios de la plataforma S3, configurar su propia fuente de identidad, usar S3 Select o usar una conexión de federación de grid.
- El acceso a raíz inicial para el inquilino, en función de si el sistema StorageGRID utiliza grupos y usuarios locales, federación de identidades o inicio de sesión único (SSO).

Además, puedes activar la configuración de S3 Object Lock para el sistema StorageGRID si las cuentas de inquilino de S3 deben cumplir con los requisitos normativos. Cuando S3 Object Lock está activado, todas las cuentas de inquilino de S3 pueden crear y gestionar buckets conformes.

¿Para qué sirve Tenant Manager?

Después de crear la cuenta de inquilino, los usuarios del inquilino pueden iniciar sesión en el Tenant Manager para realizar tareas como las siguientes:

- Configura la federación de identidades (a menos que la fuente de identidades se comparta con la grid)
- Gestiona grupos y usuarios
- Utiliza la federación de grid para la clonación de cuentas y la replicación entre grid
- Gestiona claves de acceso de S3
- Crear y gestionar buckets de S3
- Usa los servicios de la plataforma S3
- ${post_edited_translations.segment}
- Supervisa el uso del almacenamiento

Aunque los usuarios inquilinos de S3 pueden crear y gestionar claves de acceso y buckets de S3 con el Tenant Manager, deben usar una aplicación cliente de S3 para cargar y gestionar objetos. Consulta "Usa la API de REST de S3" para más detalles.

Crear una cuenta de inquilino de StorageGRID

Debes crear al menos una cuenta de inquilino para controlar el acceso al almacenamiento en tu sistema StorageGRID.

Los pasos para crear una cuenta de inquilino varían en función de si "federación de identidades" y "inicio de sesión único" están configurados y de si la cuenta de Grid Manager que usas para crear la cuenta de inquilino pertenece a un grupo de administradores con el permiso de acceso a raíz.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "${post_edited_translations.segment}".
- Si la cuenta de inquilino va a usar la fuente de identidad que se configuró para Grid Manager y quieres otorgar el permiso de acceso a raíz para la cuenta de inquilino a un grupo federado, ya habrás importado ese grupo federado en Grid Manager. No necesitas asignar ningún permiso de Grid Manager a este grupo de administradores. Consulta "${post_edited_translations.segment}".
- ${post_edited_translations.segment}
  - Tienes "configuraste la conexión de federación de grid".
  - El estado de la conexión es **Conectado**.
  - Tienes permiso de acceso root.
  - Ya has revisado las consideraciones para "gestionar los inquilinos permitidos para la federación de grid".
  - ${post_edited_translations.segment}

    Al crear el inquilino, deberás seleccionar este grupo para que tenga el permiso de acceso a raíz inicial tanto para la cuenta de inquilino de origen como para la de destino.

    Si este grupo de administradores no existe en ambas grids antes de crear el tenant, el tenant no se replica en el destino.

Accede al asistente

Pasos

1. Selecciona **Tenants**.
2. Selecciona **Crear**.

Introduce los datos

Pasos

1. Introduce los datos del inquilino.

Campo	Descripción
Nombre	Un nombre para la cuenta de inquilino. No es necesario que los nombres de los inquilinos sean únicos. Cuando se crea la cuenta de inquilino, recibe un identificador de cuenta único de 20 dígitos.
Descripción (opcional)	Una descripción que ayude a identificar al inquilino. Si vas a crear un inquilino que utilizará una conexión de federación de grid, puedes usar este campo de forma opcional para ayudar a identificar cuál es el inquilino de origen y cuál es el de destino. Por ejemplo, esta descripción para un inquilino creado en Grid 1 también aparecerá para el inquilino replicado en Grid 2: "Este inquilino fue creado en Grid 1."
Tipo de cliente	Debe ser **S3**.
Cuota de almacenamiento (opcional)	Si quieres que este inquilino tenga una cuota de almacenamiento, indica un valor numérico para la cuota y las unidades.

2. Selecciona **Continuar**.

Selecciona permisos

Pasos

1. Si lo deseas, selecciona los permisos básicos que quieres que tenga este inquilino.

> Algunos de estos permisos tienen requisitos adicionales. Para obtener más información, selecciona el icono de ayuda correspondiente a cada permiso.

Permiso	${post_edited_translations.segment}
Permitir los servicios de la plataforma	El arrendatario puede utilizar los servicios de la plataforma S3, como CloudMirror. Consulta "${post_edited_translations.segment}".
Usa tu propia fuente de identidad	El inquilino puede configurar y gestionar su propia fuente de identidad para grupos y usuarios federados. Esta opción está desactivada si tienes "SSO configurado" para tu sistema StorageGRID.
${post_edited_translations.segment}	El inquilino puede realizar solicitudes de la API SelectObjectContent de S3 para filtrar y recuperar datos de objetos. Consulta "${post_edited_translations.segment}". **Importante**: Las solicitudes de SelectObjectContent pueden reducir el rendimiento del balanceador de carga para todos los clientes de S3 y todos los inquilinos. Activa esta función solo cuando sea necesario y solo para inquilinos de confianza.

2. ${post_edited_translations.segment}

Permiso	${post_edited_translations.segment}
Conexión de federación de grid	El inquilino puede usar una conexión de federación de grid, que: • ${post_edited_translations.segment} • Permite a este inquilino configurar la replicación entre grids entre los buckets correspondientes de cada grid. Consulta "Gestiona los inquilinos permitidos para la federación de grid".
Bloqueo de objetos de S3	Permitir al inquilino usar funciones específicas de S3 Object Lock: • **Establecer el periodo máximo de retención** define durante cuánto tiempo deben conservarse los nuevos objetos añadidos a este bucket, a partir del momento en que se ingieren. • La opción «**Permitir modo de cumplimiento**» impide que los usuarios sobrescriban o eliminen versiones de objetos protegidos durante el periodo de retención.

3. Selecciona **Continuar**.

Define el acceso a raíz y crea un inquilino

Pasos

1. Define el acceso a raíz para la cuenta de inquilino, en función de si tu sistema StorageGRID utiliza la federación de identidades, el inicio de sesión único (SSO) o ambos.

Opción	Haz esto
Si la federación de identidades no está habilitada	${post_edited_translations.segment}
${post_edited_translations.segment}	a. Selecciona un grupo federado ya existente para disponer de permiso de acceso a raíz para el inquilino. b. Si lo deseas, indica la contraseña que se usará al iniciar sesión en el tenant como usuario raíz local.
${post_edited_translations.segment}	Selecciona un grupo federado existente para tener permiso de acceso a raíz para el inquilino. Ningún usuario local puede iniciar sesión.

2. Selecciona **Create tenant**.

   Aparece un mensaje de éxito y el nuevo tenant aparece en la página Tenants. Para saber cómo ver los detalles del tenant y supervisar la actividad del tenant, consulta "Supervisa la actividad de los inquilinos".

   ${post_edited_translations.segment}

3. Si has seleccionado el permiso **Usar conexión de federación de grid** para el tenant:

a. Confirma que se haya replicado un inquilino idéntico en el otro grid de la conexión. Los inquilinos de ambos grids tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos.

> Si aparece el mensaje de error «Tenant creado sin clon», consulta las instrucciones en "${post_edited_translations.segment}".

b. Si proporcionaste una contraseña de usuario raíz local al definir el acceso a raíz, "cambiar la contraseña del usuario raíz local" para el inquilino replicado.

> Un usuario raíz local no puede iniciar sesión en Tenant Manager en la red de destino hasta que se cambie la contraseña.

${post_edited_translations.segment}

Según sea necesario, puedes iniciar sesión en el nuevo inquilino ahora para completar la configuración, o puedes iniciar sesión en el inquilino más tarde. Los pasos de inicio de sesión dependen de si has iniciado sesión en el Grid Manager utilizando el puerto predeterminado (443) o un puerto restringido. Consulta "Controla el acceso en el cortafuegos externo".

${post_edited_translations.segment}

Si estás utilizando…	Haz esto…
El puerto 443 y configuras una contraseña para el usuario raíz local	1. Selecciona **Sign in as root**. ${post_edited_translations.segment} 2. Selecciona los enlaces para configurar la cuenta de inquilino. Cada enlace abre la página correspondiente en Tenant Manager. Para completar la página, consulta "Instrucciones para usar las cuentas de inquilino".
Puerto 443 y no has establecido una contraseña para el usuario raíz local	Selecciona **Sign in** e introduce las credenciales de un usuario del grupo federado de acceso a raíz.

Si estás utilizando…	Haz esto…
Un puerto restringido	1. ${post_edited_translations.segment} 2. Selecciona **Restricted** en la tabla Tenant para obtener más información sobre cómo acceder a esta cuenta de inquilino. La URL de Tenant Manager tiene este 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 exclusivo para el inquilino ◦ *20-digit-account-id* es el identificador único de la cuenta del arrendatario

${post_edited_translations.segment}

Si estás utilizando…	${post_edited_translations.segment}
${post_edited_translations.segment}	• Desde el Grid Manager, selecciona **Tenants** y luego selecciona **Sign in** a la derecha del nombre del tenant. • Introduce 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 identificador único de la cuenta del arrendatario
Un puerto restringido	• Desde el Grid Manager, selecciona **Tenants** y luego selecciona **Restricted**. • Introduce 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 inquilinos ◦ *20-digit-account-id* es el identificador único de la cuenta del arrendatario

Configura el inquilino

Sigue las instrucciones de "Utiliza una cuenta de inquilino" para gestionar los grupos y usuarios del inquilino, las claves de acceso de S3, los buckets, los servicios de plataforma, y la clonación de cuentas y la replicación entre grids.

Editar una cuenta de inquilino de StorageGRID

${post_edited_translations.segment}

> Si un inquilino tiene el permiso **Utilizar conexión de federación de grid**, puedes editar los detalles del inquilino desde cualquiera de los grids en la conexión. Sin embargo, los cambios que realices en un grid de la conexión no se copiarán al otro grid. Si quieres mantener los detalles del inquilino exactamente sincronizados entre grids, haz los mismos cambios en ambos grids. Consulta "Gestiona los inquilinos permitidos para la conexión de federación de grid".

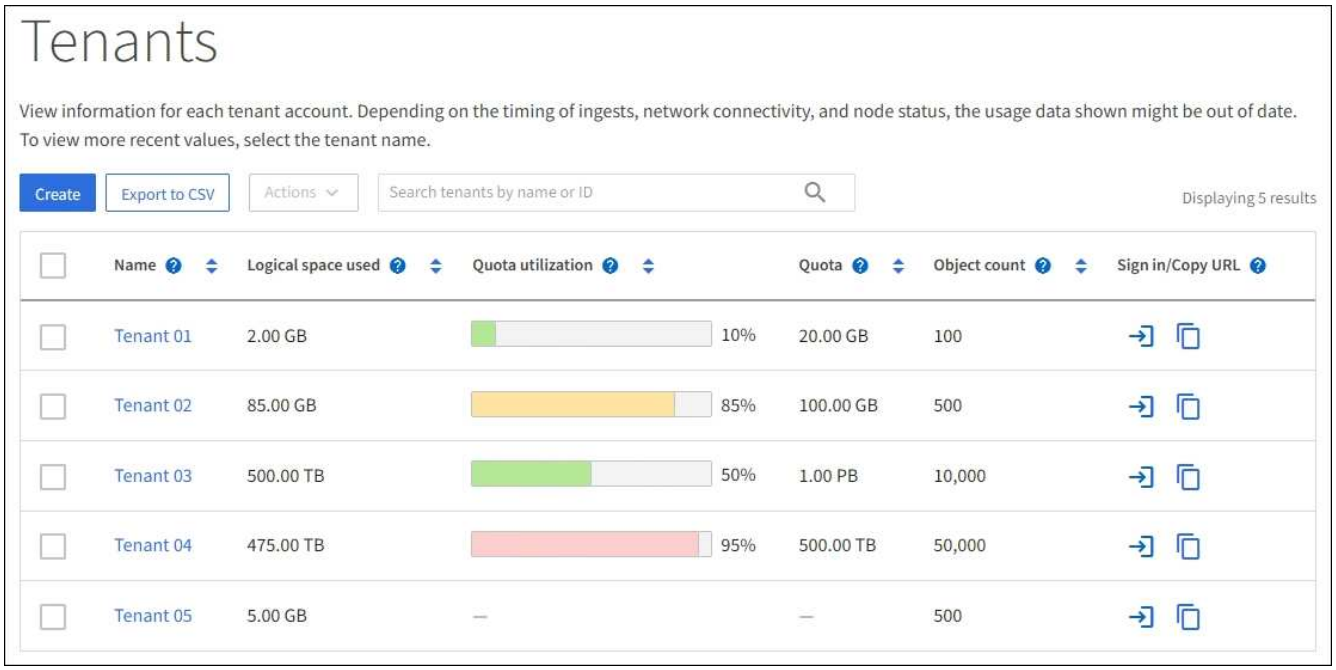
Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "${post_edited_translations.segment}".

> ${post_edited_translations.segment}

Pasos

1. Selecciona **Tenants**.



2. Busca la cuenta de inquilino que deseas modificar.

   ${post_edited_translations.segment}

3. Selecciona el inquilino. Puedes hacer cualquiera de las siguientes cosas:
   - Marca la casilla de selección correspondiente al tenant y selecciona **Actions** > **Edit**.

- ${post_edited_translations.segment}

4. ${post_edited_translations.segment}
   - **Nombre**
   - **Descripción**
   - **Cuota de almacenamiento**
5. Selecciona **Continuar**.
6. ${post_edited_translations.segment}
   - Si desactivas los **servicios de plataforma** para un inquilino que ya los está usando, los servicios que haya configurado para sus buckets S3 dejarán de funcionar. No se envía ningún mensaje de error al inquilino. Por ejemplo, si el inquilino ha configurado la replicación de CloudMirror para un bucket S3, aún podrá almacenar objetos en el bucket, pero ya no se realizarán copias de esos objetos en el bucket S3 externo que haya configurado como extremo. Consulta "${post_edited_translations.segment}".
   - ${post_edited_translations.segment}

     Si **Usar fuente de identidad propia** está:

     - Deshabilitado y seleccionado, el inquilino ya ha activado su propio origen de identidad. Un inquilino debe deshabilitar su origen de identidad antes de poder usar el origen de identidad que se configuró para el Grid Manager.
     - Si está desactivado y no se ha seleccionado, el inicio de sesión único está habilitado para el sistema StorageGRID. El inquilino debe usar la fuente de identidad que se configuró para el Grid Manager.
   - Selecciona o desmarca el permiso **Allow S3 Select** según lo necesites. Consulta "${post_edited_translations.segment}".
   - Para eliminar el permiso **Usar conexión de federación de grid**:
     i. Selecciona la pestaña **Grid federation**.
     ii. Selecciona **Eliminar permiso**.
   - Para añadir el permiso **Use grid federation connection**:
     i. Selecciona la pestaña **Grid federation**.
     ii. Selecciona la casilla **Usar conexión de federación de grid**.
     iii. Opcionalmente, selecciona **Clonar usuarios y grupos locales existentes** para clonarlos en el grid remoto. Si quieres, puedes detener la clonación en curso o reintentar la clonación si algunos usuarios o grupos locales no se pudieron clonar después de que se completara la última operación de clonación.
   - ${post_edited_translations.segment}

     Debes habilitar S3 Object Lock en la grid antes de poder usar estos ajustes.

     i. ${post_edited_translations.segment}
     ii. ${post_edited_translations.segment}
     iii. Para **Permitir el modo de cumplimiento**, marca la casilla de verificación.

Cambiar la contraseña del usuario raíz local de un tenant de StorageGRID

Es posible que tengas que cambiar la contraseña del usuario raíz local de un inquilino si el usuario raíz se queda sin acceso a la cuenta.

Antes de empezar

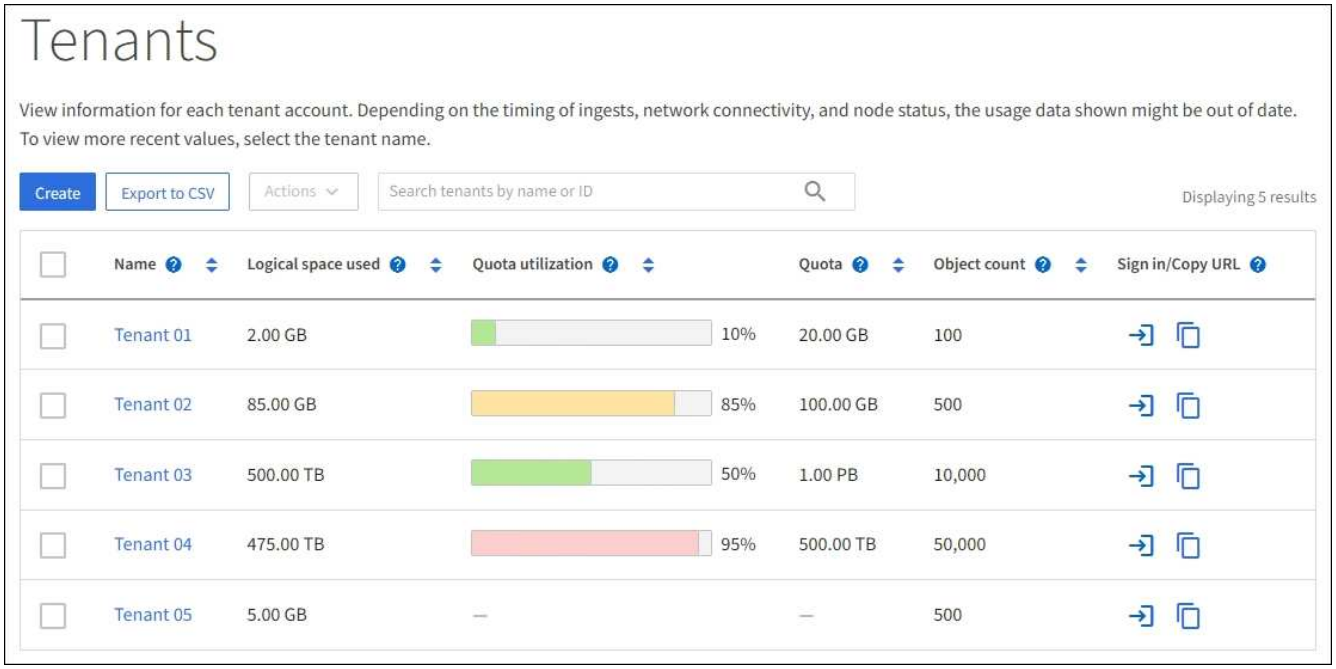
- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".

Acerca de esta tarea

Si el inicio de sesión único (SSO) está habilitado para tu sistema StorageGRID, el usuario raíz local no puede iniciar sesión en la cuenta del inquilino. Para realizar tareas de usuario raíz, los usuarios deben pertenecer a un grupo federado que tenga el permiso de acceso Root para el inquilino.

Pasos

1. Selecciona **Tenants**.



2. Selecciona la cuenta de inquilino. Puedes hacer cualquiera de las siguientes cosas:
   - Marca la casilla de selección correspondiente al tenant y selecciona **Actions** > **Change root password**.
   - Selecciona el nombre del inquilino para abrir la página de detalles y selecciona **Actions** > **Change root password**.
3. Introduce la nueva contraseña para la cuenta del inquilino.
4. Selecciona **Guardar**.

Eliminar una cuenta de inquilino de StorageGRID

Puedes eliminar una cuenta de inquilino si quieres eliminar de forma permanente el acceso de ese inquilino al sistema.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Has eliminado todos los buckets y objetos de S3 asociados con la cuenta de inquilino.
- Si se permite al inquilino utilizar una conexión de federación de grid, ya has revisado las consideraciones para "Eliminar un inquilino con el permiso Use grid federation connection".

Pasos

1. Selecciona **Tenants**.
2. Busca la cuenta o cuentas de inquilino que quieras eliminar.

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
   - Marca la casilla de selección y selecciona **Actions** > **Delete**.
   - Selecciona el nombre del inquilino para mostrar la página de detalles y, a continuación, selecciona **Actions** > **Delete**.
5. Selecciona **Sí**.

${post_edited_translations.segment}

Conoce los servicios de la plataforma StorageGRID

Los servicios de plataforma incluyen la replicación de CloudMirror, las notificaciones de eventos y el servicio de integración de búsqueda.

Si habilitas los servicios de plataforma para las cuentas de inquilino de S3, debes configurar tu grid para que los inquilinos puedan acceder a los recursos externos necesarios para utilizar estos servicios.

Los servicios de plataforma no son compatibles con "cubos de rama".

CloudMirror replicación

El servicio de replicación CloudMirror de StorageGRID se utiliza para reflejar objetos específicos de un bucket de StorageGRID en un destino externo especificado.

Por ejemplo, podrías usar la replicación CloudMirror para reflejar registros específicos de clientes en Amazon S3 y luego aprovechar los servicios de AWS para hacer análisis de tus datos.

La replicación CloudMirror tiene algunas similitudes y diferencias importantes con la función de replicación entre grids. Para obtener más información, consulta "Compara la replicación entre grids y la replicación CloudMirror".

> CloudMirror replication no es compatible si el bucket de origen tiene activada la función S3 Object Lock.

Notificaciones

Las notificaciones de eventos por bucket se utilizan para enviar notificaciones sobre acciones específicas realizadas en objetos a un clúster externo de Kafka, un endpoint de webhook o Amazon Simple Notification Service especificados.

Por ejemplo, podrías configurar alertas para que se envíen a los administradores sobre cada objeto añadido a un bucket, donde los objetos representan archivos de registro asociados con un evento crítico del sistema.

> Aunque es posible configurar las notificaciones de eventos en un bucket con S3 Object Lock activado, los metadatos de S3 Object Lock (incluidos Retain Until Date y el estado de Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

Servicio de integración de búsquedas

El servicio de integración de búsqueda se utiliza para enviar los metadatos de los objetos de S3 a un índice de Elasticsearch especificado, donde los metadatos pueden buscarse o analizarse usando el servicio externo.

Por ejemplo, podrías configurar tus buckets para que envíen los metadatos de los objetos de S3 a un servicio remoto de Elasticsearch. Luego, podrías usar Elasticsearch para realizar búsquedas en todos los buckets y hacer análisis sofisticados de los patrones presentes en los metadatos de tus objetos.

> Aunque la integración con Elasticsearch se puede configurar en un bucket con S3 Object Lock activado, los metadatos de S3 Object Lock (incluidos Retain Until Date y el estado de Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

Los servicios de plataforma les dan a los inquilinos la posibilidad de usar recursos de almacenamiento externos, servicios de notificación y servicios de búsqueda o análisis con sus datos. Como la ubicación de destino de los servicios de plataforma suele estar fuera de tu implementación de StorageGRID, debes decidir si quieres permitir que los inquilinos usen estos servicios. Si es así, debes habilitar el uso de los servicios de plataforma cuando crees o edites cuentas de inquilino. También tienes que configurar tu red para que los mensajes de los servicios de plataforma que generen los inquilinos puedan llegar a sus destinos.

Recomendaciones para usar los servicios de la plataforma

${post_edited_translations.segment}

- Si un bucket S3 en el sistema StorageGRID tiene habilitadas tanto la gestión de versiones como la replicación CloudMirror, también deberías habilitar la gestión de versiones del bucket S3 para el endpoint de destino. Esto permite que la replicación CloudMirror genere versiones de objetos similares en el endpoint.
- No debes usar más de 100 inquilinos activos con solicitudes de S3 que requieran replicación de CloudMirror, notificaciones e integración de búsqueda. Tener más de 100 inquilinos activos puede resultar en un rendimiento más lento del cliente S3.
- Las solicitudes dirigidas a un endpoint que no puedan completarse se pondrán en cola hasta un máximo de 500,000 solicitudes. Este límite se reparte a partes iguales entre los tenants activos. A los nuevos tenants se les permite superar temporalmente este límite de 500,000 para que los tenants recién creados no se vean penalizados injustamente.

Información relacionada

- "${post_edited_translations.segment}"
- "Configura los ajustes del proxy de almacenamiento"

- "Supervisar StorageGRID"

Red y puertos para los servicios de plataforma StorageGRID

${post_edited_translations.segment}

Puedes habilitar los servicios de plataforma para una cuenta de inquilino de S3 cuando crees o actualices la cuenta de inquilino. Si los servicios de plataforma están habilitados, el inquilino puede crear puntos de conexión que sirvan como destino para la replicación de CloudMirror, las notificaciones de eventos o los mensajes de integración de búsqueda de sus buckets de S3. Estos mensajes de servicios de plataforma se envían desde los nodos de almacenamiento que ejecutan el servicio ADC a los puntos de conexión de destino.

Por ejemplo, los inquilinos podrían configurar los siguientes tipos de puntos finales de destino:

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Un clúster de Kafka alojado localmente
- Un endpoint de webhook externo o alojado localmente que admite solicitudes de notificación HTTP POST.

  Este endpoint puede alojarse en diversos servidores web, frameworks o herramientas de procesamiento de datos, como Fluentd.

- Un bucket de S3 alojado localmente en la misma o en otra instancia de StorageGRID
- Un punto final externo, como un punto final en Amazon Web Services.

Para garantizar que se puedan entregar los mensajes de los servicios de la plataforma, debes configurar la red o redes que contienen los nodos de almacenamiento del ADC. Debes asegurarte de que se puedan usar los siguientes puertos para enviar mensajes de los servicios de la plataforma a los endpoints de destino.

De forma predeterminada, los mensajes de los servicios de la plataforma se envían a través de los siguientes puertos:

- **80**: Para los URI de puntos finales que comienzan por http (la mayoría de los puntos finales)
- **443**: Para los URI de puntos finales que comienzan con https (la mayoría de los puntos finales)
- ${post_edited_translations.segment}

${post_edited_translations.segment}

> Si se utiliza una implementación de StorageGRID como destino para la replicación de CloudMirror, es posible que los mensajes de replicación se reciban en un puerto que no sea el 80 o el 443. Asegúrate de que el puerto que utiliza la implementación de StorageGRID de destino para S3 esté especificado en el endpoint.

Si utilizas un proxy no transparente, también debes "configura los ajustes del proxy de almacenamiento" para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

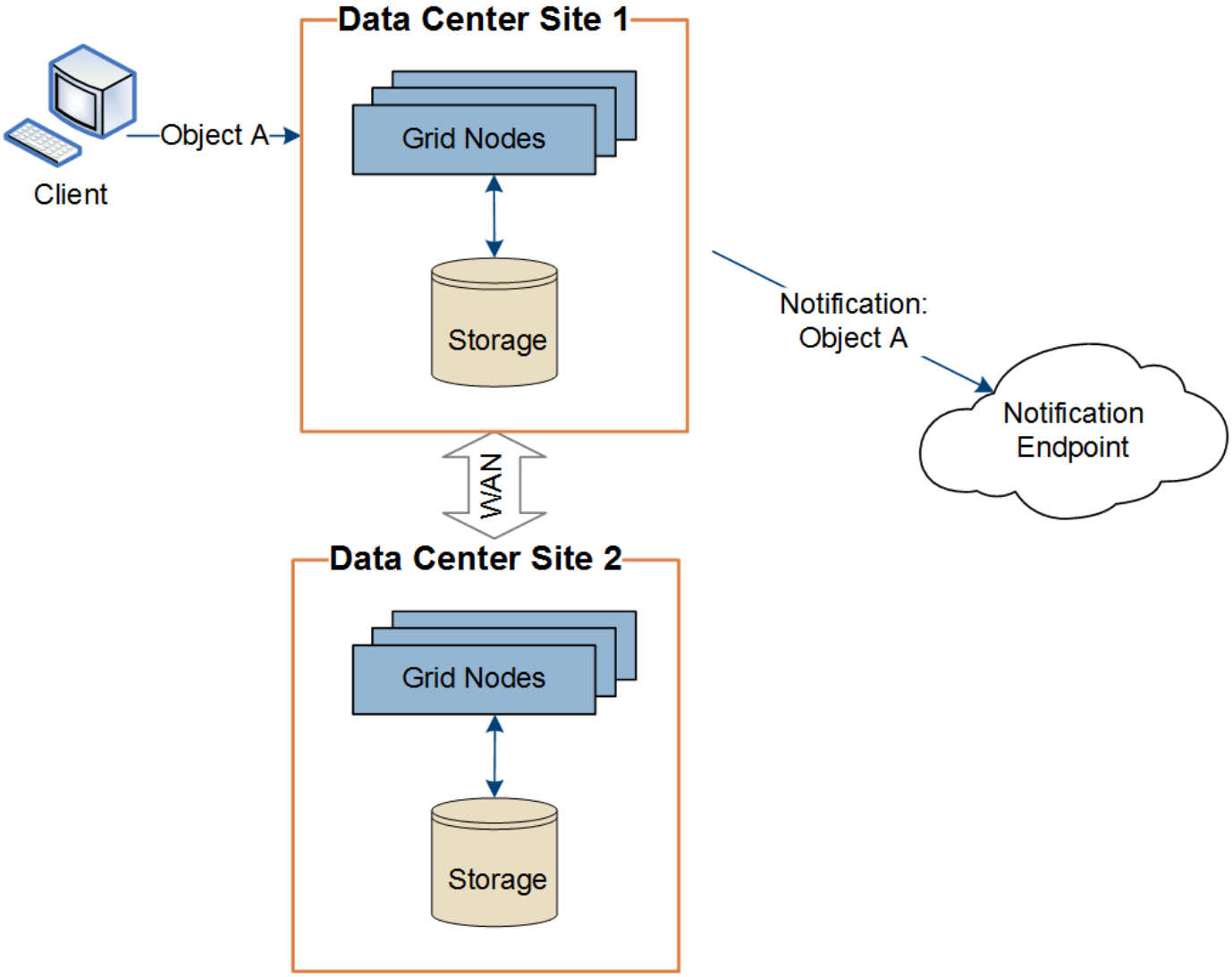
Información relacionada

"Utiliza una cuenta de inquilino"

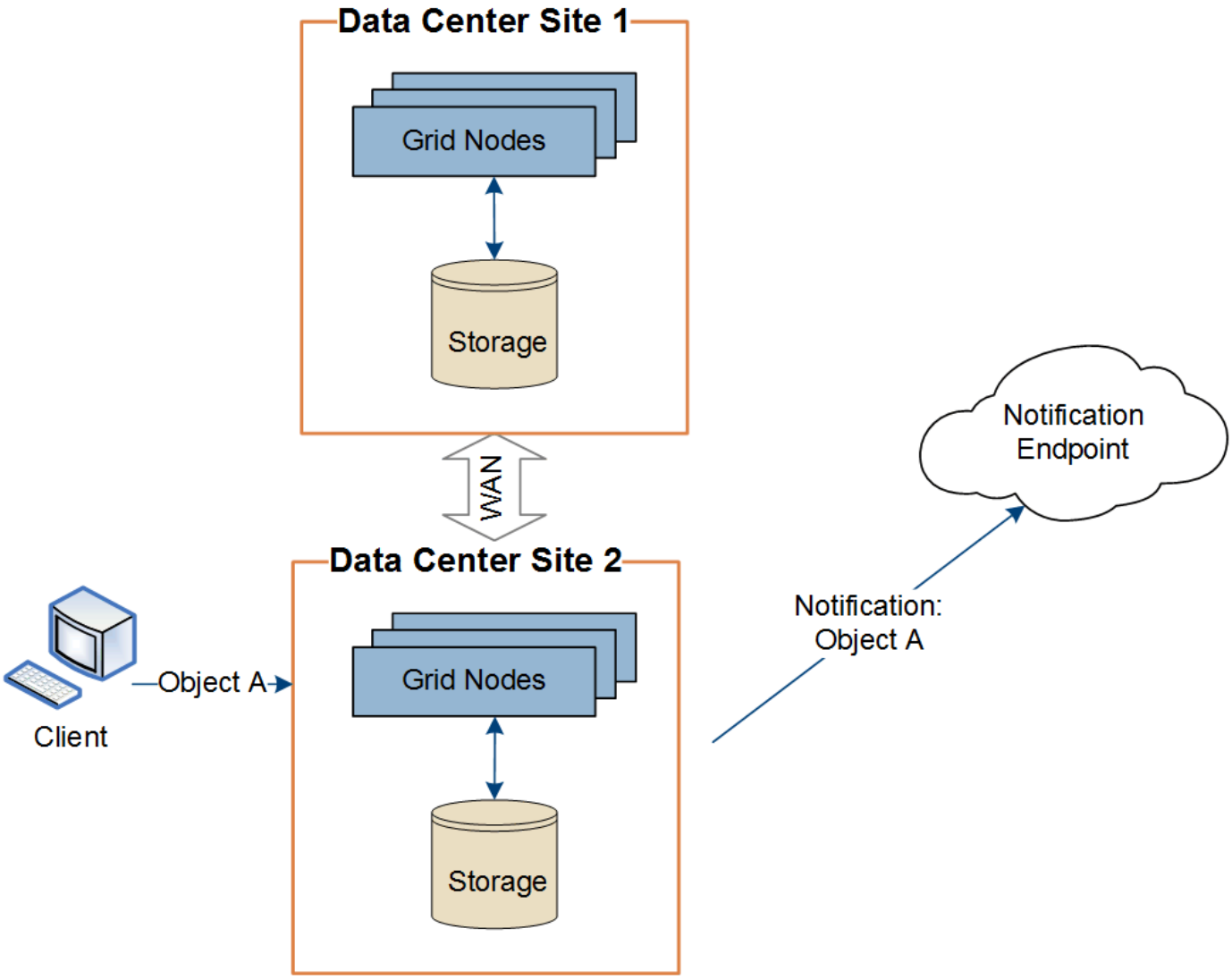
Entrega por sitio de mensajes de servicios de plataforma StorageGRID

Todas las operaciones de los servicios de la plataforma se realizan por sitio.

${post_edited_translations.segment}



${post_edited_translations.segment}



Asegúrate de que la red de cada sitio esté configurada de tal forma que los mensajes de los servicios de la plataforma puedan entregarse a sus destinos.

Soluciona problemas de los servicios de la plataforma StorageGRID

Los puntos finales utilizados en los servicios de la plataforma son creados y gestionados por los usuarios del inquilino en el Tenant Manager. Sin embargo, si un inquilino tiene problemas para configurar o usar los servicios de la plataforma, podrías usar el Grid Manager para ayudar a resolver el problema.

${post_edited_translations.segment}

Antes de que un inquilino pueda usar los servicios de plataforma, debe crear uno o varios endpoints mediante el Tenant Manager. Cada endpoint representa un destino externo para un servicio de plataforma, como un bucket S3 de StorageGRID, un bucket de Amazon Web Services, un tema de Amazon Simple Notification Service, un tema de Kafka o un clúster de Elasticsearch alojado localmente o en AWS. Cada endpoint incluye tanto la ubicación del recurso externo como las credenciales necesarias para acceder a él.

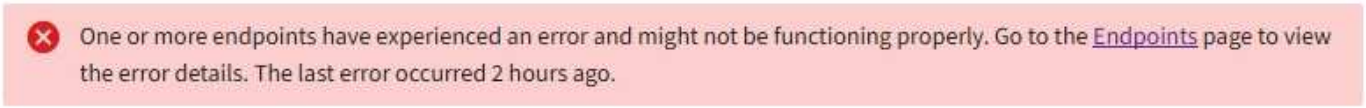
Cuando un inquilino crea un endpoint, el sistema StorageGRID valida que el endpoint existe y que se puede acceder a él usando las credenciales que se especificaron. La conexión con el endpoint se valida desde un nodo en cada sitio.

Si falla la validación del endpoint, aparecerá un mensaje de error explicando por qué falló la validación del endpoint. El usuario del tenant debe resolver el problema y luego intentar crear el endpoint de nuevo.

${post_edited_translations.segment}

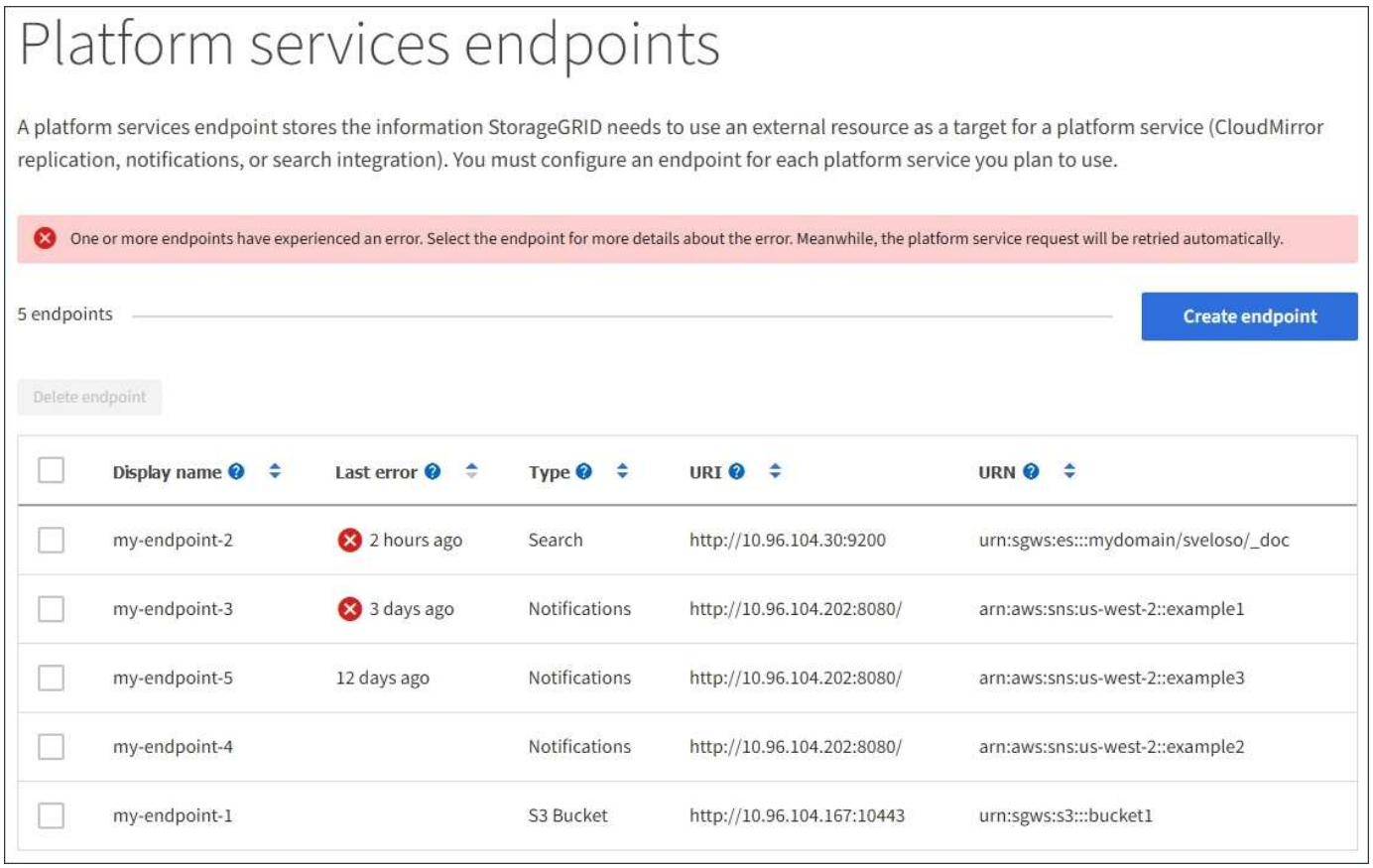
Problemas con los puntos finales existentes

Si se produce un error cuando StorageGRID intenta acceder a un punto final existente, aparece un mensaje en el panel de control de Tenant Manager.



Los usuarios de Tenant pueden acceder a la página Endpoints para consultar el mensaje de error más reciente de cada endpoint y determinar cuánto tiempo hace que ocurrió el error. La columna **Last error** muestra el mensaje de error más reciente de cada endpoint e indica cuánto tiempo hace que ocurrió el error.

Los errores que incluyen el icono ⊗ ocurrieron en los últimos 7 días.



Algunos mensajes de error en la columna **Último error** pueden incluir un logID entre paréntesis. Un administrador de grid o el soporte técnico pueden usar este ID para localizar información más detallada sobre el error en el bycast.log.

${post_edited_translations.segment}

Si has configurado un "${post_edited_translations.segment}" entre los nodos de almacenamiento y los puntos

finales del servicio de la plataforma, pueden producirse errores si tu servicio proxy no permite mensajes de StorageGRID. Para resolver estos problemas, revisa la configuración de tu servidor proxy para asegurarte de que los mensajes relacionados con el servicio de la plataforma no estén bloqueados.

Determina si se ha producido un error

Si se ha producido algún error en los endpoints en los últimos 7 días, el panel de control en Tenant Manager muestra un mensaje de alerta. Puedes ir a la página de Endpoints para ver más detalles sobre el error.

Las operaciones del cliente fallan

Algunos problemas con los servicios de plataforma pueden hacer que las operaciones del cliente en el bucket S3 fallen. Por ejemplo, las operaciones del cliente de S3 fallarán si el servicio interno Replicated State Machine (RSM) se detiene o si hay demasiados mensajes de servicios de plataforma en cola para su entrega.

${post_edited_translations.segment}

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Resuelve cualquier alerta activa. Si es necesario, ponte en contacto con soporte técnico.

Errores de endpoint recuperables e irrecuperables

Una vez creados los puntos finales, pueden producirse errores en las solicitudes de servicios de la plataforma por diversos motivos. Algunos errores se pueden solucionar con la intervención del usuario. Por ejemplo, los errores solucionables pueden deberse a las siguientes causas:

- Las credenciales del usuario se han eliminado o han caducado.
- ${post_edited_translations.segment}
- No se puede entregar la notificación.

Si StorageGRID detecta un error recuperable, la solicitud del servicio de la plataforma se volverá a intentar hasta que tenga éxito.

Otros errores son irrecuperables. Por ejemplo, los errores irrecuperables pueden ocurrir por las siguientes razones:

- El punto final se ha eliminado.
- Un punto final de webhook responde a una solicitud de notificación con un error `400 Bad Request`.

Si StorageGRID detecta un error irrecuperable en un endpoint:

- ${post_edited_translations.segment}
- En Tenant Manager, ve a **ALMACENAMIENTO (S3)** > **Puntos de conexión de servicios de la plataforma** para ver los detalles del error.
- Consulta el `/var/local/log/bycast-err.log` para ver los errores relacionados. Los nodos de almacenamiento que cuentan con el servicio ADC contienen este archivo de registro.

No se pueden entregar los mensajes de los servicios de plataforma

Si el destino experimenta un problema que le impide aceptar mensajes de servicios de plataforma, la operación del cliente en el bucket se realiza correctamente, pero el mensaje de servicios de plataforma no se

entrega. Por ejemplo, este error puede ocurrir si se actualizan las credenciales en el destino de manera que StorageGRID ya no pueda autenticarse en el servicio de destino.

Comprueba si hay alertas relacionadas.

Menor rendimiento en las solicitudes de servicios de la plataforma

El software StorageGRID puede limitar las solicitudes S3 entrantes para un bucket si la velocidad a la que se envían las solicitudes supera la velocidad a la que el extremo de destino puede recibirlas. La limitación solo se produce cuando hay una acumulación de solicitudes en espera de enviarse al extremo de destino.

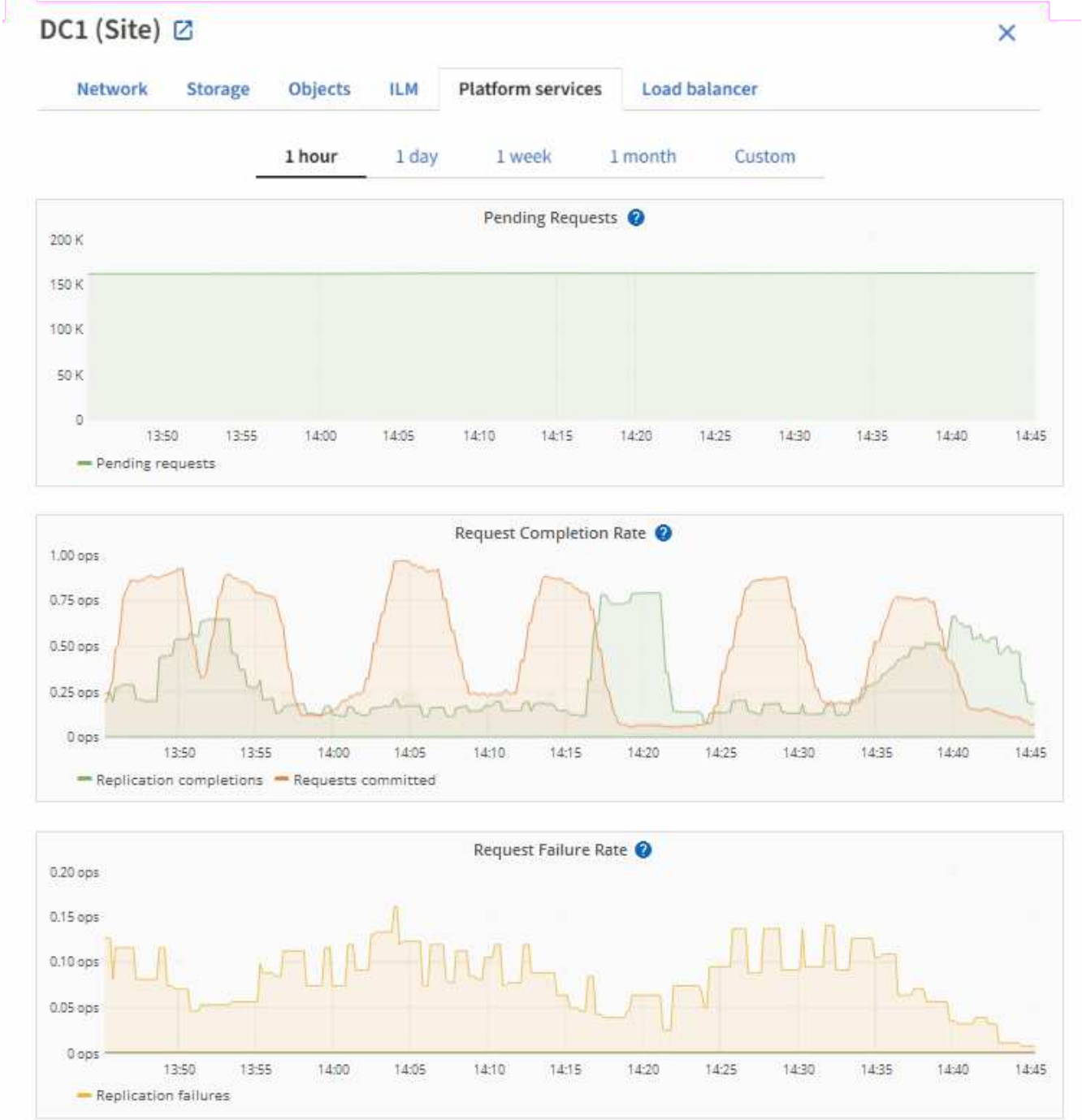
El único efecto visible es que las solicitudes S3 entrantes tardarán más en ejecutarse. Si empiezas a notar una ralentización significativa del rendimiento, deberías reducir la tasa de consumo o usar un endpoint con mayor capacidad. Si la acumulación de solicitudes sigue aumentando, las operaciones S3 de los clientes (como las solicitudes PUT) acabarán fallando.

Las solicitudes de CloudMirror tienen más probabilidades de verse afectadas por el rendimiento del punto final de destino porque normalmente implican más transferencia de datos que las solicitudes de integración de búsqueda o de notificación de eventos.

Las solicitudes de servicio de plataforma fallan

Para consultar la tasa de fallos de las solicitudes de los servicios de plataforma:

1. Selecciona **Nodos**.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}



Alerta de indisponibilidad de los servicios de la plataforma

La alerta **Servicios de la plataforma no disponibles** indica que no se pueden realizar operaciones de los servicios de la plataforma en un sitio porque hay muy pocos 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 endpoints.

Para resolver esta alerta, determina 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.) Luego, asegúrate de que una mayoría simple de esos nodos de almacenamiento estén en funcionamiento y disponibles.

Si en un sitio fallan varios nodos de almacenamiento que contienen el servicio RSM, pierdes cualquier solicitud de servicio de plataforma pendiente para ese sitio.

Guía adicional para la resolución de problemas en los endpoints de los servicios de plataforma

Para obtener más información, consulta **Utiliza una cuenta de inquilino › Soluciona problemas de los endpoints de los servicios de la plataforma**.

Información relacionada

"Soluciona problemas del sistema StorageGRID"

Administra S3 Select para cuentas de inquilinos en StorageGRID

Puedes permitir que ciertos tenants de S3 usen S3 Select para emitir solicitudes SelectObjectContent en objetos individuales.

S3 Select ofrece una forma eficaz de buscar en grandes volúmenes de datos sin tener que implementar una base de datos ni los recursos asociados para habilitar las búsquedas. También reduce el coste y la latencia al recuperar datos.

${post_edited_translations.segment}

S3 Select permite a los clientes de S3 utilizar solicitudes de SelectObjectContent para filtrar y recuperar únicamente los datos necesarios de un objeto. La implementación de S3 Select en StorageGRID incluye un subconjunto de comandos y funciones de S3 Select.

${post_edited_translations.segment}

${post_edited_translations.segment}

El administrador de la grid debe conceder a los inquilinos la capacidad de S3 Select. Selecciona **Permitir S3 Select** cuando "${post_edited_translations.segment}" o "editar un inquilino".

Requisitos de formato de los objetos

El objeto que deseas consultar debe tener uno de los siguientes formatos:

- **CSV**. Se puede usar tal cual o comprimir en archivos GZIP o BZIP2.
- **Parquet**. Requisitos adicionales para los objetos Parquet:
  - S3 Select solo admite la compresión en columnas mediante GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos Parquet.
  - S3 Select no admite la salida en formato Parquet. Debes especificar el formato de salida como CSV o JSON.
  - El tamaño máximo de un grupo de filas sin comprimir es de 512 MB.
  - Debes utilizar los tipos de datos especificados en el esquema del objeto.
  - No puedes usar los tipos lógicos INTERVAL, JSON, LIST, TIME ni UUID.

Requisitos de los endpoints

La solicitud SelectObjectContent debe enviarse a "Punto final del equilibrador de carga de StorageGRID".

Los nodos de administración y gateway que utiliza el endpoint deben ser uno de los siguientes:

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Un nodo bare metal que ejecuta un kernel con cgroup v2 habilitado

Consideraciones generales

No puedes enviar consultas directamente a los nodos de almacenamiento.

> Las solicitudes SelectObjectContent pueden reducir el rendimiento del balanceador de carga para todos los clientes de S3 y todos los inquilinos. Activa esta función solo cuando sea necesario y solo para inquilinos de confianza.

Consulta el "Instrucciones para usar S3 Select".

Para consultar "Gráficos de Grafana" de las operaciones S3 Select a lo largo del tiempo, selecciona **Soporte** > **Herramientas** > **Métricas** en el Grid Manager.

Configura las conexiones de los clientes

Configura conexiones de cliente S3 a StorageGRID

Como administrador de grid, gestionas las opciones de configuración que controlan cómo las aplicaciones cliente de S3 se conectan a tu sistema StorageGRID para almacenar y recuperar datos.

> Se han eliminado los detalles sobre Swift de esta versión del sitio de documentación. Consulta "StorageGRID 11.8: configura las conexiones de los clientes S3 y Swift".

Tareas de configuración

1. Realiza las tareas previas necesarias en StorageGRID, según cómo la aplicación cliente se conecte a StorageGRID.

Tareas obligatorias

Debes obtener:

- Direcciones IP
- ${post_edited_translations.segment}
- Certificado SSL

Tareas opcionales

Opcionalmente, configura:

- ${post_edited_translations.segment}
- SSO

1. Utiliza StorageGRID para obtener los valores que necesita la aplicación para conectarse a la grid. Puedes utilizar el asistente de configuración de S3 o configurar cada entidad de StorageGRID manualmente.

Usa el asistente de configuración de S3

${post_edited_translations.segment}

Configurar manualmente

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Crear cuenta de inquilino
4. Crear bucket y claves de acceso
5. Configura la regla y la política de ILM

1. Usa la aplicación S3 para completar la conexión con StorageGRID. Crea entradas de DNS para asociar direcciones IP a cualquier nombre de dominio que tengas pensado usar.

   ${post_edited_translations.segment}

2. Realiza tareas periódicas en la aplicación y en StorageGRID para gestionar y supervisar el almacenamiento de objetos a lo largo del tiempo.

${post_edited_translations.segment}

Antes de poder conectar StorageGRID a una aplicación cliente de S3, debes realizar pasos de configuración en StorageGRID y obtener ciertos valores.

¿Qué valores necesito?

${post_edited_translations.segment}

Valor	${post_edited_translations.segment}	Dónde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	${post_edited_translations.segment}
Puerto	StorageGRID > Punto de conexión del equilibrador de carga	Aplicación de cliente
Certificado SSL	StorageGRID > Punto de conexión del equilibrador de carga	Aplicación de cliente
Nombre del servidor (FQDN)	StorageGRID > Punto de conexión del equilibrador de carga	• Aplicación de cliente • ${post_edited_translations.segment}

Valor	${post_edited_translations.segment}	Dónde se utiliza el valor
ID de la clave de acceso de S3 y clave de acceso secreta	StorageGRID > Usuario y bucket	Aplicación de cliente
${post_edited_translations.segment}	StorageGRID > Usuario y bucket	Aplicación de cliente

${post_edited_translations.segment}

${post_edited_translations.segment}

- **Usa el "${post_edited_translations.segment}"**. El asistente de configuración de S3 te ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera uno o dos archivos que puedes usar al configurar la aplicación S3. El asistente te guía a través de los pasos necesarios y te ayuda a asegurarte de que tu configuración cumpla con las mejores prácticas de StorageGRID.

  ${post_edited_translations.segment}

- **Usa el "Asistente de configuración de FabricPool"**. De forma similar al asistente de configuración de S3, el asistente de configuración de FabricPool te ayuda a configurar rápidamente los valores necesarios y genera un archivo que puedes usar cuando configures un nivel de cloud de FabricPool en ONTAP.

  Si planeas usar StorageGRID como el sistema de almacenamiento de objetos para un nivel de cloud de FabricPool, se recomienda usar el asistente de configuración de FabricPool, a menos que sepas que tienes requisitos especiales o que tu implementación requerirá una personalización importante.

- **Configura los elementos manualmente**. Si te estás conectando a una aplicación S3 y prefieres no usar el asistente de configuración de S3, puedes obtener los valores necesarios realizando la configuración manualmente. Sigue estos pasos:

  a. Configura el grupo de alta disponibilidad (HA) que quieras utilizar para la aplicación S3. Consulta "Configurar grupos de alta disponibilidad".

  b. Crea el punto de conexión del equilibrador de carga que utilizará la aplicación S3. Consulta "Configura los puntos de conexión del equilibrador de carga".

  c. Crea la cuenta de inquilino que utilizará la aplicación S3. Consulta "Crear una cuenta de inquilino".

  d. Para un inquilino de S3, inicia sesión en la cuenta del inquilino y genera un ID de clave de acceso y una clave de acceso secreta para cada usuario que vaya a acceder a la aplicación. Consulta "Crea tus propias claves de acceso".

  e. Crea uno o más buckets de S3 dentro de la cuenta de tenant. Para S3, consulta "Crear un bucket de S3".

  f. Para añadir instrucciones de ubicación específicas para los objetos que pertenecen al nuevo inquilino o bucket/contenedor, crea una nueva regla de ILM y activa una nueva política de ILM para usar esa regla. Consulta "Crear regla de ILM" y "Crear política de ILM".

Seguridad para clientes S3 en StorageGRID

Las cuentas de inquilino de StorageGRID usan aplicaciones de cliente S3 para guardar

datos de objetos en StorageGRID. Deberías revisar las medidas de seguridad implementadas para las aplicaciones de cliente.

${post_edited_translations.segment}

La siguiente lista resume cómo se implementa la seguridad en la API de REST de S3:

${post_edited_translations.segment}
${post_edited_translations.segment}

${post_edited_translations.segment}
Certificado de servidor X.509 firmado por la CA del sistema o certificado de servidor personalizado proporcionado por el administrador

${post_edited_translations.segment}
${post_edited_translations.segment}

Autorización del cliente
La titularidad del bucket y todas las políticas de control de acceso aplicables

Cómo StorageGRID proporciona seguridad para las aplicaciones cliente

Las aplicaciones cliente de S3 pueden conectarse al servicio Load Balancer en los nodos de Gateway o Admin, o directamente a los nodos de Storage.

- Los clientes que se conectan al servicio de equilibrador de carga pueden usar HTTPS o HTTP, según cómo "${post_edited_translations.segment}".

  HTTPS ofrece una comunicación segura cifrada mediante TLS y es la opción recomendada. Debes asociar un certificado de seguridad al punto final.

  ${post_edited_translations.segment}

- Los clientes que se conectan a los nodos de almacenamiento también pueden usar HTTPS o HTTP.

  HTTPS es la opción predeterminada y se recomienda.

  HTTP proporciona una comunicación menos segura y sin cifrar, pero puede usarse opcionalmente "habilitado" para grids que no sean de producción o de prueba.

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Los clientes deben proporcionar "Encabezados de autenticación HTTP" a StorageGRID para realizar operaciones de la API de REST.

${post_edited_translations.segment}

En todos los casos, las aplicaciones cliente pueden establecer conexiones TLS utilizando ya sea un certificado de servidor personalizado cargado por el administrador de la grid o un certificado generado por el sistema StorageGRID:

- Cuando las aplicaciones cliente se conectan al servicio de equilibrador de carga, utilizan el certificado que se ha configurado para el punto final del equilibrador de carga. Cada punto final del equilibrador de carga

tiene su propio certificado—ya sea 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.

Consulta "Aspectos a tener en cuenta para el 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 crearon para los nodos de almacenamiento al instalar el sistema StorageGRID (que están firmados por la entidad de certificación del sistema) o un único certificado de servidor personalizado proporcionado para el grid por un administrador de grid. Consulta "${post_edited_translations.segment}".

Los clientes deben configurarse para que confíen en la autoridad de certificación que haya firmado el certificado que utilicen para establecer conexiones TLS.

${post_edited_translations.segment}

El sistema StorageGRID admite un conjunto de conjuntos de cifrado que las aplicaciones cliente pueden utilizar al establecer una sesión TLS. Para configurar los cifrados, ve a **Configuración** > **Seguridad** > **Ajustes de seguridad** y selecciona **Políticas de TLS y SSH**.

Versiones compatibles de TLS

${post_edited_translations.segment}

SSLv3 y TLS 1.1 (o versiones anteriores) ya no son compatibles.

Usa el asistente de configuración de S3

Consideraciones y requisitos del asistente de configuración de StorageGRID S3

Puedes utilizar el asistente de configuración de S3 para configurar StorageGRID como sistema de almacenamiento de objetos para una aplicación S3.

Cuándo utilizar el asistente de configuración de S3

El asistente de configuración de S3 te guía a lo largo de cada paso de la configuración de StorageGRID para su uso con una aplicación S3. Como parte de completar el asistente, descargas archivos que puedes usar para introducir valores en la aplicación S3. Utiliza el asistente para configurar tu sistema más rápido y para asegurarte de que tus ajustes cumplen con las mejores prácticas de StorageGRID.

Si tienes la "Permiso de acceso raíz", puedes completar el asistente de configuración de S3 cuando empieces a usar StorageGRID Grid Manager, o puedes acceder y completar el asistente en cualquier momento después. Dependiendo de tus necesidades, también puedes configurar manualmente algunos o todos los elementos necesarios y luego usar el asistente para reunir los valores que necesita una aplicación S3.

Antes de utilizar el asistente

Antes de utilizar el asistente, comprueba que has cumplido estos requisitos previos.

Obtener direcciones IP y configurar interfaces VLAN

Si vas a configurar un grupo de alta disponibilidad (HA), ya sabes a qué nodos se conectará la aplicación S3 y qué red StorageGRID se utilizará. También sabes qué valores debes introducir para el CIDR de la subred, la dirección IP de la puerta de enlace y las direcciones IP virtuales (VIP).

Si tienes previsto usar una LAN virtual para segregar el tráfico de la aplicación S3, ya configuraste la interfaz de la VLAN. Consulta "Configurar interfaces VLAN".

Configura la federación de identidades y el inicio de sesión único (SSO)

Si tienes previsto usar la federación de identidades o el inicio de sesión único (SSO) para tu sistema StorageGRID, ya habrás habilitado estas funciones. También sabes qué grupo federado debe tener acceso a raíz para la cuenta de inquilino que usará la aplicación S3. Consulta "Usa la federación de identidades" y "${post_edited_translations.segment}".

Obtener y configurar nombres de dominio

Ya sabes qué nombre de dominio completo (FQDN) debes usar para StorageGRID. Las entradas del servidor de nombres (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad (HA) que crees usando el asistente.

Si tienes pensado utilizar solicitudes de S3 de tipo virtual hosted-style, debes tener "Nombres de dominio de los endpoints S3 configurados". Se recomienda utilizar solicitudes de tipo virtual hosted-style.

Revisa los requisitos del equilibrador de carga y del certificado de seguridad

Si tienes previsto utilizar el equilibrador de carga de StorageGRID, ya revisaste las consideraciones generales para el equilibrio de carga. Tienes los certificados que vas a cargar o los valores que necesitas para generar un certificado.

Si tienes previsto usar un endpoint de un equilibrador de carga externo (de terceros), tienes el nombre de dominio completo (FQDN), el puerto y el certificado para ese equilibrador de carga.

Configura cualquier conexión de federación de redes

Si deseas permitir que el inquilino de S3 clone los datos de la cuenta y replique los objetos del bucket en otra grid mediante una conexión de federación de grids, comprueba lo siguiente antes de iniciar el asistente de configuración:

- Tienes "configuraste la conexión de federación de grid".
- El estado de la conexión es **Conectado**.
- Tienes permiso de acceso root.

Accede y completa el asistente de configuración de S3 en StorageGRID

Puedes 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 necesita la aplicación para acceder a un bucket de StorageGRID y guardar objetos.

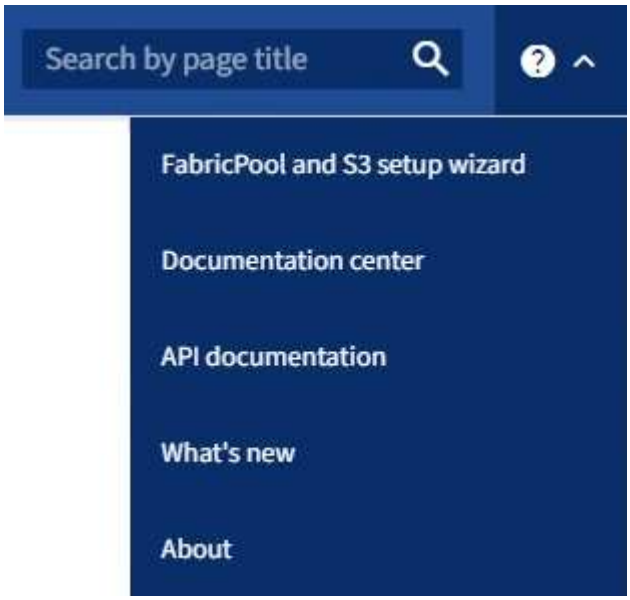
Antes de empezar

- Tienes el "Permiso de acceso raíz".
- Has revisado la "${post_edited_translations.segment}" para usar el asistente.

Accede al asistente

Pasos

1. Inicia sesión en Grid Manager usando una "navegador web compatible" cuenta.
2. Si aparece en el panel de control el banner **FabricPool and S3 setup wizard**, selecciona el enlace que aparece en el banner. Si el banner ya no aparece, selecciona el icono de ayuda de la barra de encabezado en el Grid Manager y selecciona **FabricPool and S3 setup wizard**.



3. En la sección de aplicación S3 de la página del asistente de configuración de FabricPool y S3, selecciona **Configurar ahora**.

Paso 1 de 6: Configura el grupo de alta disponibilidad

Un grupo de alta disponibilidad (HA) es un conjunto de nodos que contienen, cada uno de ellos, el servicio StorageGRID Load Balancer. Un grupo de alta disponibilidad (HA) puede contener Gateway Nodes, Admin Nodes o ambos.

Puedes usar un grupo HA para ayudar a mantener disponibles las conexiones de datos S3. Si la interfaz activa en el grupo HA falla, una interfaz de respaldo puede gestionar la carga de trabajo con poco impacto en las operaciones de S3.

Para obtener más información sobre esta tarea, consulta "Gestiona grupos de alta disponibilidad".

Pasos

1. Si tienes pensado utilizar un equilibrador de carga externo, no es necesario que crees un grupo de alta disponibilidad. Selecciona **Omitir este paso** y ve a Paso 2 de 6: Configura el endpoint del balanceador de carga.
2. Para utilizar el equilibrador de carga de StorageGRID, puedes crear un nuevo grupo de alta disponibilidad (HA) o usar un grupo de alta disponibilidad (HA) existente.

Crear grupo de alta disponibilidad

a. Para crear un nuevo grupo de alta disponibilidad, selecciona **Crear grupo de alta disponibilidad**.

b. En el paso **Introducir datos**, rellena los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo de alta disponibilidad.
Descripción (opcional)	La descripción de este grupo de HA.

c. En el paso **Add interfaces**, selecciona las interfaces de nodo que quieres usar en este grupo de alta disponibilidad.

${post_edited_translations.segment}

Puedes seleccionar uno o varios nodos, pero solo puedes seleccionar una interfaz por cada nodo.

d. Para el paso **Priorizar interfaces**, determina la interfaz principal y cualquier interfaz de respaldo para este grupo de alta disponibilidad.

Arrastra las filas para cambiar los valores de la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa salvo que se produzca un fallo.

Si el grupo de alta disponibilidad (HA) incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se transfieren a la primera interfaz de respaldo según el orden de prioridad. Si esa interfaz falla, las direcciones VIP se transfieren a la siguiente interfaz de respaldo y así sucesivamente. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz disponible con mayor prioridad.

e. En el paso **Introducir direcciones IP**, completa los siguientes campos.

Campo	Descripción
CIDR de la subred	La dirección de la subred VIP en notación CIDR — una dirección IPv4 seguida de una barra y la longitud de la subred (0-32). La dirección de red no debe tener ningún bit de host activado. 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 se encuentran en la misma subred que las direcciones VIP de StorageGRID, introduce la dirección IP de la puerta de enlace local de la VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred de la VIP.

Campo	Descripción
Dirección IP virtual	Introduce al menos una y no más de diez direcciones VIP para la interfaz activa del grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. Opcionalmente, puedes especificar direcciones IPv4 e IPv6 adicionales.

f. Selecciona **Crear grupo de alta disponibilidad** y luego selecciona **Finalizar** para volver al asistente de configuración de S3.

g. Selecciona **Continuar** para pasar al paso del equilibrador de carga.

Usa el grupo de alta disponibilidad existente

a. Para utilizar un grupo de alta disponibilidad ya existente, selecciona el nombre del grupo en la opción **Select an HA group**.

b. Selecciona **Continuar** para pasar al paso del equilibrador de carga.

Paso 2 de 6: Configura el endpoint del balanceador de carga

StorageGRID utiliza un equilibrador de carga para gestionar la carga de trabajo de las aplicaciones cliente. El equilibrio de carga maximiza la velocidad y la capacidad de conexión entre varios Storage Nodes.

Puedes utilizar el servicio StorageGRID Load Balancer, que está disponible en todos los nodos Gateway y Admin, o puedes conectarte a un equilibrador de carga externo (de terceros). Se recomienda usar el load balancer de StorageGRID.

Para obtener más información sobre esta tarea, consulta "Aspectos a tener en cuenta para el equilibrio de carga".

Para usar el servicio StorageGRID Load Balancer, selecciona la pestaña **StorageGRID load balancer** y luego crea o selecciona el endpoint del load balancer que quieras usar. Para usar un load balancer externo, selecciona la pestaña **External load balancer** y proporciona los detalles sobre el sistema que ya configuraste.

Crear punto final

Pasos

1. Para crear un punto de conexión de equilibrador de carga, selecciona **Crear punto de conexión**.
2. En el paso **Introducir los datos del punto final**, rellena los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el endpoint.
Puerto	El puerto de StorageGRID que deseas utilizar para el equilibrio de carga. Este campo tiene por defecto el valor 10433 para el primer punto final que crees, pero puedes introducir cualquier puerto externo que no esté en uso. Si introduces 80 o 443, el punto final solo se configura en los nodos de Gateway, porque estos puertos están reservados en los nodos de Admin. **Nota:** No se permiten los puertos utilizados por otros servicios de la red. Consulta "Puertos internos de StorageGRID".
Tipo de cliente	Debe ser **S3**.
Protocolo de red	Selecciona **HTTPS**. **Nota**: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

3. En el paso **Seleccionar modo de enlace**, especifica el modo de enlace. El modo de enlace controla cómo se accede al endpoint utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final usando la dirección IP de cualquier Gateway Node o Admin Node, la dirección IP virtual (VIP) de cualquier grupo HA en cualquier red, o el FQDN correspondiente. ${post_edited_translations.segment}
Direcciones IP virtuales de los grupos de alta disponibilidad	Los clientes deben utilizar una dirección IP virtual (o el nombre de dominio completo correspondiente) de un grupo de alta disponibilidad para acceder a este endpoint. Todos los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que selecciones para los puntos finales no se solapen.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o los FQDN correspondientes) de las interfaces de los nodos seleccionados para acceder a este endpoint.

Modo	Descripción
Tipo de nodo	En función del tipo de nodo que selecciones, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier Admin Node o la dirección IP (o el FQDN correspondiente) de cualquier Gateway Node para acceder a este endpoint.

4. Para el paso de acceso del inquilino, selecciona una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (por defecto)	${post_edited_translations.segment}
Permitir inquilinos seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este endpoint para acceder a sus buckets.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este endpoint para acceder a sus buckets. El resto de inquilinos sí pueden utilizar este endpoint.

5. En el paso **Adjuntar certificado**, selecciona una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utiliza esta opción para cargar un certificado de servidor firmado por una CA, la clave privada del certificado y, opcionalmente, el paquete de CA.
Generar certificado	Utiliza esta opción para generar un certificado autofirmado. Consulta "Configura los puntos de conexión del equilibrador de carga" para ver los detalles de qué debes introducir.
Usa el certificado S3 de StorageGRID	Utiliza esta opción solo si ya has subido o generado una versión personalizada del certificado global de StorageGRID. Consulta "Configura los certificados de la API de S3" para obtener más información.

6. Selecciona **Finalizar** para volver al asistente de configuración de S3.
7. Selecciona **Continuar** para pasar al paso del inquilino y el bucket.

> Los cambios en el certificado de un endpoint pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utiliza el punto de conexión del equilibrador de carga existente

Pasos

1. Para utilizar un endpoint ya existente, selecciona su nombre en **Selecciona un endpoint del balanceador de carga**.

2. Selecciona **Continuar** para pasar al paso del inquilino y el bucket.

Utilizar un equilibrador de carga externo

Pasos

1. Para utilizar un equilibrador de carga externo, completa los siguientes campos.

Campo	Descripción
FQDN	El nombre de dominio completo (FQDN) del equilibrador de carga externo.
Puerto	El número de puerto que utilizará la aplicación S3 para conectarse al equilibrador de carga externo.
Certificado	Copia el certificado del servidor del equilibrador de carga externo y pégalo en este campo.

2. Selecciona **Continuar** para pasar al paso del inquilino y el bucket.

Paso 3 de 6: crea un inquilino y un bucket

Un inquilino es una entidad que puede utilizar aplicaciones de S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, buckets, objetos y un conjunto específico de capacidades.

Un bucket es un contenedor que se utiliza para almacenar los objetos y los metadatos de un inquilino. Aunque los inquilinos pueden tener muchos buckets, el asistente te ayuda a crear un inquilino y un bucket de la forma más rápida y sencilla. Si necesitas añadir buckets o configurar opciones más adelante, puedes utilizar el Tenant Manager.

Para obtener más información sobre esta tarea, consulta "Crear cuenta de inquilino" y "Crear un bucket de S3".

Pasos

1. Introduce un nombre para la cuenta de inquilino.

   Los nombres de los inquilinos no tienen por qué ser únicos. Al crear la cuenta de un inquilino, esta recibe un identificador de cuenta numérico único.

2. Define el acceso a raíz para la cuenta de inquilino, en función de si tu sistema StorageGRID utiliza "federación de identidades", "inicio de sesión único (SSO)" o ambos.

Opción	Haz esto
Si la federación de identidades no está habilitada	${post_edited_translations.segment}

Opción	Haz esto
${post_edited_translations.segment}	a. Selecciona un grupo federado ya existente para que el inquilino tenga "Permiso de acceso raíz". b. Si lo deseas, indica la contraseña que se usará al iniciar sesión en el tenant como usuario raíz local.
${post_edited_translations.segment}	Selecciona un grupo federado existente para que el inquilino tenga "Permiso de acceso raíz". Ningún usuario local puede iniciar sesión.

3. Si quieres que el asistente cree el ID de la clave de acceso y la clave de acceso secreta para el usuario raíz, selecciona **Crear automáticamente la clave de acceso S3 del usuario raíz**.

   Selecciona esta opción si el único usuario del inquilino va a ser el usuario raíz. Si otros usuarios van a utilizar este inquilino, "usar Tenant Manager" para configurar claves y permisos.

4. Si quieres crear un bucket para este inquilino ahora, selecciona **Crear bucket para este inquilino**.

   Si S3 Object Lock está habilitado para la grid, el bucket creado en este paso no tiene S3 Object Lock habilitado. Si necesitas usar un bucket con S3 Object Lock para esta aplicación de S3, no selecciones crear un bucket ahora. En su lugar, usa Tenant Manager para "crear el bucket" más adelante.

   a. Introduce el nombre del bucket que utilizará la aplicación S3. Por ejemplo, `s3-bucket`.

      No puedes cambiar el nombre del bucket después de crearlo.

   b. Selecciona la **región** para este depósito.

      Utiliza la región predeterminada (`us-east-1`) a menos que tengas previsto utilizar ILM en el futuro para filtrar objetos en función de la región del bucket.

5. Selecciona **Crear y continuar**.

Paso 4 de 6: descargar datos

En el paso de descarga de datos, puedes descargar uno o dos archivos para guardar los detalles de lo que acabas de configurar.

Pasos

1. Si has seleccionado **Crear automáticamente la clave de acceso S3 del usuario raíz**, haz una o ambas de las siguientes cosas:
   - Selecciona **Descargar claves de acceso** para descargar un archivo `.csv` que contiene el nombre de la cuenta del inquilino, el ID de la clave de acceso y la clave de acceso secreta.
   - Selecciona el icono de copiar ( ) para copiar el ID de la clave de acceso y la clave secreta de acceso en el portapapeles.
2. Selecciona **Descargar valores de configuración** para descargar un `.txt` archivo que contiene la configuración del punto final del balanceador de carga, el inquilino, el bucket y el usuario raíz.
3. Guarda esta información en un lugar seguro.

No cierres esta página hasta que hayas copiado ambas claves de acceso. Las claves dejarán de estar disponibles una vez que cierres esta página. Asegúrate de guardar esta información en un lugar seguro porque puede usarse para obtener datos de tu sistema StorageGRID.

4. Si se te solicita, marca la casilla para confirmar que has descargado o copiado las claves.
5. Selecciona **Continuar** para ir al paso de reglas y políticas de ILM.

Paso 5 de 6: revisa la regla de ILM y la política de ILM para S3

Las reglas de gestión del ciclo de vida de la información (ILM) controlan la ubicación, la duración y el comportamiento de ingesta de todos los objetos en tu sistema StorageGRID. La política de ILM incluida con StorageGRID crea dos copias replicadas de todos los objetos. Esta política está vigente hasta que actives al menos una nueva política.

Pasos

1. Revisa la información que aparece en la página.
2. Si deseas añadir instrucciones específicas para los objetos que pertenecen al nuevo inquilino o bucket, crea una nueva regla y una nueva política. Consulta "Crear regla de ILM" y "Usa políticas de ILM".
3. Selecciona **He revisado estos pasos y entiendo lo que tengo que hacer**.
4. Marca la casilla de verificación para indicar que sabes qué hacer a continuación.
5. Selecciona **Continuar** para ir a **Resumen**.

Paso 6 de 6: resumen de revisión

Pasos

1. Revisa el resumen.
2. Toma nota de los detalles de los siguientes pasos, en los que se describe la configuración adicional que podría ser necesaria antes de conectarte al cliente S3. Por ejemplo, al seleccionar **Sign in as root** vas al Tenant Manager, donde puedes añadir usuarios del tenant, crear buckets adicionales y actualizar la configuración de los buckets.
3. Selecciona **Finalizar**.
4. Configura la aplicación usando el archivo que descargaste de StorageGRID o los valores que obtuviste manualmente.

Gestiona grupos de alta disponibilidad

Conoce los grupos de alta disponibilidad de StorageGRID

${post_edited_translations.segment}

Puedes agrupar las interfaces de red de varios nodos de administración y de puerta de enlace en un grupo de alta disponibilidad (HA). Si la interfaz activa del grupo de HA falla, una interfaz de respaldo puede gestionar la carga de trabajo.

Cada grupo de HA proporciona acceso a los servicios compartidos en los nodos seleccionados.

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

- Un grupo de alta disponibilidad (HA) que incluya únicamente dispositivos de servicios y nodos de software basados en VMware puede proporcionar conexiones de alta disponibilidad para "${post_edited_translations.segment}". Se recomienda usar grupos de alta disponibilidad (HA) cuando usas S3 Select, pero no es obligatorio.

¿Cómo creas un grupo de alta disponibilidad?

1. Selecciona una interfaz de red para uno o varios nodos de administración o nodos de puerta de enlace. Puedes utilizar una interfaz de red Grid Network (eth0), una interfaz Client Network (eth2), una interfaz VLAN o una interfaz de acceso que hayas añadido al nodo.

   > ⓘ No puedes añadir una interfaz a un grupo de alta disponibilidad si tiene una dirección IP asignada por DHCP.

2. Tú especificas una interfaz para que sea la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra un fallo.
3. Tú determinas el orden de prioridad para cualquier interfaz de Backup.
4. Asignas entre una y diez direcciones IP virtuales (VIP) al grupo. Las aplicaciones de los clientes pueden usar cualquiera de estas direcciones VIP para conectarse a StorageGRID.

Para ver las instrucciones, consulta "Configurar grupos de alta disponibilidad".

¿Qué es la interfaz activa?

Durante el funcionamiento normal, todas las direcciones VIP del grupo de alta disponibilidad (HA) se añaden a la interfaz primaria, que es la primera interfaz en el orden de prioridad. Mientras la interfaz primaria siga estando disponible, se utiliza cuando los clientes se conectan a cualquier dirección VIP del grupo. Es decir, durante el funcionamiento normal, la interfaz primaria es la interfaz "activa" del grupo.

Del mismo modo, durante el funcionamiento normal, cualquier interfaz de menor prioridad del grupo de alta disponibilidad actúa como interfaz «de reserva». Estas interfaces de reserva no se utilizan a menos que la interfaz principal (la que está activa en ese momento) deje de estar disponible.

Ver el estado actual del grupo de alta disponibilidad de un nodo

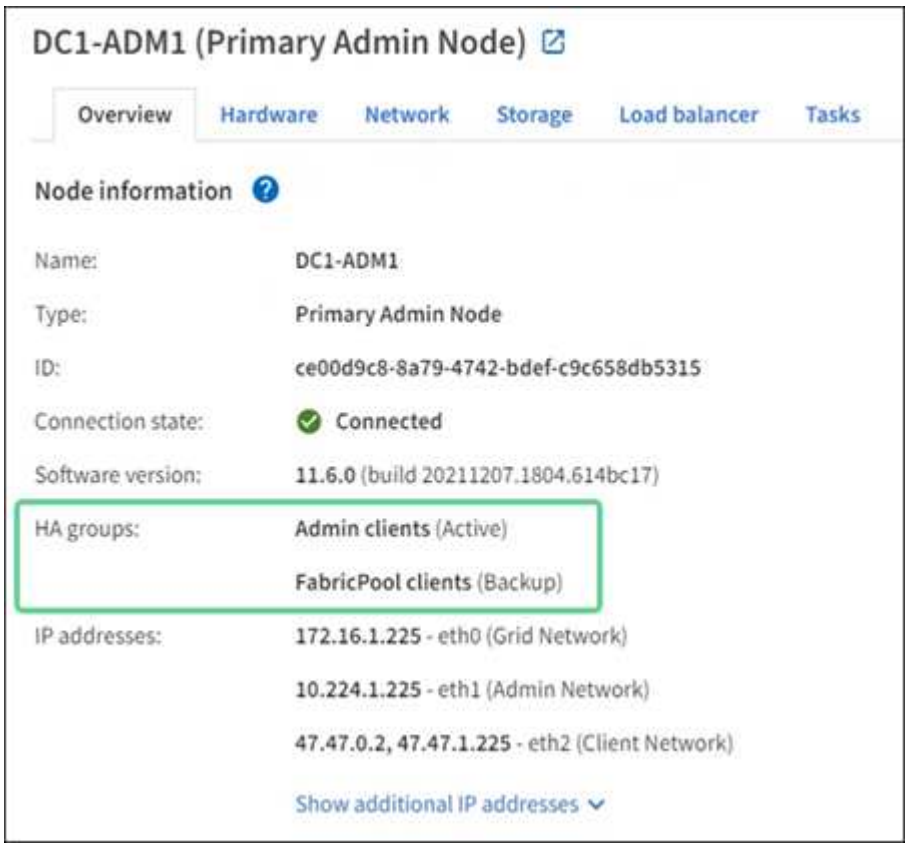
Para comprobar si un nodo está asignado a un grupo de alta disponibilidad y determinar su estado actual, selecciona **Nodos** > ***nodo***.

Si la pestaña **Resumen** incluye una entrada para **HA groups**, el nodo está asignado a los HA groups que aparecen en la lista. El valor que aparece tras el nombre del grupo es el estado actual del nodo en el HA group:

- **Activo**: El grupo de alta disponibilidad está alojado actualmente en este nodo.
- **Reserva**: El grupo de alta disponibilidad no está utilizando este nodo en este momento; esta es una interfaz de reserva.
- **Detenido**: El grupo de alta disponibilidad no se puede alojar en este nodo porque el servicio de alta disponibilidad (keepalived) se ha detenido manualmente.
- **Error**: El grupo de alta disponibilidad no se puede alojar en este nodo debido a una o varias de las siguientes causas:
  - 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 para el grupo de clientes Admin y una interfaz de respaldo para el grupo de clientes FabricPool.



¿Qué ocurre cuando falla la interfaz activa?

La interfaz que actualmente aloja las direcciones VIP es la interfaz activa. Si el grupo de alta disponibilidad (HA) incluye más de una interfaz y la interfaz activa falla, las direcciones VIP se trasladan a la primera interfaz de respaldo disponible según el orden de prioridad. Si esa interfaz falla, las direcciones VIP se trasladan a la siguiente interfaz de respaldo disponible, y así sucesivamente.

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

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

> Es posible que la conmutación por error no se active debido a fallos de red externos al nodo que aloja la interfaz activa. Del mismo modo, la conmutación por error no se activa por los servicios de Grid Manager o Tenant Manager.

El proceso de conmutación por error suele durar solo unos segundos y es lo suficientemente rápido como

para que las aplicaciones cliente apenas noten el impacto y puedan seguir funcionando con normalidad mediante los mecanismos habituales de reintento.

${post_edited_translations.segment}

Cómo los grupos de HA de StorageGRID proporcionan alta disponibilidad

Puedes utilizar grupos de alta disponibilidad (HA) 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 Grid Manager o al Tenant Manager.
- Un grupo de alta disponibilidad puede proporcionar conexiones de datos altamente disponibles para los clientes de S3.
- Un grupo HA que contiene solo una interfaz te permite proporcionar muchas direcciones VIP y configurar explícitamente direcciones IPv6.

Un grupo de alta disponibilidad (HA) solo puede ofrecer alta disponibilidad si todos los nodos incluidos en el grupo prestan los mismos servicios. Al crear un grupo de alta disponibilidad, añade interfaces de los tipos de nodos que prestan los servicios que necesitas.

- **Nodos de administración**: Incluye el servicio de equilibrador de carga y habilita el acceso al Grid Manager o al Tenant Manager.
- **Nodos de puerta de enlace**: Incluyen el servicio de Load Balancer.

Objetivo del grupo HA	Agrega nodos de este tipo al grupo de alta disponibilidad
Acceso a Grid Manager	• Nodo de administración principal (**Principal**) • Nodos de administración no primarios **Nota:** El nodo de administración principal debe ser la interfaz principal. Algunos procedimientos de mantenimiento solo pueden realizarse desde el nodo de administración principal.
Acceso solo a Tenant Manager	• Nodos de administración primarios o no primarios
Acceso de cliente S3—servicio de equilibrador de carga	• Nodos de administración • Nodos de puerta de enlace
Acceso de cliente S3 para "S3 Select"	• Dispositivos de servicios • Nodos de software basados en VMware **Nota**: Se recomienda utilizar grupos HA al emplear S3 Select, aunque no es obligatorio.

Limitaciones de usar grupos HA con Grid Manager o Tenant Manager

Si falla el servicio Grid Manager o Tenant Manager, no se activa la conmutación por error del grupo HA.

Si has iniciado sesión en Grid Manager o en Tenant Manager cuando se produce una conmutación por error,

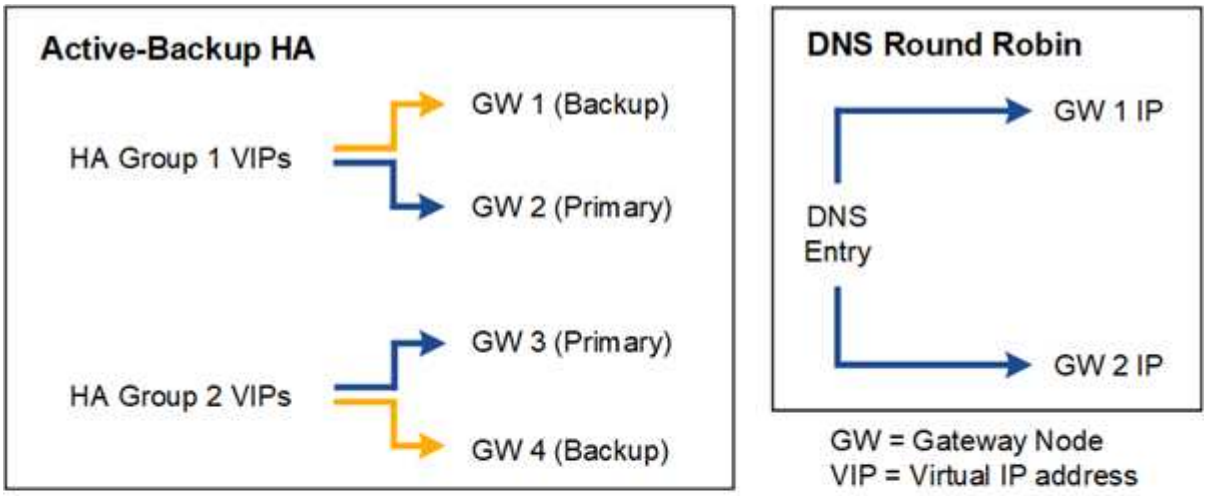
se cerrará tu sesión y debes volver a iniciar sesión para reanudar tu tarea.

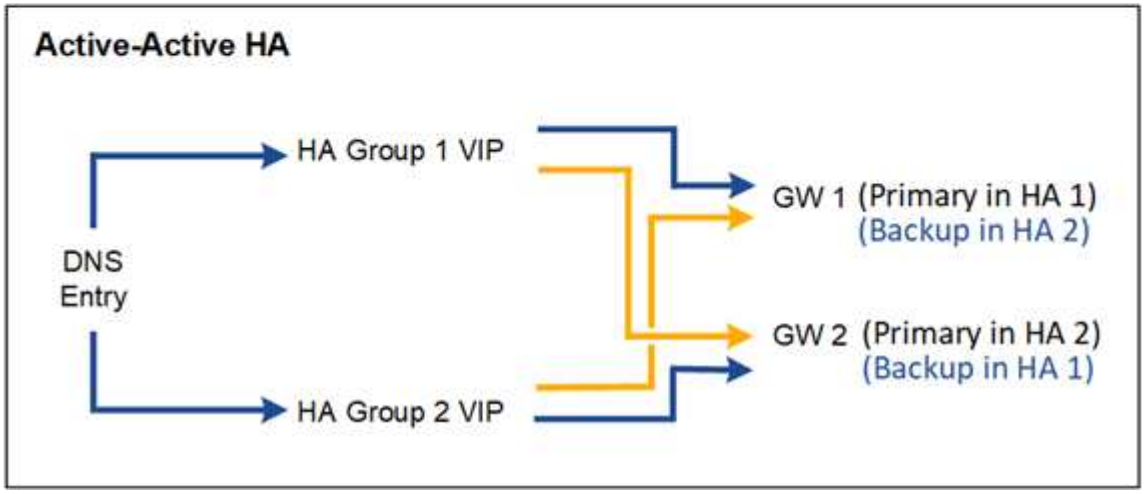
Algunos procedimientos de mantenimiento no se pueden llevar a cabo cuando el nodo de administración principal no está disponible. Durante la conmutación por error, puedes usar Grid Manager para supervisar tu sistema StorageGRID.

Opciones de configuración para los grupos de alta disponibilidad de StorageGRID

Los siguientes diagramas ofrecen ejemplos de diferentes formas en que puedes configurar grupos de alta disponibilidad (HA). Cada opción tiene ventajas y desventajas.

${post_edited_translations.segment}





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

Configuración	Ventajas	Desventajas
HA activo-backup	• Gestionado por StorageGRID sin dependencias externas. • Conmutación rápida por error.	• Solo un nodo de un grupo de alta disponibilidad está activo. Al menos un nodo por grupo de alta disponibilidad estará inactivo.

Configuración	Ventajas	Desventajas
DNS Round Robin	• Aumento del rendimiento total. • No hay hosts inactivos.	• Conmutación por error lenta, que podría depender del comportamiento del cliente. • Requiere configuración de hardware fuera de StorageGRID. • Es necesario que el cliente realice una comprobación del estado.
HA activo-activo	• ${post_edited_translations.segment} • Alto rendimiento agregado que escala con el número de grupos de alta disponibilidad. • Conmutación rápida por error.	• Más complicado de configurar. • Requiere configuración de hardware fuera de StorageGRID. • Es necesario que el cliente realice una comprobación del estado.

Configura grupos de alta disponibilidad en StorageGRID

Puedes configurar grupos de alta disponibilidad (HA) para proporcionar acceso de alta disponibilidad a los servicios en los nodos de administración o los nodos de puerta de enlace.

${post_edited_translations.segment}

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".
- Si tienes previsto utilizar una interfaz VLAN en un grupo de alta disponibilidad (HA), ya has creado la interfaz VLAN. Consulta "Configurar interfaces VLAN".
- Si tienes previsto utilizar una interfaz de acceso para un nodo de un grupo de alta disponibilidad, ya creaste la interfaz:
  - **Linux (antes de instalar el nodo)**: "Crear archivos de configuración de nodos"
  - **Linux (después de instalar el nodo)**: "Agrega interfaces trunk o de acceso a un nodo"
  - **VMware (tras instalar el nodo)**: "Agrega interfaces trunk o de acceso a un nodo"

«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita "Herramienta de matriz de interoperabilidad (IMT) de NetApp".

Crear un grupo de alta disponibilidad

Cuando creas un grupo de alta disponibilidad, seleccionas una o más interfaces y las organizas por orden de prioridad. Luego, asignas una o más direcciones VIP al grupo.

Una interfaz debe pertenecer a un Gateway Node o a un Admin Node para poder incluirse en un grupo de HA. Un grupo de HA solo puede usar una interfaz para un nodo determinado; sin embargo, puedes usar otras interfaces del mismo nodo en otros grupos de HA.

Accede al asistente

Pasos

1. ${post_edited_translations.segment}
2. Selecciona **Crear**.

${post_edited_translations.segment}

Pasos

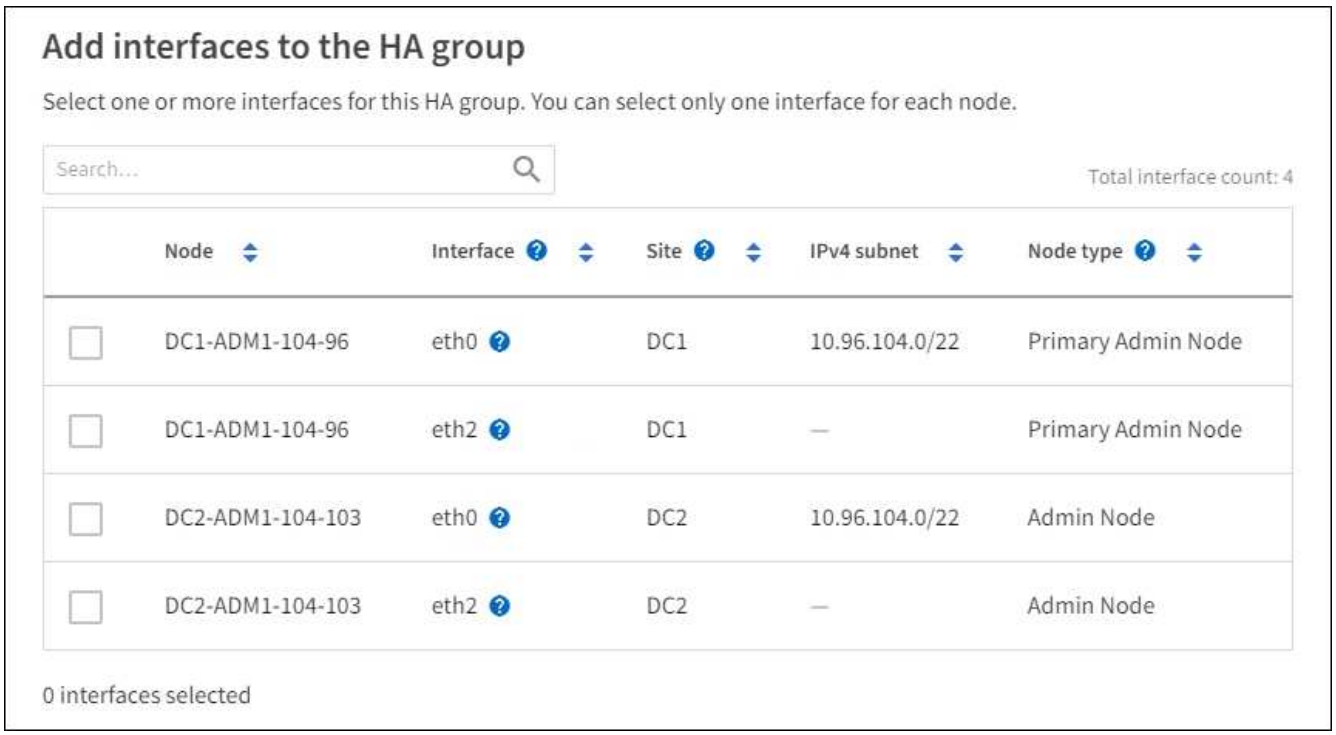
1. Introduce un nombre único para el grupo de alta disponibilidad.
2. Si lo deseas, introduce una descripción para el grupo de alta disponibilidad.
3. Selecciona **Continuar**.

${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

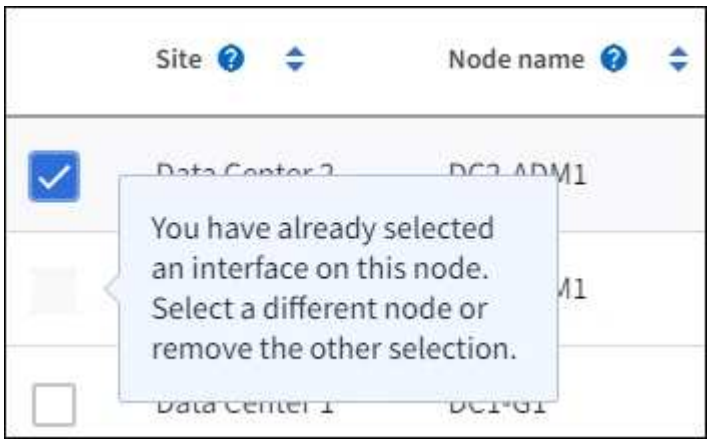


> Una vez creada la interfaz VLAN, espera hasta 5 minutos para que la nueva interfaz aparezca en la tabla.

${post_edited_translations.segment}

- Debes seleccionar al menos una interfaz.
- Solo puedes seleccionar una interfaz por nodo.
- Si el grupo HA está destinado a la protección HA de los servicios de Admin Node, que incluyen Grid Manager y Tenant Manager, selecciona únicamente las interfaces en los Admin Nodes.

- ${post_edited_translations.segment}
- Si seleccionas interfaces en diferentes tipos de nodos, aparecerá una nota informativa. Se te recuerda que, si ocurre una conmutación por error, es posible que los servicios proporcionados por el nodo que estaba activo anteriormente no estén disponibles en el nuevo nodo activo. Por ejemplo, un nodo Gateway de respaldo no puede proporcionar protección HA de los servicios del nodo Admin. De manera similar, un nodo Admin de respaldo no puede realizar todos los procedimientos de mantenimiento que puede proporcionar el nodo Admin principal.
- Si no puedes seleccionar una interfaz, su casilla de verificación estará desactivada. La descripción emergente proporciona más información.



- No puedes seleccionar una interfaz si el valor de su subred o su puerta de enlace entra en conflicto con el de otra interfaz seleccionada.
- ${post_edited_translations.segment}

2. Selecciona **Continuar**.

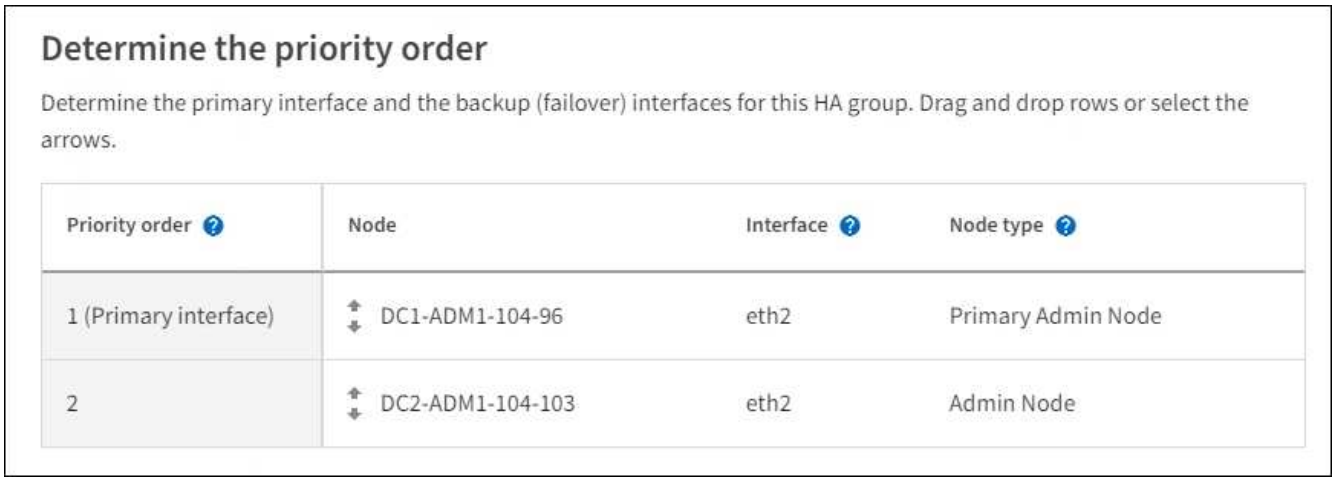
Determina el orden de prioridad

Si el grupo de HA incluye más de una interfaz, puedes determinar cuál es la interfaz primaria y cuáles son las interfaces de respaldo (conmutación por error). Si la interfaz primaria falla, las direcciones VIP se trasladan a la interfaz disponible que tenga la mayor prioridad. Si esa interfaz falla, las direcciones VIP se trasladan a la siguiente interfaz disponible con mayor prioridad, y así sucesivamente.

Pasos

1. ${post_edited_translations.segment}

   La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa salvo que se produzca un fallo.



Si el grupo de HA proporciona acceso al Grid Manager, debes seleccionar una interfaz en el nodo de administración primario para que sea la interfaz primaria. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración primario.

2. Selecciona **Continuar**.

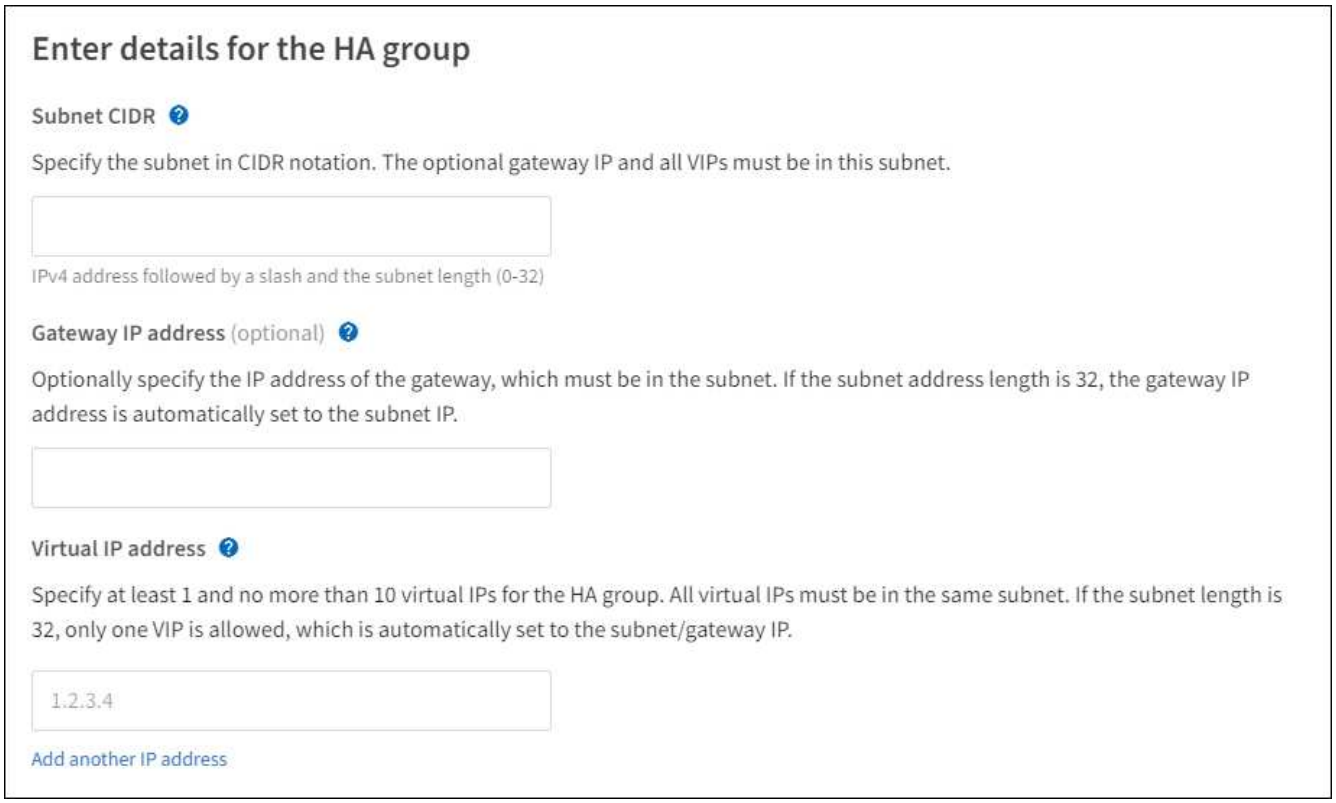
Introduce direcciones IP

Pasos

1. En el campo **CIDR de la subred**, especifica la subred VIP en notación CIDR: una dirección IPv4 seguida de una barra y la longitud de la subred (0-32).

   La dirección de red no debe tener ningún bit de host activado. Por ejemplo, `192.16.0.0/22`.

   Si utilizas un prefijo de 32 bits, la dirección de red VIP también sirve como dirección de puerta de enlace y dirección VIP.



2. Si lo deseas, en caso de que algún cliente administrativo o de inquilino de S3 vaya a acceder a estas direcciones VIP desde una subred diferente, introduce la **dirección IP de la puerta de enlace**. La dirección de la puerta de enlace debe estar dentro de la subred VIP.

   ${post_edited_translations.segment}

3. Introduce al menos una y no más de diez direcciones VIP para la interfaz activa del 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.

   Debes proporcionar al menos una dirección IPv4. Si lo deseas, puedes especificar direcciones IPv4 e IPv6 adicionales.

4. Selecciona **Crear grupo de alta disponibilidad** y selecciona **Finalizar**.

   Se ha creado el grupo HA y ya puedes utilizar las direcciones IP virtuales configuradas.

Próximos pasos

Si vas a utilizar este grupo de alta disponibilidad (HA) para el equilibrio de carga, crea un punto de conexión del equilibrador de carga para determinar el puerto y el protocolo de red y para asociar los certificados necesarios. Consulta "Configura los puntos de conexión del equilibrador de carga".

Editar un grupo de alta disponibilidad

${post_edited_translations.segment}

Por ejemplo, es posible que tengas que editar un grupo de alta disponibilidad (HA) si quieres eliminar el nodo asociado con una interfaz seleccionada en un procedimiento de decomisionar un sitio o nombre de nodo.

Pasos

1. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

2. Marca la casilla correspondiente al grupo de alta disponibilidad que quieras editar.
3. ${post_edited_translations.segment}
   - Selecciona **Acciones** > **Editar dirección IP virtual** para añadir o eliminar direcciones VIP.
   - Selecciona **Acciones** > **Editar grupo de alta disponibilidad** para actualizar el nombre o la descripción del grupo, añadir o eliminar interfaces, cambiar el orden de prioridad o añadir o eliminar direcciones VIP.
4. Si has seleccionado **Editar dirección IP virtual**:
   a. Actualiza las direcciones IP virtuales del grupo de alta disponibilidad.
   b. Selecciona **Guardar**.
   c. Selecciona **Finalizar**.
5. Si has seleccionado **Editar grupo de alta disponibilidad**:
   a. Opcionalmente, actualiza el nombre o la descripción del grupo.
   b. Si lo deseas, selecciona o desmarca las casillas para añadir o eliminar interfaces.

      Si el grupo HA proporciona acceso al Grid Manager, debes seleccionar una interfaz en el nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo pueden realizarse desde el nodo de administración principal.

   c. Si lo deseas, arrastra las filas para cambiar el orden de prioridad de la interfaz principal y de cualquier interfaz de respaldo de este grupo de alta disponibilidad.
   d. Opcionalmente, actualiza las direcciones IP virtuales.
   e. ${post_edited_translations.segment}

Eliminar un grupo de alta disponibilidad

${post_edited_translations.segment}

No puedes eliminar un grupo de alta disponibilidad si está vinculado a un punto final del equilibrador de carga. Para eliminar un grupo de alta disponibilidad, debes quitarlo de cualquier punto final del equilibrador de carga que lo use.

Para evitar interrupciones en los clientes, actualiza las aplicaciones cliente de S3 afectadas antes de eliminar un grupo de HA. Actualiza cada cliente para que se conecte usando otra dirección IP; por ejemplo, la dirección IP virtual de un grupo de HA diferente o la dirección IP configurada para una interfaz durante la instalación.

Pasos

1. ${post_edited_translations.segment}
2. Revisa la columna **Puntos de conexión del equilibrador de carga** de cada grupo de alta disponibilidad que quieras eliminar. Si aparece algún punto de conexión del equilibrador de carga:
   a. Ve a **Configuración** > **Red** > **Puntos finales del equilibrador de carga**.
   b. Marca la casilla correspondiente al endpoint.

c. Selecciona **Actions** > **Edit endpoint binding mode**.

d. ${post_edited_translations.segment}

e. Selecciona **Guardar cambios**.

3. ${post_edited_translations.segment}
4. Selecciona **Acciones** > **Eliminar grupo de alta disponibilidad**.
5. Revisa el mensaje y selecciona **Eliminar grupo de HA** para confirmar tu elección.

   Se han eliminado todos los grupos de alta disponibilidad que has seleccionado. Aparece un banner verde de éxito en la página de grupos de alta disponibilidad.

Gestiona el equilibrio de carga

Conoce el equilibrio de carga de StorageGRID

Puedes utilizar el equilibrio de carga para gestionar las cargas de trabajo de ingesta y recuperación de los clientes S3.

¿Qué es el equilibrio de carga?

Cuando una aplicación cliente guarda o recupera datos de un sistema StorageGRID, StorageGRID utiliza un equilibrador de carga para gestionar la carga de trabajo de ingesta y recuperación. El equilibrio de carga maximiza la velocidad y la capacidad de conexión al distribuir la carga de trabajo entre varios Storage Nodes.

El servicio StorageGRID Load Balancer está instalado en todos los nodos de administración y en todos los nodos de puerta de enlace y proporciona equilibrio de carga de capa 7. Realiza la terminación de Transport Layer Security (TLS) de las solicitudes de los clientes, inspecciona las solicitudes y establece nuevas conexiones seguras con los nodos de almacenamiento.

El servicio de equilibrio de carga de cada nodo funciona de forma independiente a la hora de reenviar el tráfico de los clientes a los nodos de almacenamiento. Mediante un proceso de ponderación, el servicio de equilibrio de carga dirige más solicitudes hacia los nodos de almacenamiento con mayor disponibilidad de CPU.

> Aunque el servicio StorageGRID Load Balancer es el mecanismo de equilibrio de carga recomendado, es posible que quieras integrar un equilibrador de carga de terceros en su lugar. Para obtener más información, contacta a tu representante de cuenta de NetApp o consulta "Usa balanceadores de carga de terceros con StorageGRID".

¿Cuántos nodos de equilibrio de carga necesito?

Como práctica recomendada general, cada sitio de tu sistema StorageGRID debería incluir dos o más nodos con el servicio Load Balancer. Por ejemplo, un sitio puede incluir dos Gateway Nodes o tanto un Admin Node como un Gateway Node. Asegúrate de que haya una infraestructura de red, hardware o virtualización adecuada para cada nodo de equilibrio de carga, ya sea que uses servicios appliances, nodos bare metal o nodos basados en máquinas virtuales (VM).

¿Qué es un endpoint de un equilibrador de carga?

Un punto final del equilibrador de carga define el puerto y el protocolo de red (HTTPS o HTTP) que utilizarán las solicitudes entrantes y salientes de las aplicaciones cliente para acceder a los nodos que contienen el servicio Load Balancer. El punto final también define el tipo de cliente (S3), el modo de enlace y, opcionalmente, una lista de inquilinos permitidos o bloqueados.

Para crear un endpoint de equilibrador de carga, usa el Grid Manager o completa los asistentes de configuración de S3 y FabricPool:

- "Configura los puntos de conexión del equilibrador de carga"
- "Utiliza el asistente de configuración de S3"
- "Usa el asistente de configuración de FabricPool"

Aspectos a tener en cuenta para el almacenamiento en caché del equilibrador de carga

El almacenamiento en caché mejora considerablemente el rendimiento cuando una carga de trabajo opera sobre un subconjunto de datos y accede a los objetos varias veces. Además, el almacenamiento en caché permite el acceso remoto al almacenamiento de objetos sin una implementación completa del grid. El almacenamiento en caché del balanceador de carga solo está disponible para Gateway Nodes.

Al crear puntos de conexión del equilibrador de carga:

- Activa el almacenamiento en caché únicamente para las cargas de trabajo almacenables en caché. Las cargas de trabajo que acceden a datos no almacenados en caché con más frecuencia que a los datos almacenados en caché tendrán un rendimiento inferior al que tendrían si no se hubieran gestionado mediante la caché. En algunos casos, las cargas de trabajo con altas tasas de sobrescritura y expulsión también podrían superar la resistencia garantizada de la unidad a la escritura.
- Considera añadir puntos finales o nodos adicionales para almacenar en caché cargas de trabajo individuales que sean buenas candidatas para el almacenamiento en caché.
- Utiliza puntos finales distintos para las cargas de trabajo almacenables en caché y las que no lo son. Esta separación garantiza que los mecanismos de almacenamiento en caché se apliquen correctamente y no interfieran en el procesamiento de datos que no son almacenables en caché.
- Evalúa una carga de trabajo almacenable en caché dirigiéndola al endpoint habilitado para caché. Supervisa y verifica la tasa de aciertos en caché para determinar la idoneidad de la carga de trabajo para el almacenamiento en caché. Esta evaluación ayuda a optimizar el rendimiento y a asegurar un uso eficiente de los recursos de caché.
- "Revisar los registros de auditoría" para determinar si una carga de trabajo existente sería una buena candidata para el almacenamiento en caché. Para un periodo de tiempo determinado, determina qué porcentaje de solicitudes GET corresponden a objetos únicos. Para que sea adecuado para el almacenamiento en caché, este valor debería ser inferior al 50%.

Ejemplos de cargas de trabajo que podrían ser buenas candidatas para el almacenamiento en caché

- Lagos de datos
- ${post_edited_translations.segment}
- Entrenamiento de IA/ML
- Redes de distribución de contenidos (CDN)
- ${post_edited_translations.segment}
- Producción de vídeos

- Se pueden almacenar en caché varias versiones de un objeto.
- Se admiten operaciones de lectura de rango.

Ejemplos de cargas de trabajo que no son buenas candidatas para el almacenamiento en caché

- FabricPool
- Aplicaciones de backup
- Niveles de almacenamiento

> Si algún contenido que vaya a servirse desde la caché requiere cifrado en reposo, "activar el cifrado de nodos o unidades" en el nodo de la caché.

Tipos de objetos y solicitudes que no se almacenarán en la caché

- El `response-content-encoding` parámetro de consulta
- El parámetro de consulta `partNumber`
- 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 gestionadas por StorageGRID)
  - SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente)
  - Cifrado de objetos almacenados

Las solicitudes que no estén almacenadas en la caché se reenvían a un LDR de nivel superior como si la caché no estuviera activada.

Información relacionada

- "Soluciona problemas relacionados con el almacenamiento en caché del equilibrador de carga"
- Para obtener más información sobre el almacenamiento en caché del equilibrador de carga, ponte en contacto con soporte técnico.

Consideraciones para el puerto

El puerto para un punto final del equilibrador de carga es 10433 de forma predeterminada para el primer punto final que crees, pero puedes especificar cualquier puerto externo no utilizado entre 1 y 65535. Si usas el puerto 80 o 443, el punto final usará el servicio de Load Balancer solo en los Gateway Nodes. Estos puertos están reservados en los Admin Nodes. Si usas el mismo puerto para más de un punto final, debes especificar un modo de enlace diferente para cada punto final.

No se permiten los puertos utilizados por otros servicios de grid. Consulta "Puertos internos de 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 TLS (Transport Layer Security). Conectarse a StorageGRID sin cifrado TLS es compatible pero no se recomienda, especialmente en entornos de producción. Cuando selecciones el protocolo de red para el punto final del equilibrador de carga de StorageGRID, debes seleccionar **HTTPS**.

Consideraciones sobre los certificados de los puntos finales del equilibrador de carga

Si seleccionas **HTTPS** como protocolo de red para el punto final del equilibrador de carga, debes proporcionar un certificado de seguridad. Puedes 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 autoridad de certificación (CA) de confianza pública o privada. La mejor práctica es usar un certificado de servidor de una CA de confianza pública para asegurar la conexión. A diferencia de los certificados generados, los certificados firmados por una CA pueden rotarse sin interrupciones, lo que puede ayudar a evitar problemas de caducidad.

  Debes obtener los siguientes archivos antes de crear el punto de conexión del equilibrador de carga:

  - El archivo del certificado del servidor personalizado.
  - El archivo de la clave privada del certificado de servidor personalizado.
  - Opcionalmente, un paquete CA de los certificados de cada autoridad de certificación emisora intermedia.
- **Generar un certificado autofirmado**.
- **Utiliza el certificado global de StorageGRID S3**. Debes cargar o generar una versión personalizada de este certificado antes de poder seleccionarlo para el punto final del equilibrador de carga. Consulta "Configura los certificados de la API de S3".

¿Qué valores necesito?

Para crear el certificado, debes conocer todos los nombres de dominio y direcciones IP que utilizarán las aplicaciones cliente de S3 para acceder al endpoint.

La entrada **DN del sujeto** (nombre distintivo) del certificado debe incluir el nombre de dominio completo que utilizará la aplicación cliente 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 completos de todos los nodos de administración y nodos de puerta de enlace que ejecutan el servicio de Load Balancer. Por ejemplo, `*.storagegrid.example.com` utiliza el comodín * para representar `adm1.storagegrid.example.com` y `gn1.storagegrid.example.com`.

Si tienes pensado utilizar solicitudes de estilo virtual hosted de S3, el certificado también debe incluir una entrada de **nombre alternativo** para cada "${post_edited_translations.segment}" que hayas configurado, incluidos los nombres de comodín. Por ejemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> Si usas comodines para nombres de dominio, revisa "Directrices de refuerzo de la seguridad para certificados de servidor".

También debes definir una entrada DNS para cada nombre que figure en el certificado de seguridad.

${post_edited_translations.segment}

> Si caduca el certificado utilizado para proteger la conexión entre la aplicación S3 y StorageGRID, es posible que la aplicación pierda temporalmente el acceso a StorageGRID.

Para evitar problemas relacionados con la caducidad de los certificados, sigue estas recomendaciones:

- Presta especial atención a cualquier alerta que avise de la proximidad de la fecha de caducidad de un certificado, como las alertas **Caducidad del certificado del punto final del equilibrador de carga** y **Caducidad del certificado global del servidor para la API de S3**.
- Mantén siempre sincronizadas las versiones del certificado de StorageGRID y de la aplicación S3. Si sustituyes o renuevas el certificado utilizado para un punto final del equilibrador de carga, debes sustituir o renovar el certificado equivalente utilizado por la aplicación S3.
- Utiliza un certificado de CA firmado públicamente. Si utilizas un certificado firmado por una CA, puedes reemplazar los certificados que estén a punto de caducar sin interrumpir el servicio.
- Si has generado un certificado autofirmado de StorageGRID y dicho certificado está a punto de caducar, debes sustituirlo manualmente tanto en StorageGRID como en la aplicación S3 antes de que caduque el certificado actual.

${post_edited_translations.segment}

El modo de vinculación te permite controlar qué direcciones IP se pueden usar para acceder a un endpoint del equilibrador de carga. Si un endpoint utiliza un modo de vinculación, las aplicaciones cliente solo pueden acceder al endpoint si usan una dirección IP permitida o su dominio completo (FQDN) correspondiente. Las aplicaciones cliente que usen cualquier otra dirección IP o FQDN no pueden acceder al endpoint.

${post_edited_translations.segment}

- **Global** (predeterminado): Las aplicaciones cliente pueden acceder al endpoint utilizando la dirección IP de cualquier Gateway Node o Admin Node, la dirección IP virtual (VIP) de cualquier HA group en cualquier red, o el FQDN correspondiente. Usa esta configuración a menos que necesites restringir la accesibilidad de un endpoint.
- **Direcciones IP virtuales de los grupos de alta disponibilidad**. Las aplicaciones cliente deben utilizar una dirección IP virtual (o el nombre de dominio completo correspondiente) de un grupo de alta disponibilidad.
- **Interfaces de nodo**. Los clientes deben utilizar las direcciones IP (o los dominios completos correspondientes) de las interfaces de nodo seleccionadas.
- **Tipo de nodo**. En función del tipo de nodo que selecciones, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier Admin Node o la dirección IP (o el FQDN correspondiente) de cualquier Gateway Node.

Consideraciones para el acceso de los inquilinos

El acceso de los inquilinos es una función de seguridad opcional que te permite controlar qué cuentas de inquilinos de StorageGRID pueden utilizar un punto de conexión del equilibrador de carga para acceder a sus buckets. Puedes permitir que todos los inquilinos accedan a un punto de conexión (por defecto) o especificar una lista de los inquilinos permitidos o bloqueados para cada punto de conexión.

Puedes usar esta función para proporcionar un mejor aislamiento de seguridad entre los inquilinos y sus endpoints. Por ejemplo, podrías usar esta función para asegurarte de que los materiales top-secret o altamente clasificados que pertenecen a un inquilino sigan siendo completamente inaccesibles para los demás inquilinos.

A efectos del 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 ocurre con el acceso anónimo), se utiliza al propietario del bucket para determinar el inquilino.

${post_edited_translations.segment}

${post_edited_translations.segment}

1. Has creado dos puntos de conexión del equilibrador de carga, como sigue:
   - Punto de conexión **público**: utiliza el puerto 10443 y permite el acceso a todos los inquilinos.
   - Punto final **Top secret**: utiliza el puerto 10444 y solo permite el acceso al inquilino **Top secret**. Todos los demás inquilinos tienen bloqueado el acceso a este punto final.
2. El `top-secret.pdf` está en un bucket propiedad del inquilino **Top secret**.

Para acceder a `top-secret.pdf`, un usuario del tenant **Top secret** puede enviar una solicitud GET a `https://w.x.y.z:10444/top-secret.pdf`. Dado que este tenant tiene permiso para utilizar el endpoint 10444, el usuario puede acceder al objeto. Sin embargo, si un usuario perteneciente a cualquier otro tenant envía la misma solicitud a la misma URL, recibe inmediatamente un mensaje de Acceso denegado. Se deniega el acceso incluso si las credenciales y la firma son válidas.

${post_edited_translations.segment}

El servicio Load Balancer en cada nodo de administración y nodo de puerta de enlace funciona de forma independiente al reenviar el tráfico S3 a los nodos de almacenamiento. A través de un proceso de ponderación, el servicio Load Balancer dirige más solicitudes a los nodos de almacenamiento con mayor disponibilidad de CPU. La información de carga de la CPU del nodo se actualiza cada pocos minutos, pero la ponderación podría actualizarse con más frecuencia. A todos los nodos de almacenamiento se les asigna un valor de peso base mínimo, incluso si un nodo informa de un 100 % de utilización o no informa de su utilización.

${post_edited_translations.segment}

Configura los puntos finales del equilibrador de carga StorageGRID

Los puntos de conexión del equilibrador de carga determinan los puertos y los protocolos de red que pueden utilizar los clientes de S3 al conectarse al equilibrador de carga de StorageGRID en los nodos Gateway y Admin. También puedes utilizar los puntos de conexión para acceder a Grid Manager, Tenant Manager o a ambos.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".
- Has revisado la "${post_edited_translations.segment}".
- Si anteriormente has reasignado un puerto que pretendes utilizar para el punto final del equilibrador de carga, tienes "${post_edited_translations.segment}".
- Ya has creado los grupos de alta disponibilidad (HA) que planeas usar. Se recomiendan los grupos de alta disponibilidad, pero no son obligatorios. Consulta "Gestiona grupos de alta disponibilidad".
- Si el endpoint del equilibrador de carga lo va a utilizar "Arrendatarios de S3 para S3 Select", no debe usar

las direcciones IP ni los FQDN de ningún nodo bare-metal. Solo se admiten dispositivos de servicios y nodos de software basados en VMware para los endpoints del equilibrador de carga que se utilicen para S3 Select.

- Ya has configurado todas las interfaces VLAN que planeas usar. Consulta "Configurar interfaces VLAN".
- ${post_edited_translations.segment}

> Los cambios en el certificado de un endpoint pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

  - Para cargar un certificado, necesitas el certificado del servidor, la clave privada del certificado y, opcionalmente, un paquete de CA.
  - Para generar un certificado, necesitas todos los nombres de dominio y direcciones IP que los clientes de S3 usarán para acceder al endpoint. También debes conocer el sujeto (Distinguished Name).
  - Si deseas utilizar el certificado de la API S3 de StorageGRID (que también se puede utilizar para conexiones directas a Storage Nodes), ya has reemplazado el certificado predeterminado por un certificado personalizado firmado por una autoridad de certificación externa. Consulta "Configura los certificados de la API de S3".

Crear un punto de conexión del equilibrador de carga

Cada punto de conexión del equilibrador de carga de clientes S3 especifica un puerto, un tipo de cliente (S3) y un protocolo de red (HTTP o HTTPS). Los puntos de conexión del equilibrador de carga de la interfaz de gestión especifican un puerto, un tipo de interfaz y una Client Network no fiable.

Accede al asistente

Pasos

1. Selecciona **Configuración** > **Red** > **Puntos finales del equilibrador de carga**.
2. Para crear un endpoint para un cliente S3, selecciona la pestaña **S3 client**.
3. Para crear un punto de acceso a Grid Manager, Tenant Manager o ambos, selecciona la pestaña **Interfaz de gestión**.
4. Selecciona **Crear**.

Introduce los datos del punto final

Pasos

1. ${post_edited_translations.segment}

${post_edited_translations.segment}

Campo	Descripción
Nombre	${post_edited_translations.segment}
Puerto	El puerto de StorageGRID que quieres usar para el equilibrio de carga. Este campo tiene por defecto el valor 10433 para el primer endpoint que crees, pero puedes ingresar cualquier puerto externo sin usar entre 1 y 65535. Si introduces **80** o **8443**, el endpoint solo se configura en los nodos de Gateway, a menos que hayas liberado el puerto 8443. Entonces puedes usar el puerto 8443 como endpoint S3, y el puerto se configurará tanto en los nodos de Gateway como en los nodos de Admin.
Tipo de cliente	Debe ser **S3**.
Protocolo de red	El protocolo de red que utilizarán los clientes al conectarse a este endpoint. • Selecciona **HTTPS** para una comunicación segura y cifrada mediante TLS (recomendado). Debes adjuntar un certificado de seguridad antes de poder guardar el endpoint. • Selecciona **HTTP** para una comunicación menos segura y sin cifrar. Utiliza HTTP únicamente para una red que no sea de producción.
${post_edited_translations.segment}	Activa o desactiva "${post_edited_translations.segment}" para este endpoint del balanceador de carga. Si surgen problemas con el almacenamiento en caché, consulta "Soluciona problemas relacionados con el almacenamiento en caché del equilibrador de carga".

Interfaz de gestión

Campo	Descripción
Nombre	${post_edited_translations.segment}
Puerto	El puerto de StorageGRID que deseas utilizar para acceder al Grid Manager, al Tenant Manager o a ambos. • Grid Manager: **8443** • Tenant Manager: **9443** • ${post_edited_translations.segment} **Nota**: Puedes utilizar estos puertos predefinidos u otros puertos disponibles.
Tipo de interfaz	${post_edited_translations.segment}

Campo	Descripción
${post_edited_translations.segment}	Selecciona **Sí** si este endpoint debe estar accesible para redes de clientes no confiables. De lo contrario, selecciona **No**. Cuando seleccionas **Sí**, el puerto está abierto en todas las redes de clientes no confiables. ${post_edited_translations.segment}

1. Selecciona **Continuar**.

Selecciona un modo de encuadernación

Pasos

1. Selecciona un modo de enlace para el punto final para controlar cómo se accede a él usando cualquier dirección IP o usando direcciones IP e interfaces de red específicas.

   Algunos modos de enlace están disponibles tanto para los puntos finales de cliente como para los de la interfaz de gestión. Aquí se enumeran todos los modos para ambos tipos de puntos finales.

Modo	Descripción
Global (valor predeterminado para los puntos finales de cliente)	Los clientes pueden acceder al punto final usando la dirección IP de cualquier Gateway Node o Admin Node, la dirección IP virtual (VIP) de cualquier grupo HA en cualquier red, o el FQDN correspondiente. Utiliza la configuración **Global** a menos que necesites restringir la accesibilidad de este endpoint.
Direcciones IP virtuales de los grupos de alta disponibilidad	Los clientes deben utilizar una dirección IP virtual (o el nombre de dominio completo correspondiente) de un grupo de alta disponibilidad para acceder a este endpoint. Todos los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que selecciones para los puntos finales no se solapen.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o los FQDN correspondientes) de las interfaces de los nodos seleccionados para acceder a este endpoint.
Tipo de nodo (solo puntos finales de cliente)	En función del tipo de nodo que selecciones, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier Admin Node o la dirección IP (o el FQDN correspondiente) de cualquier Gateway Node para acceder a este endpoint.
${post_edited_translations.segment}	Los clientes deben utilizar la dirección IP (o el nombre de dominio completo correspondiente) de cualquier Admin Node para acceder a este endpoint.

   Si hay más de un endpoint que utiliza el mismo puerto, StorageGRID usa este orden de prioridad para

decidir qué endpoint usar: **Virtual IPs of HA groups** > **Node interfaces** > **Node type** > **Global**.

Si vas a crear puntos finales de la interfaz de gestión, solo se permiten los nodos de administración.

2. ${post_edited_translations.segment}

   Si estás creando puntos finales de la interfaz de gestión, selecciona las VIP asociadas únicamente con los Admin Nodes.

3. ${post_edited_translations.segment}
4. Si seleccionaste **Tipo de nodo**, elige entre Admin Nodes, que incluye tanto el Admin Node principal como cualquier Admin Node no principal, o Gateway Nodes.

${post_edited_translations.segment}

Un punto final de la interfaz de gestión solo puede controlar el acceso de los inquilinos cuando el punto final tiene el Tipo de interfaz de Tenant Manager.

Pasos

1. Para el paso **Acceso del inquilino**, selecciona una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (por defecto)	${post_edited_translations.segment} Debes seleccionar esta opción si aún no has creado ninguna cuenta de inquilino. Una vez que hayas añadido cuentas de inquilino, puedes editar el endpoint del balanceador de carga para permitir o bloquear cuentas específicas.
Permitir inquilinos seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este endpoint para acceder a sus buckets.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este endpoint para acceder a sus buckets. El resto de inquilinos sí pueden utilizar este endpoint.

2. Si estás creando un punto final **HTTP**, no necesitas adjuntar un certificado. Selecciona **Crear** para añadir el nuevo punto final del equilibrador de carga. Luego, ve a Después de que termines. De lo contrario, selecciona **Continuar** para adjuntar el certificado.

${post_edited_translations.segment}

Pasos

1. Si vas a crear un punto final **HTTPS**, selecciona el tipo de certificado de seguridad que deseas asociar al punto final.

   El certificado protege las conexiones entre los clientes S3 y el servicio Load Balancer en el nodo de administración o en los nodos Gateway.

   - **Cargar certificado**. Selecciona esta opción si tienes certificados personalizados para cargar.

- **Generar certificado**. Selecciona esta opción si tienes los valores necesarios para generar un certificado personalizado.
- **Utilizar el certificado S3 de StorageGRID**. Selecciona esta opción si deseas utilizar el certificado global de la API de S3, que también puede usarse para conexiones directas a Storage Nodes.

  No puedes seleccionar esta opción a menos que hayas sustituido el certificado predeterminado de la API de S3, que está firmado por la CA de la red, por un certificado personalizado firmado por una autoridad de certificación externa. Consulta "Configura los certificados de la API de S3".

- **Usar el certificado de la interfaz de gestión**. Selecciona esta opción si quieres usar el certificado de la interfaz de gestión global, que también se puede usar para conexiones directas a Admin Nodes.

2. Si no estás utilizando el certificado S3 de StorageGRID, sube o genera el certificado.

Subir certificado

a. Selecciona **Cargar certificado**.

b. ${post_edited_translations.segment}

- **Certificado del servidor**: el archivo del certificado personalizado del servidor en codificación PEM.
- **Clave privada del certificado**: El archivo de la 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 de CA**: Un único archivo opcional que contiene los certificados de cada autoridad de certificación (CA) emisora intermedia. El archivo debe contener cada uno de los archivos de certificados de CA codificados en formato PEM, concatenados en el orden de la cadena de certificados.

c. Despliega **Detalles del certificado** para ver los metadatos de cada certificado que subiste. Si subiste un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

- ${post_edited_translations.segment}

  Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Selecciona **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Selecciona **Crear**. + Se crea el extremo del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones posteriores entre los clientes de S3 o la interfaz de gestión y el extremo.

Generar certificado

a. Selecciona **Generar certificado**.

b. ${post_edited_translations.segment}

Campo	Descripción
Nombre de dominio	Uno o más dominios completos para incluir en el certificado. Usa un * como comodín para representar varios nombres de dominio.
${post_edited_translations.segment}	Una o varias direcciones IP para incluir en el certificado.
${post_edited_translations.segment}	${post_edited_translations.segment} Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la primera dirección IP como nombre común (CN) del sujeto.

Campo	Descripción
Días de validez	Número de días después de la creación en los que caduca el certificado.
${post_edited_translations.segment}	${post_edited_translations.segment} ${post_edited_translations.segment} **Nota**: Deja esta casilla marcada a menos que tengas problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

c. Selecciona **Generar**.

d. Selecciona **Detalles del certificado** para ver los metadatos del certificado generado.

- ${post_edited_translations.segment}

  Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Selecciona **Crear**.

Se ha creado el extremo del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones posteriores entre los clientes de S3 o la interfaz de gestión y este extremo.

Después de que termines

Pasos

1. Si utilizas un servidor DNS, asegúrate de que el DNS incluya un registro que asocie el nombre de dominio completo (FQDN) de StorageGRID a cada dirección IP que los clientes usarán para hacer conexiones.

   La dirección IP que introduzcas en el registro DNS depende de si estás utilizando un grupo de alta disponibilidad (HA) de nodos con equilibrio de carga:

   - Si has configurado un grupo de alta disponibilidad, los clientes se conectarán a las direcciones IP virtuales de ese grupo.
   - Si no utilizas un grupo de alta disponibilidad (HA), los clientes se conectarán al servicio StorageGRID Load Balancer usando la dirección IP de un Gateway Node o Admin Node.

     ${post_edited_translations.segment}

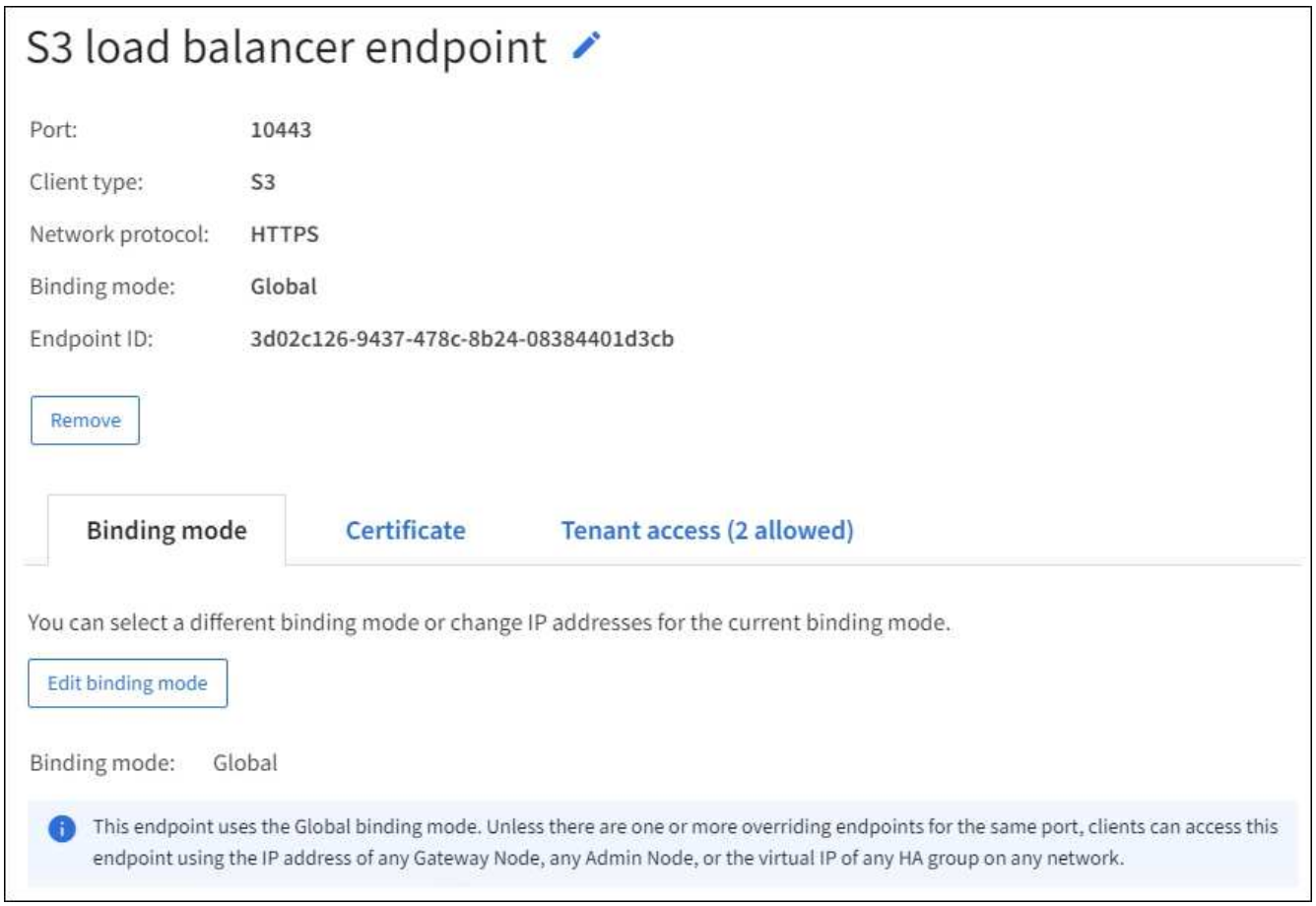
2. Proporciona a los clientes de S3 la información necesaria para conectarse al endpoint:
   - ${post_edited_translations.segment}

- Nombre de dominio completo o dirección IP
- ${post_edited_translations.segment}

Ver y editar los puntos de conexión del equilibrador de carga

Puedes ver los detalles de los puntos de conexión del equilibrador de carga existentes, incluidos los metadatos del certificado de un punto de conexión seguro. Puedes cambiar ciertos ajustes de un punto de conexión.

- ${post_edited_translations.segment}
- Para ver todos los detalles sobre un endpoint concreto, incluidos los metadatos del certificado, selecciona el nombre del endpoint en la tabla. La información que se muestra varía en función del tipo de endpoint y de cómo esté configurado.



- Para editar un punto final, utiliza el menú **Acciones** en la página de puntos finales del equilibrador de carga.

${post_edited_translations.segment}

Tras editar un punto final, es posible que tengas que esperar hasta 15 minutos para que los cambios se apliquen a todos los nodos.

Tarea	Menú de acciones	${post_edited_translations.segment}
${post_edited_translations.segment}	a. Marca la casilla correspondiente al endpoint. b. Selecciona **Acciones** > **Editar nombre del punto final**. c. ${post_edited_translations.segment} d. Selecciona **Guardar**.	a. Selecciona el nombre del endpoint para ver los detalles. b. Selecciona el icono de edición . c. ${post_edited_translations.segment} d. Selecciona **Guardar**.
${post_edited_translations.segment}	a. Marca la casilla correspondiente al endpoint. b. Selecciona **Actions** > **Edit endpoint port** c. Introduce un número de puerto válido. d. Selecciona **Guardar**.	*n/a*
Editar el modo de enlace del punto final	a. Marca la casilla correspondiente al endpoint. b. Selecciona **Actions** > **Edit endpoint binding mode**. c. Actualiza el modo de enlace según sea necesario. d. Selecciona **Guardar cambios**.	a. Selecciona el nombre del endpoint para ver los detalles. b. Selecciona **Editar modo de enlace**. c. Actualiza el modo de enlace según sea necesario. d. Selecciona **Guardar cambios**.
${post_edited_translations.segment}	a. Marca la casilla correspondiente al endpoint. b. ${post_edited_translations.segment} c. Sube o genera un nuevo certificado personalizado o empieza a utilizar el certificado global de S3, según sea necesario. d. Selecciona **Guardar cambios**.	a. Selecciona el nombre del endpoint para ver los detalles. b. Selecciona la pestaña **Certificate**. c. ${post_edited_translations.segment} d. Sube o genera un nuevo certificado personalizado o empieza a utilizar el certificado global de S3, según sea necesario. e. Selecciona **Guardar cambios**.
${post_edited_translations.segment}	a. Marca la casilla correspondiente al endpoint. b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. Selecciona **Guardar cambios**.	a. Selecciona el nombre del endpoint para ver los detalles. b. ${post_edited_translations.segment} c. Selecciona **Editar acceso de inquilino**. d. ${post_edited_translations.segment} e. Selecciona **Guardar cambios**.

Eliminar puntos de conexión del equilibrador de carga

Puedes eliminar uno o varios puntos finales mediante el menú **Actions**, o bien eliminar un único punto final desde la página de detalles.

> Para evitar interrupciones en los clientes, actualiza cualquier aplicación cliente de S3 afectada antes de eliminar un endpoint del equilibrador de carga. Actualiza cada cliente para que se conecte usando un puerto asignado a otro endpoint del equilibrador de carga. Asegúrate también de actualizar cualquier información necesaria sobre certificados.

> Si pierdes el acceso a Grid Manager al eliminar un punto final de la interfaz de gestión, actualiza la URL.

- Para eliminar uno o varios puntos finales:
  a. En la página Load balancer, marca la casilla correspondiente a cada endpoint que quieras eliminar.
  b. ${post_edited_translations.segment}
  c. Selecciona **Aceptar**.
- Para eliminar un endpoint de la página de detalles:
  a. ${post_edited_translations.segment}
  b. Selecciona **Eliminar** en la página de detalles.
  c. Selecciona **Aceptar**.

Configura los nombres de dominio del endpoint S3 en StorageGRID

Para admitir las solicitudes de S3 con alojamiento virtual, debes usar Grid Manager para configurar la lista de nombres de dominio de los endpoints de S3 a los que se conectan los clientes de S3.

> No se admite el uso de una dirección IP como nombre de dominio de un endpoint. Las próximas versiones impedirán esta configuración.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Has confirmado que no hay ninguna actualización de grid en curso.

> No realices ningún cambio en la configuración del nombre de dominio mientras una actualización de la grid está en curso.

Acerca de esta tarea

${post_edited_translations.segment}

- Utiliza el Grid Manager para añadir los nombres de dominio de los endpoints S3 al sistema StorageGRID.
- Asegúrate de que el "certificado que utiliza el cliente para las conexiones HTTPS con StorageGRID" esté firmado para todos los nombres de dominio que necesite el cliente.

Por ejemplo, si el endpoint es `s3.company.com`, debes asegurarte de que el certificado utilizado para las conexiones HTTPS incluya el endpoint `s3.company.com` y el nombre alternativo del sujeto (SAN) comodín de ese endpoint: `*.s3.company.com`.

- Configura el servidor DNS que utiliza el cliente. Incluye registros DNS para las direcciones IP que utilizan los clientes para establecer conexiones y asegúrate de que los registros hagan referencia a todos los nombres de dominio de los endpoints S3 necesarios, incluidos los nombres con comodines.

> Los clientes pueden conectarse a StorageGRID utilizando la dirección IP de un nodo de puerta de enlace, un nodo de administración o un nodo de almacenamiento, o conectándose a la dirección IP virtual de un grupo de alta disponibilidad. Debes entender cómo se conectan las aplicaciones cliente a la grid para que incluyas las direcciones IP correctas en los registros DNS.

${post_edited_translations.segment}

- Los clientes que se conectan a un endpoint de equilibrador de carga pueden usar un certificado personalizado para ese endpoint. Cada endpoint de equilibrador de carga se puede configurar para reconocer diferentes nombres de dominio de endpoint de S3.
- Los clientes que se conectan a un punto de conexión del balanceador de carga o directamente a un Storage Node pueden personalizar el certificado global de la API de S3 para incluir todos los nombres de dominio de los puntos de conexión de S3 necesarios.

> Si no añades nombres de dominio de endpoint S3 y la lista está vacía, el soporte para solicitudes de S3 con estilo virtual-hosted estará desactivado.

${post_edited_translations.segment}

Pasos

1. Selecciona **Configuración** > **Red** > **Nombres de dominio de endpoint S3**.
2. Introduce el nombre de dominio en el campo **Nombre de dominio 1**. Selecciona **Add another domain name** para añadir más nombres de dominio.
3. Selecciona **Guardar**.
4. Asegúrate de que los certificados del servidor que utilizan los clientes coincidan con los nombres de dominio de los endpoints de S3 requeridos.
   - Si los clientes se conectan a un punto de conexión del equilibrador de carga que utiliza su propio certificado, "Actualiza el certificado asociado al endpoint".
   - Si los clientes se conectan a un endpoint del equilibrador de carga que utiliza el certificado global de la API de S3 o directamente a los nodos de almacenamiento, "${post_edited_translations.segment}".
5. Agrega los registros DNS necesarios para garantizar que se puedan resolver las solicitudes de nombres de dominio de los endpoints.

Resultado

Ahora, cuando los clientes usan el endpoint *`bucket.s3.company.com`*, el servidor DNS resuelve al endpoint correcto y el certificado autentica el endpoint como se espera.

Cambiar el nombre de dominio del endpoint S3

Si cambias un nombre utilizado por las aplicaciones S3, las solicitudes de tipo virtual-hosted-style fallarán.

Pasos

1. Selecciona **Configuración** > **Red** > **Nombres de dominio de endpoint S3**.
2. Selecciona el campo del nombre de dominio que quieras editar y realiza los cambios necesarios.
3. Selecciona **Guardar**.
4. Selecciona **Sí** para confirmar tu cambio.

${post_edited_translations.segment}

Si eliminas un nombre utilizado por las aplicaciones S3, las solicitudes de tipo virtual-hosted-style fallarán.

Pasos

1. Selecciona **Configuración** > **Red** > **Nombres de dominio de endpoint S3**.
2. Selecciona el icono de eliminación ✕ junto al nombre de dominio.
3. ${post_edited_translations.segment}

Información relacionada

- "Usa la API de REST de S3"
- "${post_edited_translations.segment}"
- "Configurar grupos de alta disponibilidad"

Direcciones IP y puertos para conexiones de cliente de StorageGRID

Para almacenar o recuperar objetos, las aplicaciones cliente de S3 se conectan al servicio Load Balancer, que está incluido en todos los Admin Nodes y Gateway Nodes, o al servicio Local Distribution Router (LDR), que está incluido en todos los Storage Nodes.

Las aplicaciones cliente pueden conectarse a StorageGRID utilizando la dirección IP de un nodo de la red y el número de puerto del servicio en ese nodo. Opcionalmente, puedes crear grupos de alta disponibilidad (HA) de nodos de balanceo de carga para ofrecer conexiones altamente disponibles que usen direcciones IP virtuales (VIP). Si quieres conectarte a StorageGRID usando un dominio completo (FQDN) en vez de una dirección IP o VIP, puedes configurar entradas DNS.

Esta tabla resume las diferentes 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 creaste puntos finales del equilibrador de carga y grupos de alta disponibilidad (HA), consulta Dónde encontrar direcciones IP para encontrar estos valores en Grid Manager.

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Grupo HA	Equilibrador de carga	Dirección IP virtual de un grupo de alta disponibilidad	Puerto asignado al punto final del equilibrador de carga
Nodo de administración	Equilibrador de carga	${post_edited_translations.segment}	Puerto asignado al punto final del equilibrador de carga

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
${post_edited_translations.segment}	Equilibrador de carga	${post_edited_translations.segment}	Puerto asignado al punto final del equilibrador de carga
Nodo de almacenamiento	LDR	Dirección IP del nodo de almacenamiento	Puertos predeterminados de S3: • HTTPS: 18082 • ${post_edited_translations.segment}

${post_edited_translations.segment}

Para conectar una aplicación cliente al punto final del equilibrador de carga de un grupo de alta disponibilidad (HA) de Gateway Nodes, utiliza una URL con la estructura que se muestra a continuación:

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

Por ejemplo, si la dirección IP virtual del grupo de alta disponibilidad es 192.0.2.5 y el número de puerto del punto final 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. Inicia sesión en Grid Manager usando una "navegador web compatible" cuenta.
2. Para averiguar la dirección IP de un nodo de la red:
   a. Selecciona **Nodos**.
   b. Selecciona el nodo de administración, el nodo de puerta de enlace o el nodo de almacenamiento al que quieras conectarte.
   c. Selecciona la pestaña **Vista general**.
   d. En la sección Información del nodo, anota las direcciones IP del nodo.
   e. ${post_edited_translations.segment}

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

      - ${post_edited_translations.segment}
      - **eth1:** Red de administración (opcional)
      - ${post_edited_translations.segment}

        ${post_edited_translations.segment}
3. Para averiguar la dirección IP virtual de un grupo de alta disponibilidad:

a. ${post_edited_translations.segment}

b. En la tabla, toma nota de la dirección IP virtual del grupo de HA.

4. ${post_edited_translations.segment}

a. Selecciona **Configuración** > **Red** > **Puntos finales del equilibrador de carga**.

b. ${post_edited_translations.segment}

> Si el número de puerto es 80 o 443, el endpoint solo se configura en los Gateway Nodes, ya que esos puertos están reservados en los Admin Nodes. Todos los demás puertos se configuran tanto en los Gateway Nodes como en los Admin Nodes.

c. ${post_edited_translations.segment}

d. Comprueba que el **tipo de cliente** (S3) coincida con la aplicación cliente que va a utilizar el endpoint.

Gestiona redes y conexiones

Configura los ajustes de red de StorageGRID

Desde Grid Manager puedes configurar diversos parámetros de red para ajustar con precisión el funcionamiento de tu sistema StorageGRID.

Configurar interfaces VLAN

Puedes "crear interfaces de red local virtual (VLAN)" para aislar y dividir el tráfico por seguridad, flexibilidad y rendimiento. Cada interfaz VLAN está asociada con una o más interfaces principales en los nodos de administración y los nodos de puerta de enlace. Puedes usar interfaces VLAN en grupos HA y en endpoints de balanceador de carga para segregar el tráfico de cliente o de administración por aplicación o tenant.

Políticas de clasificación del tráfico

Puedes utilizar "políticas de clasificación del tráfico" para identificar y gestionar diferentes tipos de tráfico de red, incluido el tráfico relacionado con buckets, tenants, subredes de clientes o endpoints de balanceadores de carga específicos. Estas políticas pueden ayudarte a limitar y supervisar el tráfico.

Directrices para redes StorageGRID

Puedes utilizar el Grid Manager para configurar y gestionar las redes y conexiones de StorageGRID.

Consulta "${post_edited_translations.segment}" para saber cómo conectar clientes de S3.

${post_edited_translations.segment}

${post_edited_translations.segment}

Para obtener más información sobre la topología de red, consulta "${post_edited_translations.segment}".

Red de grid

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

Red de administración

Opcional. La red de administración se utiliza normalmente para la administración y el mantenimiento del sistema. También puede usarse para el acceso de protocolos de cliente. La red de administración suele ser una red privada y no necesita ser enrutable entre sitios.

Red de clientes

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

${post_edited_translations.segment}

- Cada nodo de StorageGRID requiere una interfaz de red dedicada, una dirección IP, una máscara de subred y una puerta de enlace para cada red a la que esté asignado.
- Un nodo de red no puede tener más de una interfaz en una red.
- Se admite una única puerta de enlace por red y por nodo de grid, y debe estar en la misma subred que el nodo. Puedes implementar un enrutamiento más complejo en la puerta de enlace si lo necesitas.
- En cada nodo, cada red se asigna a una interfaz de red específica.

Red	Nombre de la interfaz
${post_edited_translations.segment}	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, consulta las instrucciones de instalación de tu dispositivo.
- La ruta predeterminada se genera automáticamente para cada nodo. Si eth2 está habilitada, entonces 0.0.0.0/0 utiliza la red de cliente en eth2. Si eth2 no está habilitada, entonces 0.0.0.0/0 utiliza la Grid Network en eth0.
- La red de clientes no entra en funcionamiento hasta que el nodo de la red se une a la red
- La red de administración se puede configurar durante la implementación del nodo de la red para permitir el acceso a la interfaz de usuario de instalación antes de que la red esté completamente instalada.

Interfaces opcionales

Si lo deseas, puedes añadir interfaces adicionales a un nodo. Por ejemplo, quizá quieras añadir una interfaz de enlace troncal a un nodo Admin o Gateway, para que puedas usar "Interfaces de VLAN" para segregar el tráfico que pertenece a diferentes aplicaciones o tenants. O quizá quieras añadir una interfaz de acceso para usarla en un "grupo de alta disponibilidad (HA)".

Para añadir interfaces de tronco o de acceso, consulta lo siguiente:

- **VMware (tras instalar el nodo)**: "VMware: Añadir interfaces de tronco o de acceso a un nodo"
  - **Linux (antes de instalar el nodo)**: "Crear archivos de configuración de nodos"

- **Linux (después de instalar el nodo)**: "Agrega interfaces trunk o de acceso a un nodo"

> «Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita "Herramienta de matriz de interoperabilidad (IMT) de NetApp".

Ver direcciones IP en StorageGRID

Puedes consultar la dirección IP de cada nodo de grid en tu sistema StorageGRID. Luego, puedes usar esta dirección IP para iniciar sesión en el nodo de grid desde la línea de comandos y realizar varios procedimientos de mantenimiento.

Antes de empezar

Has iniciado sesión en Grid Manager mediante un "navegador web compatible".

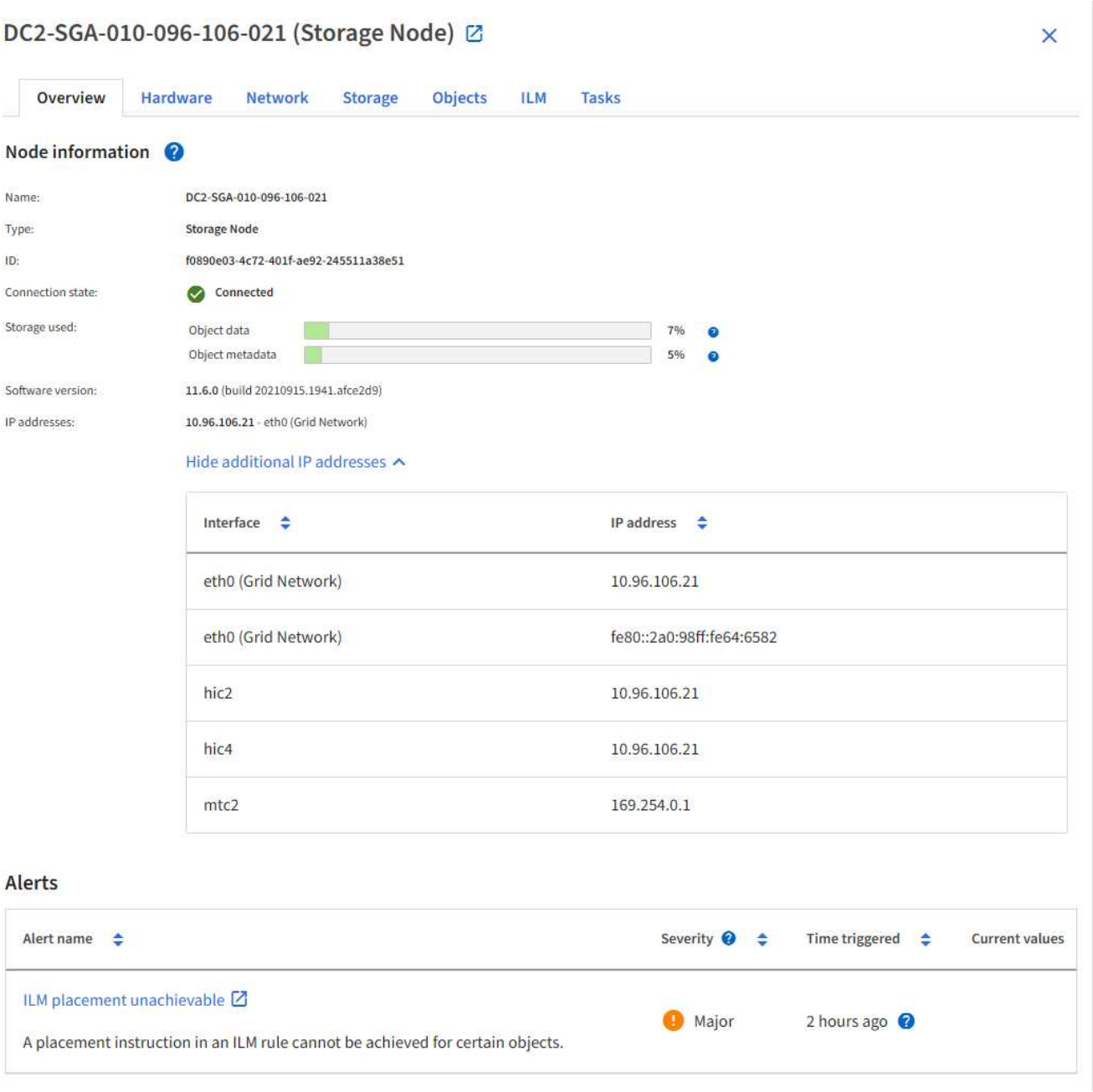
Acerca de esta tarea

Para obtener información sobre cómo cambiar las direcciones IP, consulta "Configurar direcciones IP".

Pasos

1. Selecciona **Nodos** > ***nodo de cuadrícula*** > **Resumen**.
2. Selecciona **Mostrar más** a la derecha del título Direcciones IP.

   Las direcciones IP de ese nodo de la grid aparecen en una tabla.



Configura interfaces VLAN en StorageGRID

Crea interfaces de LAN virtual (VLAN) en los nodos de administración y los nodos de puerta de enlace y utilízalas en grupos de alta disponibilidad y puntos finales del equilibrador de carga para aislar y dividir el tráfico por seguridad, flexibilidad y rendimiento. Los nodos seleccionados en el grupo de alta disponibilidad pueden usar las interfaces VLAN para compartir hasta 10 direcciones IP virtuales, así que si un nodo se cae, otro nodo toma el control del tráfico hacia y desde las direcciones IP virtuales.

Aspectos a tener en cuenta sobre las interfaces VLAN

- Creas una interfaz VLAN introduciendo un ID de VLAN y eligiendo una interfaz principal en uno o varios nodos.

- Una interfaz principal debe configurarse como interfaz troncal en el switch.
- Una interfaz principal puede ser la Grid Network (eth0), la Client Network (eth2) o una interfaz troncal adicional para la VM o el host bare-metal (por ejemplo, ens256).
- Para cada interfaz VLAN, solo puedes seleccionar una interfaz principal para un nodo determinado. Por ejemplo, no puedes usar tanto la interfaz Grid Network como la interfaz Client Network en el mismo Gateway Node como interfaz principal para la misma VLAN.
- Si la interfaz VLAN está destinada al tráfico de los nodos de administración, lo que incluye el tráfico relacionado con el Grid Manager y el Tenant Manager, selecciona únicamente las interfaces de los nodos de administración.
- Si la interfaz VLAN está destinada al tráfico del cliente S3, selecciona interfaces en los nodos de administración o en los nodos de puerta de enlace.
- Si necesitas añadir interfaces de enlace troncal, consulta la siguiente información para obtener más detalles:
  - **VMware (tras instalar el nodo)**: "VMware: Añadir interfaces de tronco o de acceso a un nodo"
  - **Linux (antes de instalar el nodo)**: "Crear archivos de configuración de nodos"
  - **Linux (después de instalar el nodo)**: "Agrega interfaces trunk o de acceso a un nodo"

> «Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita "Herramienta de matriz de interoperabilidad (IMT) de NetApp".

Crear una interfaz VLAN

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".
- Se ha configurado una interfaz de enlace troncal en la red y se ha conectado a la VM o al nodo Linux. Conoces el nombre de la interfaz de enlace troncal.
- Ya conoces el ID de la VLAN que estás configurando.

Acerca de esta tarea

Es posible que tu administrador de red haya configurado una o varias interfaces de enlace troncal y una o varias VLAN para segregar el tráfico de clientes o de administración correspondiente a diferentes aplicaciones o inquilinos. Cada VLAN se identifica mediante un identificador numérico o una etiqueta. Por ejemplo, tu red podría usar la VLAN 100 para el tráfico de FabricPool y la VLAN 200 para una aplicación de archivado.

Puedes utilizar el Grid Manager para crear interfaces VLAN que permitan a los clientes acceder a StorageGRID en una VLAN específica. Cuando creas interfaces VLAN, debes especificar el ID de la VLAN y seleccionar las interfaces principales (trunk) en uno o varios nodos.

Accede al asistente

Pasos

1. Selecciona **Configuración** > **Red** > **Interfaces VLAN**.
2. Selecciona **Crear**.

Introduce los datos de las interfaces de VLAN

Pasos

1. Especifica el ID de la VLAN en tu red. Puedes introducir cualquier valor entre 1 y 4094.

   Los ID de VLAN no tienen por qué ser únicos. Por ejemplo, puedes usar el ID de VLAN 200 para el tráfico de administración en un sitio y el mismo ID de VLAN para el tráfico de clientes en otro sitio. Puedes crear interfaces de 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 especificas un ID que ya se ha utilizado, aparece un mensaje.

2. Opcionalmente, escribe una breve descripción para la interfaz VLAN.
3. Selecciona **Continuar**.

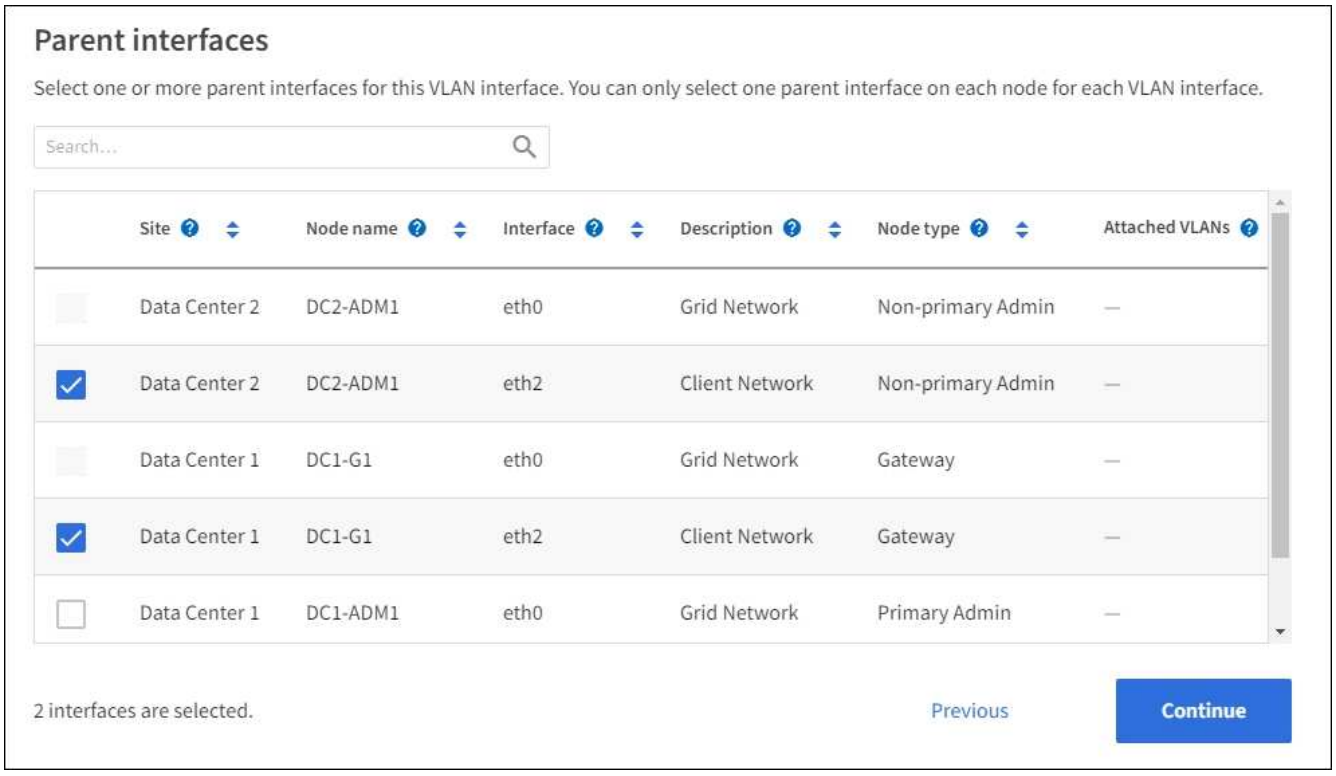
Elige interfaces principales

La tabla muestra las interfaces disponibles para todos los nodos de administración y los nodos de pasarela en cada sitio de tu grid. Las interfaces de Admin Network (eth1) no pueden usarse como interfaces principales y no se muestran.

Pasos

1. Selecciona una o más interfaces principales a las que conectar esta VLAN.

   Por ejemplo, podrías querer asociar una VLAN a la interfaz Client Network (eth2) de un Gateway Node y un Admin Node.



2. Selecciona **Continuar**.

Confirma la configuración

Pasos

1. Revisa la configuración y realiza los cambios que sean necesarios.
   - Si necesitas cambiar el ID de la VLAN o la descripción, selecciona **Introducir detalles de la VLAN** en la parte superior de la página.
   - Si necesitas cambiar una interfaz principal, selecciona **Elegir interfaces principales** en la parte superior de la página o selecciona **Anterior**.
   - Si necesitas eliminar una interfaz principal, selecciona el icono de la papelera .
2. Selecciona **Guardar**.
3. Espera hasta 5 minutos para que la nueva interfaz aparezca como opción en la página **Grupos de alta disponibilidad** y se incluya en la tabla **Interfaces de red** del nodo (**Nodos** > ***parent interface node*** > **Red**).

Editar una interfaz VLAN

Al editar una interfaz VLAN, puedes realizar los siguientes tipos de cambios:

- Modifica el ID o la descripción de la VLAN.
- Agregar o eliminar interfaces principales.

Por ejemplo, es posible que quieras eliminar una interfaz principal de una interfaz de VLAN si tienes previsto decomisionar el nodo asociado.

Ten en cuenta lo siguiente:

- No puedes cambiar el ID de una VLAN si la interfaz de la VLAN se usa en un grupo HA.
- No puedes eliminar una interfaz principal si esa interfaz se usa en un grupo de alta disponibilidad.

  Por ejemplo, supón que la VLAN 200 está conectada a las interfaces principales en los nodos A y B. Si un grupo HA usa la interfaz VLAN 200 para el nodo A y la interfaz eth2 para el nodo B, puedes eliminar la interfaz principal no utilizada del nodo B, pero no puedes eliminar la interfaz principal utilizada del nodo A.

Pasos

1. Selecciona **Configuración** > **Red** > **Interfaces VLAN**.
2. Marca la casilla de la interfaz VLAN que quieras editar. A continuación, selecciona **Acciones** > **Editar**.
3. Si lo deseas, actualiza el ID de la VLAN o la descripción. Luego, selecciona **Continuar**.

   No puedes actualizar el ID de una VLAN si la VLAN se usa en un grupo de alta disponibilidad (HA).

4. Si lo deseas, marca o desmarca las casillas de selección para añadir interfaces principales o eliminar interfaces que no se utilicen. Luego, selecciona **Continuar**.
5. Revisa la configuración y realiza los cambios que sean necesarios.
6. Selecciona **Guardar**.

Eliminar una interfaz VLAN

Puedes eliminar una o varias interfaces VLAN.

No puedes eliminar una interfaz VLAN si actualmente se está usando en un grupo HA. Debes quitar la interfaz VLAN del grupo HA antes de poder eliminarla.

Para evitar cualquier interrupción en el tráfico de clientes, considera hacer una de las siguientes cosas:

- Agrega una nueva interfaz VLAN al grupo HA antes de eliminar esta interfaz VLAN.
- Crea un nuevo grupo de alta disponibilidad que no utilice esta interfaz VLAN.
- Si la interfaz VLAN que quieres eliminar es actualmente la interfaz activa, edita el grupo de alta disponibilidad. Mueve la interfaz VLAN que quieres eliminar al final de la lista de prioridades. Espera hasta que se establezca la comunicación en la nueva interfaz primaria y luego elimina la interfaz anterior del grupo de alta disponibilidad. Por último, elimina la interfaz VLAN de ese nodo.

Pasos

1. Selecciona **Configuración** > **Red** > **Interfaces VLAN**.
2. Marca la casilla de selección correspondiente a cada interfaz VLAN que desees eliminar. A continuación, selecciona **Actions** > **Delete**.
3. Selecciona **Sí** para confirmar tu elección.

   Se han eliminado todas las interfaces VLAN que has seleccionado. Aparece un mensaje verde de éxito en la página de interfaces VLAN.

${post_edited_translations.segment}

Como administrador de la grid, puedes habilitar el intercambio de recursos entre orígenes (CORS) para las solicitudes de la API de gestión a StorageGRID, si quieres que los datos en StorageGRID sean accesibles usando las API de gestión desde otro dominio.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "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 a las aplicaciones web cliente de un dominio acceder a recursos de un dominio diferente. Por ejemplo, supón que quieres crear un panel de control de monitorización para StorageGRID en el dominio `http://www.example.com`. Al habilitar CORS en StorageGRID para `http://www.example.com` y "Grid Manager", el dominio de StorageGRID responde a las solicitudes de la API de gestión de Grid desde `http://www.example.com`.

Las solicitudes de la API de gestión (mgmt-api) con `application/json` o `multipart/formdata` solicitudes para `Content-Type` son compatibles con CORS.

Pasos

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - **Tenant Manager**: habilita CORS para las solicitudes de la API de gestión de inquilinos entre dominios.
3. ${post_edited_translations.segment}

   Selecciona **Add another domain** si deseas habilitar CORS en StorageGRID para más de un dominio.

4. Selecciona **Guardar**.

Información relacionada

"${post_edited_translations.segment}"

Gestiona las políticas de clasificación del tráfico

Políticas de clasificación de tráfico en StorageGRID

Las políticas de clasificación de tráfico te permiten identificar y supervisar diferentes tipos de tráfico de red. Estas políticas pueden ayudarte a limitar y supervisar el tráfico para mejorar tus ofertas de calidad de servicio (QoS).

Las políticas de clasificación de tráfico se aplican a los puntos de conexión en el servicio de equilibrador de carga de StorageGRID para los nodos de puerta de enlace y los nodos de administración. Para crear políticas de clasificación de tráfico, ya debes haber creado puntos de conexión del equilibrador de carga.

Reglas de coincidencia

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- Subred
- Inquilino
- ${post_edited_translations.segment}

StorageGRID supervisa el tráfico que coincide con cualquier regla de la política de acuerdo con los objetivos de dicha regla. Todo el tráfico que coincida con cualquier regla de una política se gestiona mediante dicha política. Por el contrario, puedes establecer reglas para que coincidan con todo el tráfico excepto el de una entidad específica.

Limitación del tráfico

Si lo deseas, puedes añadir los siguientes tipos de límite a una política:

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Solicitudes simultáneas
- Tasa de solicitud

Los valores límite se aplican por cada equilibrador de carga. Si el tráfico se distribuye simultáneamente entre varios equilibradores de carga, las tasas máximas totales son un múltiplo de los límites de tasa que especifiques.

> Puedes crear políticas para limitar el ancho de banda de agregado o para limitar el ancho de banda por solicitud. Sin embargo, StorageGRID no puede limitar ambos tipos de ancho de banda al mismo tiempo. Los límites de ancho de banda de agregado pueden imponer un impacto adicional menor en el rendimiento del tráfico no limitado.

Para los límites de ancho de banda de agregado o por solicitud, las solicitudes se transmiten de entrada o de

salida a la velocidad que configures. StorageGRID solo puede aplicar una velocidad, por lo que la coincidencia de política más específica, por tipo de comparador, es la que se aplica. El ancho de banda consumido por la solicitud no cuenta para otras políticas coincidentes menos específicas que contengan políticas de límite de ancho de banda de agregado. Para todos los demás tipos de límites, las solicitudes de los clientes se retrasan 250 milisegundos y reciben una respuesta 503 Slow Down en el caso de las solicitudes que superen cualquier límite de política coincidente.

${post_edited_translations.segment}

${post_edited_translations.segment}

Puedes usar las políticas de clasificación del tráfico junto con los límites de capacidad y la protección de datos para hacer cumplir los acuerdos de nivel de servicio (SLA) que proporcionan detalles específicos sobre capacidad, protección de datos y rendimiento.

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

${post_edited_translations.segment}	Capacidad	Protección de datos	Rendimiento máximo permitido	Coste
Oro	1 PB de almacenamiento permitido	${post_edited_translations.segment}	${post_edited_translations.segment} 5 GB/s (40 Gbps) de ancho de banda	$$$ al mes
${post_edited_translations.segment}	250 TB de almacenamiento permitidos	2 copia de la regla ILM	10 K solicitudes/seg 1,25 GB/s (10 Gbps) de ancho de banda	$$ al mes
Bronce	100 TB de almacenamiento permitidos	2 copia de la regla ILM	${post_edited_translations.segment} ${post_edited_translations.segment}	$ al mes

Crear políticas de clasificación de tráfico StorageGRID

Puedes crear políticas de clasificación de tráfico si quieres supervisar y, opcionalmente, limitar el tráfico de red por bucket, expresión regular de bucket, CIDR, extremo de equilibrador de carga o inquilino. Opcionalmente, puedes establecer límites para una política en función del ancho de banda, el número de solicitudes simultáneas o la tasa de solicitudes.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".
- Has creado los puntos de conexión del equilibrador de carga que deseas hacer coincidir.

- ${post_edited_translations.segment}

Pasos

1. Selecciona **Configuración** > **Red** > **Clasificación del tráfico**.
2. Selecciona **Crear**.
3. Introduce un nombre y una descripción (opcional) para la política y selecciona **Continuar**.

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

4. Selecciona **Add rule** e indica los siguientes datos para crear una o varias reglas de coincidencia para la política. Cualquier política que crees debe tener al menos una regla de coincidencia. Selecciona **Continue**.

Campo	Descripción
Tipo	Selecciona 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	Introduce el valor que coincida con el tipo seleccionado. • ${post_edited_translations.segment} • Expresión regular de buckets: introduce una o varias expresiones regulares que se usan para buscar coincidencias con un conjunto de nombres de buckets. La expresión regular no está anclada. Usa el ancla ^ para buscar coincidencias al principio del nombre del bucket y usa el ancla $ para buscar coincidencias al final del nombre. La coincidencia de expresiones regulares admite un subconjunto de la sintaxis de PCRE (expresión regular compatible con Perl). • CIDR: introduce una o varias subredes IPv4, en notación CIDR, que coincidan con la subred deseada. • Punto final del equilibrador de carga: selecciona un nombre de punto final. Estos son los puntos finales del equilibrador de carga que has definido en el "Configura los puntos de conexión del equilibrador de carga". • Inquilino: la coincidencia de inquilino usa el ID de la clave de acceso. Si la solicitud no contiene un ID de clave de acceso (por ejemplo, acceso anónimo), entonces se utiliza la titularidad del bucket al que se accede para determinar el inquilino.
Coincidencia inversa	Si deseas filtrar todo el tráfico de red *excepto* aquel que coincida con el tipo y el valor de coincidencia que acabas de definir, marca la casilla **Coincidencia inversa**. En caso contrario, deja la casilla desmarcada. ${post_edited_translations.segment} En una política que contenga varios criterios de coincidencia, donde al menos uno sea un criterio de coincidencia inversa, ten cuidado de no crear una política que coincida con todas las solicitudes.

5. Si lo deseas, selecciona **Add a limit** y elige los siguientes detalles para añadir uno o varios límites con los que controlar el tráfico de red al que se aplica una regla.

> StorageGRID recopila métricas incluso si no agregas ningún límite, así puedes entender las tendencias del tráfico.

Campo	Descripción
Tipo	El tipo de límite que deseas aplicar al tráfico de red que coincide con la regla. Por ejemplo, puedes limitar el ancho de banda o la frecuencia de solicitudes. **Nota**: Puedes crear políticas para limitar el ancho de banda de agregado o para limitar el ancho de banda por solicitud. Sin embargo, StorageGRID no puede limitar ambos tipos de ancho de banda al mismo tiempo. Cuando se utiliza el ancho de banda de 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 de agregado no está disponible. Los límites del ancho de banda de agregado pueden suponer un impacto menor adicional en el rendimiento del tráfico no limitado. En cuanto a los límites de ancho de banda, StorageGRID aplica la política que mejor se ajusta al tipo de límite establecido. Por ejemplo, si tienes una política que limita el tráfico en una sola dirección, el tráfico en la dirección opuesta no tendrá límite, incluso si hay tráfico que coincide con políticas adicionales que tienen límites de ancho de banda. StorageGRID aplica las "mejores" coincidencias para los límites de ancho de banda en el siguiente orden: • Dirección IP exacta (máscara /32) • Nombre exacto del depósito • Expresión regular de bucket • Inquilino • Punto final • Coincidencias CIDR no exactas (que no sean /32) • Coincidencias inversas
${post_edited_translations.segment}	Si este límite se aplica a las solicitudes de lectura de los clientes (GET o HEAD) o a las solicitudes de escritura (PUT, POST o DELETE).
Valor	El valor al que se limitará el tráfico de red, según la unidad que selecciones. Por ejemplo, introduce 10 y selecciona MiB/s para evitar que el tráfico de red que coincida con esta regla supere los 10 MiB/s. **Nota**: dependiendo del ajuste de las unidades, las unidades disponibles serán binarias (por ejemplo, GiB) o decimales (por ejemplo, GB). Para cambiar el ajuste de las unidades, selecciona el menú desplegable de usuario en la parte superior derecha de Grid Manager y, a continuación, selecciona **Preferencias de usuario**.
Unidad	La unidad que describe el valor que has introducido.

Por ejemplo, si quieres establecer un límite de ancho de banda de 4 GB/s para un nivel de SLA, crea dos límites de ancho de banda de agregado: GET/HEAD a 4 GB/s y PUT/POST/DELETE a 4 GB/s.

6. Selecciona **Continuar**.
7. Lee y revisa la política de clasificación de tráfico. Usa el botón **Anterior** para volver y realizar cambios según sea necesario. Cuando estés satisfecho con la política, selecciona **Guardar y continuar**.

   El tráfico del cliente S3 ahora se gestiona según la política de clasificación del tráfico.

Después de que termines

"Ver métricas de tráfico de red" para verificar que las políticas estén aplicando los límites de tráfico que esperas.

Edita una política de clasificación de tráfico de StorageGRID

Puedes editar una política de clasificación del tráfico para cambiar su nombre o descripción, o para crear, editar o eliminar cualquier regla o límite de la política.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".

Pasos

1. Selecciona **Configuración** > **Red** > **Clasificación del tráfico**.

   Aparece la página «Políticas de clasificación del tráfico» y las políticas existentes se muestran en una tabla.

2. Edita la política mediante el menú «Acciones» o la página de detalles. Consulta "${post_edited_translations.segment}" para saber qué datos debes introducir.

   Menú de acciones

   a. Marca la casilla para la política.

   b. Selecciona **Acciones** > **Editar**.

   ${post_edited_translations.segment}

   a. Selecciona el nombre de la política.

   b. ${post_edited_translations.segment}

3. En el paso «Introducir el nombre de la política», si lo deseas, edita el nombre o la descripción de la política y selecciona **Continuar**.
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}

   Se han guardado los cambios que has realizado en la política y ahora el tráfico de red se gestiona de acuerdo con las políticas de clasificación de tráfico. Puedes ver los gráficos de tráfico y verificar que las políticas estén aplicando los límites de tráfico que esperas.

Eliminar una política de clasificación de tráfico StorageGRID

Puedes eliminar una política de clasificación de tráfico si ya no la necesitas. Asegúrate de eliminar la política correcta porque una política no se puede recuperar cuando se elimina.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".

Pasos

1. Selecciona **Configuración** > **Red** > **Clasificación del tráfico**.

   Aparece la página de políticas de clasificación del tráfico con las políticas existentes listadas en una tabla.

2. Elimina la política usando el menú Acciones o la página de detalles.

   Menú de acciones

   a. Marca la casilla para la política.

   b. ${post_edited_translations.segment}

   Página de detalles de la política

   a. Selecciona el nombre de la política.

   b. Selecciona el botón **Eliminar** junto al nombre de la política.

3. ${post_edited_translations.segment}

   La política se eliminó.

Ver métricas de tráfico de red en StorageGRID

${post_edited_translations.segment}

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "${post_edited_translations.segment}".

Acerca de esta tarea

Para cualquier política de clasificación de tráfico existente, puedes consultar las métricas del servicio de equilibrador de carga para determinar si la política está limitando correctamente el tráfico en la red. Los datos de los gráficos pueden ayudarte a determinar si necesitas ajustar la política.

${post_edited_translations.segment}

Pasos

1. Selecciona **Configuración** > **Red** > **Clasificación del tráfico**.

   ${post_edited_translations.segment}

2. Selecciona el nombre de la política de clasificación de tráfico para la que quieres ver las métricas.
3. Selecciona la pestaña **Métricas**.

   Aparecen los gráficos de la política de clasificación del tráfico. Los gráficos muestran métricas únicamente para el tráfico que coincide con la política seleccionada.

   En esta página se incluyen los siguientes gráficos.

   - Tasa de solicitudes: Este gráfico muestra la cantidad de ancho de banda que se ajusta a esta política y que gestionan todos los equilibradores de carga. Los datos recibidos incluyen los encabezados de todas las solicitudes y el tamaño del cuerpo de las respuestas que contienen datos en el cuerpo. Los datos enviados incluyen los encabezados de todas las solicitudes y el tamaño del cuerpo de las respuestas que contienen datos en el cuerpo.

     > Cuando las solicitudes se han completado, este gráfico solo muestra el uso del ancho de banda. En el caso de solicitudes lentas o de objetos de gran tamaño, el ancho de banda instantáneo real puede diferir de los valores que se muestran en este gráfico.

   - Tasa de respuestas con error: Este gráfico muestra una tasa aproximada a la que las solicitudes que cumplen esta política devuelven errores (código de estado HTTP >= 400) a los clientes.
   - Duración media de las solicitudes (sin errores): este gráfico muestra la duración media de las solicitudes correctas que cumplen esta política.
   - Uso del ancho de banda de la política: Este gráfico muestra la cantidad de ancho de banda correspondiente a esta política gestionada por todos los equilibradores de carga. Los datos recibidos incluyen los encabezados de las solicitudes y el tamaño del cuerpo de las respuestas que tienen datos en el cuerpo. Los datos enviados incluyen los encabezados de las respuestas y el tamaño del cuerpo de las respuestas para las solicitudes que incluyen datos en el cuerpo de la respuesta.
4. Coloca el cursor sobre un gráfico de líneas para que aparezca una ventana emergente con los valores correspondientes a una parte concreta del gráfico.
5. Selecciona **Grafana dashboard** justo debajo del título Metrics para ver todos los gráficos de una política. Además de los cuatro gráficos de la pestaña **Metrics**, puedes ver dos gráficos más:
   - Tasa de solicitudes de escritura por tamaño de objeto: la tasa correspondiente a las solicitudes PUT/POST/DELETE que cumplen esta política. Al situar el cursor sobre una celda concreta, se muestran las tasas por segundo. Las tasas que se muestran al pasar el cursor por encima se redondean a números enteros y pueden indicar 0 aunque haya solicitudes distintas de cero en el bucket.
   - Tasa de solicitudes de lectura por tamaño de objeto: la tasa de solicitudes GET/HEAD que coinciden con esta política. Al colocarte sobre una celda individual, verás las tasas por segundo. Las tasas que se muestran en la vista al pasar el cursor se truncan a números enteros y podrían mostrar 0 si hay solicitudes distintas de cero en el bucket.
6. También puedes acceder a los gráficos desde el menú **Support**.
   a. Selecciona **Soporte** > **Herramientas** > **Métricas**.
   b. Selecciona **Política de clasificación del tráfico** en la sección **Grafana**.
   c. Selecciona la política en el menú situado en la parte superior izquierda de la página.
   d. ${post_edited_translations.segment}

      Las políticas de clasificación de tráfico se identifican por su ID. Los ID de las políticas se muestran en la página Políticas de clasificación de tráfico.

7. ${post_edited_translations.segment}

Cifrados admitidos para conexiones TLS salientes en StorageGRID

${post_edited_translations.segment}

Versiones compatibles de TLS

StorageGRID es compatible con TLS 1.2 y TLS 1.3 para conexiones con sistemas externos usados para la federación de identidades y Cloud Storage Pools.

Los algoritmos de cifrado TLS compatibles con sistemas externos se han seleccionado para garantizar la compatibilidad con una amplia gama de sistemas externos. Esta lista es más amplia que la de los algoritmos de cifrado compatibles con las aplicaciones cliente de S3. Para configurar los algoritmos de cifrado, ve a **Configuración** > **Seguridad** > **Ajustes de seguridad** y selecciona **Políticas de TLS y SSH**.

> Las opciones de configuración de TLS, como las versiones de protocolo, los cifrados, los algoritmos de intercambio de claves y los algoritmos MAC, no se pueden configurar en StorageGRID. Ponte en contacto con tu representante de cuenta de NetApp si tienes alguna solicitud específica sobre estos ajustes.

Beneficios de las conexiones HTTP activas, inactivas y concurrentes en StorageGRID

La forma en que configuras las conexiones HTTP puede afectar el rendimiento del sistema StorageGRID. Las configuraciones varían según si la conexión HTTP está activa o inactiva, o si tienes varias conexiones simultáneas.

Puedes identificar los beneficios de rendimiento para los siguientes tipos de conexiones HTTP:

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Conexiones HTTP simultáneas

Ventajas de mantener abiertas las conexiones HTTP inactivas

Mantén abiertas las conexiones HTTP cuando las aplicaciones cliente estén inactivas para permitir transacciones posteriores. Mantén 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.

${post_edited_translations.segment}

- ${post_edited_translations.segment}

  La reducción de la latencia es la principal ventaja, especialmente por el tiempo que se necesita para establecer conexiones TCP/IP y TLS.

- Aumento de la tasa de transferencia de datos al preparar el algoritmo de inicio lento de TCP/IP con transferencias realizadas anteriormente
- 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 slow start y la asignación de recursos.

Ventajas de las conexiones HTTP activas

${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}

  Con el tiempo, puede que una conexión HTTP ya no sea óptima a medida que cambian los requisitos de balanceo de carga. El sistema realiza su mejor balanceo de carga cuando las aplicaciones cliente establecen una conexión HTTP independiente para cada transacción, pero este método anula las valiosas ventajas asociadas con las conexiones persistentes.

- ${post_edited_translations.segment}
- Permite iniciar los procedimientos de mantenimiento.

  Algunos procedimientos de mantenimiento solo comienzan después de que se completan todas las conexiones HTTP en curso.

En el caso de las conexiones de los clientes al servicio Load Balancer, limitar la duración de las conexiones abiertas puede ser útil para permitir que algunos procedimientos de mantenimiento se inicien sin demora. Si no se limita la duración de las conexiones de los clientes, las conexiones activas pueden tardar varios minutos en cerrarse automáticamente.

${post_edited_translations.segment}

Debes mantener abiertas varias conexiones TCP/IP con el 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 ofrecen las siguientes ventajas:

- Latencia reducida

  Las transacciones pueden iniciarse de inmediato en lugar de esperar a que se completen otras transacciones.

- Aumento del rendimiento

  El sistema StorageGRID puede realizar transacciones en paralelo y aumentar el rendimiento global de las transacciones.

Las aplicaciones cliente deberían establecer varias conexiones HTTP. Cuando una aplicación cliente tenga que realizar una transacción, puede seleccionar y usar inmediatamente cualquier conexión establecida que no esté procesando una transacción en ese momento.

La topología de cada sistema StorageGRID tiene un rendimiento máximo diferente para las transacciones y conexiones simultáneas. El rendimiento máximo depende de la computación, la red, los recursos de

almacenamiento, los enlaces WAN y el número de servidores, servicios y aplicaciones que admite el sistema StorageGRID.

Los sistemas StorageGRID suelen admitir varias aplicaciones cliente. Ten esto en cuenta cuando determines el número máximo de conexiones simultáneas. Si la aplicación cliente consta de varias entidades de software y cada una de ellas establece conexiones con el sistema StorageGRID, suma todas las conexiones de las distintas entidades. Es posible que tengas que ajustar el número máximo de conexiones simultáneas en las siguientes situaciones:

- La topología del sistema StorageGRID influye en el número máximo de transacciones y conexiones simultáneas que el sistema puede admitir.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

${post_edited_translations.segment}

Puedes usar pools de conexiones HTTP independientes para las operaciones de lectura y escritura, y controlar qué parte de un pool utilizar para cada una. Los pools de conexiones HTTP independientes te permiten controlar mejor las transacciones y equilibrar las cargas.

Las aplicaciones cliente pueden generar cargas en las que predomine la recuperación de datos (lectura) o el almacenamiento de datos (escritura). Con grupos separados de conexiones HTTP para las transacciones de lectura y escritura, puedes ajustar cuánto de cada grupo se dedica a las transacciones de lectura o escritura.

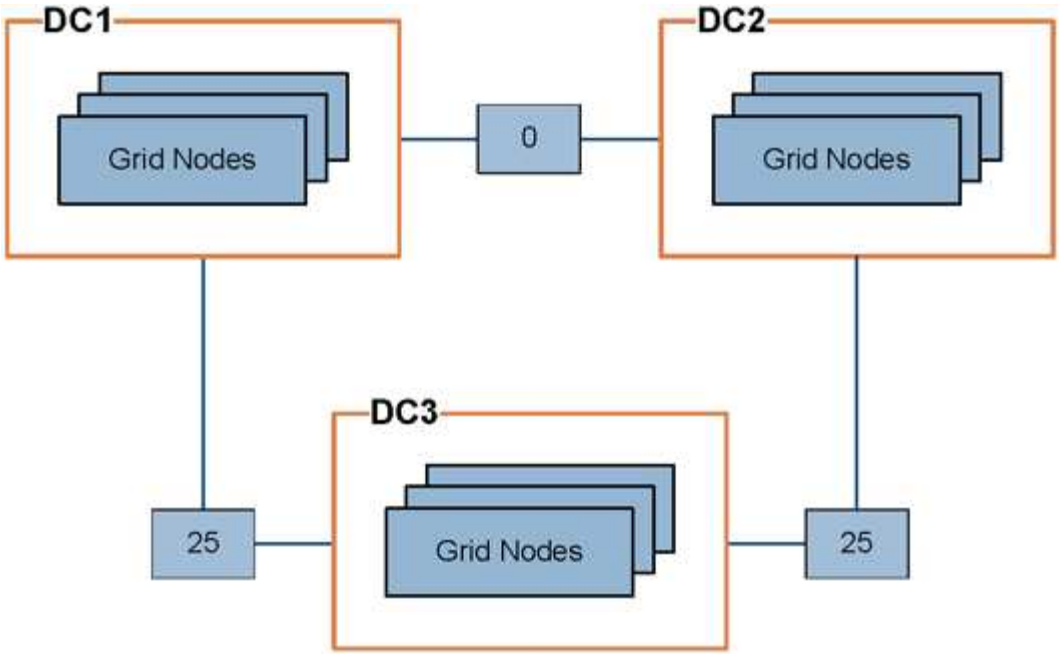
Administra los costes de enlace en StorageGRID

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

¿Qué son los costes de enlace?

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- El servicio Load Balancer en los nodos de administración y los nodos de puerta de enlace utiliza los costes de enlace para dirigir las conexiones de clientes. Consulta "Aspectos a tener en cuenta para el equilibrio de carga".

El diagrama muestra una red de tres sitios en la que se han configurado los costes de enlace entre los sitios:



- El servicio de equilibrio de carga en los nodos de administración y los nodos de puerta de enlace distribuye por igual las conexiones de los clientes a todos los nodos de almacenamiento en el mismo sitio del centro de datos y a cualquier sitio de centro de datos con un coste de enlace de 0.

  En el ejemplo, un nodo de puerta de enlace en el centro de datos 1 (DC1) distribuye de forma equitativa las conexiones de los clientes a los nodos de almacenamiento en DC1 y a los nodos de almacenamiento en DC2. Un nodo de puerta de enlace en DC3 envía las conexiones de los clientes solo a los nodos de almacenamiento en DC3.

- Al recuperar un objeto del que existen varias copias replicadas, StorageGRID recupera la copia del centro de datos que tiene el menor coste de enlace.

  En el ejemplo, si una aplicación cliente en DC2 recupera un objeto que está almacenado tanto en DC1 como en DC3, el objeto se recupera de DC1, porque el coste de enlace de DC1 a DC2 es 0, que es menor que el coste de enlace de DC3 a DC2 (25).

Los costes de enlace son valores numéricos relativos arbitrarios que carecen de una unidad de medida específica. Por ejemplo, un coste de enlace de 50 se utiliza con menos preferencia que un coste de 25. La tabla muestra los costes de enlace más habituales.

${post_edited_translations.segment}	**${post_edited_translations.segment}**	**Notas**
Entre los sitios físicos del centro de datos	${post_edited_translations.segment}	${post_edited_translations.segment}
Entre centros de datos lógicos en la misma ubicación física	0	Centros de datos lógicos en el mismo edificio físico o campus conectados por una LAN.

Actualizar los costes de los enlaces

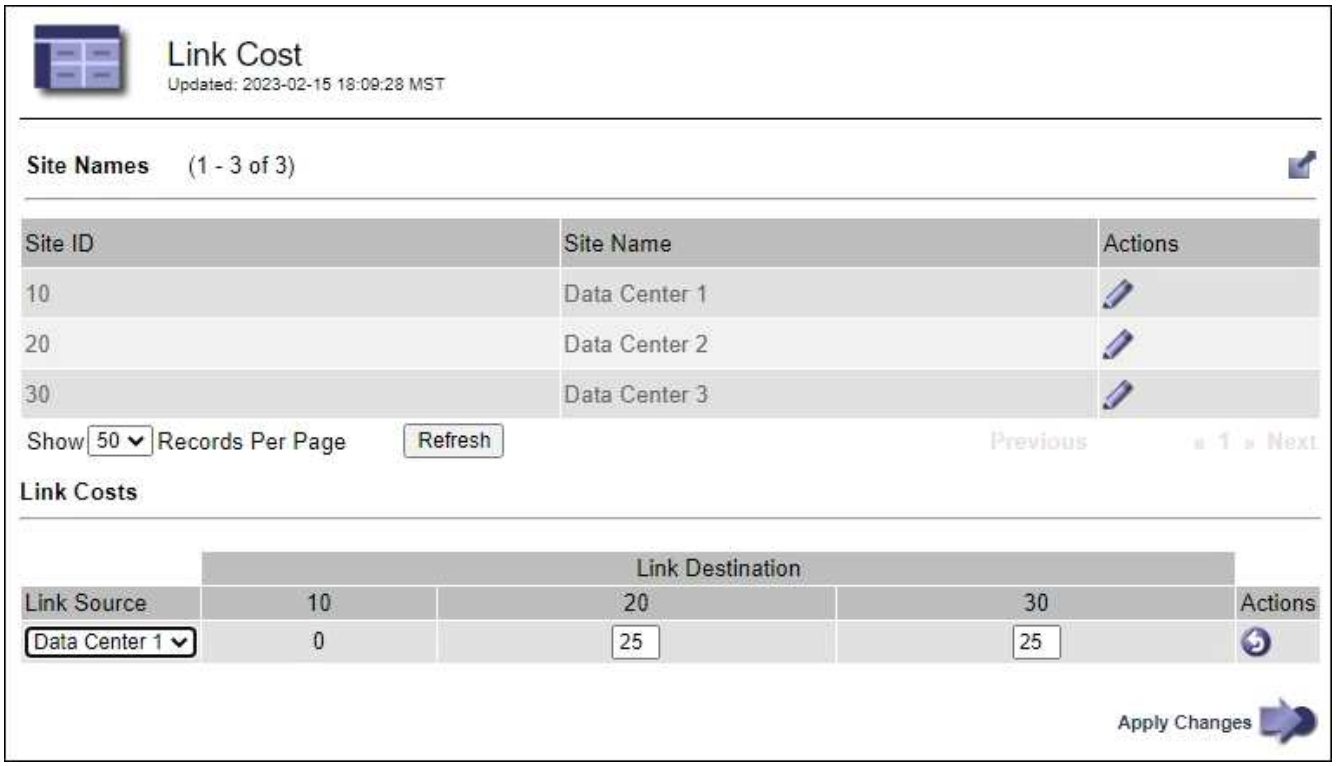
${post_edited_translations.segment}

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "${post_edited_translations.segment}".

Pasos

1. ${post_edited_translations.segment}



2. Selecciona un sitio en **Origen del enlace** e introduce un valor de coste comprendido entre 0 y 100 en **Destino del enlace**.

   No puedes cambiar el coste del enlace si el origen es el mismo que el destino.

   Para cancelar los cambios, selecciona **Revert**.

3. Selecciona **Aplicar cambios**.

Usa AutoSupport

Conoce AutoSupport en StorageGRID

La función AutoSupport permite que StorageGRID envíe paquetes de estado y salud al soporte técnico de NetApp.

Usar AutoSupport ayuda a resolver los problemas más rápido. El soporte técnico puede supervisar las necesidades de almacenamiento de tu sistema y ayudarte a determinar si necesitas añadir nuevos nodos o sitios. Opcionalmente, AutoSupport puede enviar paquetes a un destino adicional.

StorageGRID tiene dos tipos de AutoSupport:

- **StorageGRID AutoSupport** informa de los problemas de software de StorageGRID. Activado de forma predeterminada la primera vez que instalas StorageGRID. Puedes "cambia la configuración predeterminada de AutoSupport" si lo necesitas.

> Si StorageGRID AutoSupport no está habilitado, aparece un mensaje en el panel de control de Grid Manager. El mensaje incluye un enlace a la página de configuración de AutoSupport. Si cierras el mensaje, no volverá a aparecer hasta que se borre la caché del navegador, incluso si AutoSupport sigue deshabilitado.

- El **AutoSupport de hardware del appliance** informa de los problemas del appliance StorageGRID. Debes "Configura el hardware AutoSupport en cada dispositivo".

¿Qué es Active IQ?

Active IQ es un asesor digital basado en cloud que aprovecha el análisis predictivo y la sabiduría colectiva de la base instalada de NetApp. Sus evaluaciones continuas de riesgos, alertas predictivas, orientación prescriptiva y acciones automatizadas te ayudan a prevenir problemas antes de que ocurran, lo que lleva a una mejor salud del sistema y una mayor disponibilidad del sistema.

Si deseas utilizar los paneles de control y las funciones de Active IQ en el sitio de soporte de NetApp, debes activar AutoSupport.

"${post_edited_translations.segment}"

Información incluida en el paquete AutoSupport

Un paquete de AutoSupport contiene los siguientes archivos y detalles.

Nombre del archivo	Campos	Descripción
${post_edited_translations.segment}	Número de secuencia de AutoSupport + destino para este AutoSupport + estado de la entrega + intentos de entrega + asunto de AutoSupport + URI de entrega + último error + nombre de archivo PUT de AutoSupport + hora de generación + tamaño comprimido de AutoSupport + tamaño descomprimido de AutoSupport + tiempo total de recopilación (ms)	Archivo de historial de AutoSupport.

Nombre del archivo	Campos	Descripción
${post_edited_translations.segment}	Nodo + Protocolo para contactar soporte técnico + URL de soporte técnico para HTTP/HTTPS + Dirección de soporte técnico + AutoSupport OnDemand estado + AutoSupport OnDemand URL del servidor + AutoSupport OnDemand intervalo de sondeo	Archivo de estado de AutoSupport. Proporciona detalles del protocolo utilizado, la dirección y URL de soporte técnico, el intervalo de sondeo y si OnDemand AutoSupport está habilitado o deshabilitado.
BUCKETS.XML	ID del bucket + ID de la cuenta + Versión de compilación + Configuración de restricción de ubicación + Cumplimiento activado + Configuración de cumplimiento + Bloqueo de objetos S3 activado + Configuración de bloqueo de objetos S3 + Configuración de consistencia + CORS activado + Configuración de CORS + Tiempo de último acceso activado + Política activada + Configuración de política + Notificaciones activadas + Configuración de notificaciones + Cloud Mirror activado + Configuración de Cloud Mirror + Búsqueda activada + Configuración de búsqueda + Etiquetado de bucket activado + Configuración de etiquetado de bucket + Configuración de versionado	Proporciona detalles de configuración y estadísticas a nivel de bucket. Los ejemplos de configuraciones de bucket incluyen servicios de plataforma, cumplimiento y consistencia de bucket.
GRID-CONFIGURATIONS.XML	ID del atributo + Nombre del atributo + Valor + Índice + ID de la tabla + Nombre de la tabla	Archivo de configuración para toda la red. Contiene información sobre los certificados de la red, el espacio reservado para metadatos, los parámetros de configuración para toda la red (cumplimiento, S3 Object Lock, compresión de objetos, alertas, syslog y configuración de ILM), detalles del perfil de código de borrado, el nombre DNS y "Nombre de la NMS".

Nombre del archivo	Campos	Descripción
GRID-SPEC.XML	Especificaciones de grid, XML sin procesar	Se utiliza para configurar e implementar StorageGRID. Contiene las especificaciones de grid, la dirección IP del servidor NTP, la dirección IP del servidor DNS, la topología de red y los perfiles de hardware de los nodos.
GRID-TASKS.XML	Nodo + Ruta del servicio + ID del atributo + Nombre del atributo + Valor + Índice + ID de la tabla + Nombre de la tabla	Archivo de estado de las tareas de grid (procedimientos de mantenimiento). Proporciona detalles sobre las tareas activas, finalizadas, completadas, fallidas y pendientes de grid.
GRID.JSON	Grid + Revisión + Versión del software + Descripción + Licencia + Contraseñas + DNS + NTP + Sitios + Nodos	${post_edited_translations.segment}
ILM-CONFIGURATION.XML	ID del atributo + Nombre del atributo + Valor + Índice + ID de la tabla + Nombre de la tabla	${post_edited_translations.segment}
${post_edited_translations.segment}	${post_edited_translations.segment}	Archivo de información de métricas de ILM. Contiene las tasas de evaluación de ILM para cada nodo y las métricas de todo el grid.
${post_edited_translations.segment}	XML sin procesar de ILM	Archivo de políticas activas de ILM. Contiene información detallada sobre las políticas activas de ILM, como el ID del grupo 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.
MANIFEST.XML	Orden de recopilación + Nombre de archivo de contenido de AutoSupport para estos datos + Descripción de este elemento de datos + Número de bytes recopilados + Tiempo empleado en la recopilación + Estado de este elemento de datos + Descripción del error + Tipo de contenido de AutoSupport para estos datos	Contiene metadatos de AutoSupport y descripciones breves de todos los archivos de AutoSupport.

Nombre del archivo	Campos	Descripción
NMS-ENTITIES.XML	Índice de atributo + OID de la entidad + ID del nodo + ID del modelo del dispositivo + Versión del modelo del dispositivo + Nombre de la entidad	Entidades de grupo y de servicio en el "Árbol NMS". Proporciona detalles de la topología de grid. El nodo se puede determinar según los servicios que se ejecutan en el nodo.
${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	${post_edited_translations.segment}	Configuraciones del servidor. Contiene los siguientes datos 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 error del controlador de almacenamiento, temperatura del chasis del controlador de cómputo, hardware de cómputo, número de serie del controlador de cómputo, fuente de alimentación, tamaño de la unidad y tipo de unidad.
SERVICE-STATUS.XML	${post_edited_translations.segment}	Archivo de información del nodo de servicio. Contiene detalles como el espacio de tabla asignado, el espacio de tabla libre, las métricas de Reaper de la base de datos, la duración de la reparación de segmentos, la duración del trabajo de reparación, los reinicios automáticos de trabajos y la finalización automática de trabajos.
${post_edited_translations.segment}	ID de nivel de almacenamiento + Nombre del nivel de almacenamiento + ID del nodo de almacenamiento + Ruta del nodo de almacenamiento	${post_edited_translations.segment}
${post_edited_translations.segment}	${post_edited_translations.segment}	Datos a grandes rasgos sobre el estado del sistema que resumen la información de uso de StorageGRID. Proporciona detalles como el nombre de grid, los nombres de los sitios, el número de Storage Nodes por grid y por sitio, el tipo de licencia, la capacidad y el uso de la licencia, las condiciones de soporte técnico del software y los detalles de las operaciones S3.

Nombre del archivo	Campos	Descripción
SYSTEM-ALERTS.XML	${post_edited_translations.segment}	Alertas actuales del sistema que indican posibles problemas en el sistema StorageGRID.
USERAGENTS.XML	Agente de usuario + Número de días + Total de peticiones HTTP + Total de bytes ingeridos + Total de bytes recuperados + Peticiones PUT + Peticiones GET + Peticiones DELETE + Peticiones HEAD + Peticiones POST + Peticiones OPTIONS + Tiempo medio de petición (ms) + Tiempo medio de petición PUT (ms) + Tiempo medio de petición GET (ms) + Tiempo medio de petición DELETE (ms) + Tiempo medio de petición HEAD (ms) + Tiempo medio de petición POST (ms) + Tiempo medio de petición OPTIONS (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 en bytes de cada operación.
X-HEADER-DATA	${post_edited_translations.segment}	Datos de cabecera de AutoSupport.

Configura AutoSupport en StorageGRID

De forma predeterminada, la función AutoSupport de StorageGRID está habilitada cuando instalas StorageGRID por primera vez. Sin embargo, debes configurar el hardware AutoSupport en cada appliance. Si lo necesitas, puedes cambiar la configuración de AutoSupport.

Si quieres cambiar la configuración de StorageGRID AutoSupport, realiza tus cambios solo en el nodo de administración primario. Debes configura el hardware AutoSupport en cada appliance.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".
- Si vas a utilizar HTTPS para enviar paquetes de AutoSupport, has proporcionado acceso saliente a internet al nodo de administración primario, ya sea directamente o "${post_edited_translations.segment}" (no se requieren conexiones entrantes).
- Si se selecciona HTTP en la página de StorageGRID AutoSupport, tienes "configuraste un servidor proxy" para reenviar los paquetes de AutoSupport como HTTPS. Los servidores de NetApp AutoSupport rechazarán los paquetes enviados mediante HTTP.
- Si vas a utilizar SMTP como protocolo para los paquetes de AutoSupport, ya has configurado un servidor

de correo SMTP.

Acerca de esta tarea

Puedes usar cualquier combinación de las siguientes opciones para enviar paquetes de AutoSupport al soporte técnico:

- **Semanal**: envía automáticamente paquetes de AutoSupport una vez a la semana. Configuración predeterminada: habilitado.
- **Activado por eventos**: envía automáticamente paquetes de AutoSupport cada hora o cuando ocurran eventos importantes del sistema. Configuración predeterminada: habilitado.
- **Bajo demanda**: Permite que el soporte técnico solicite que tu sistema StorageGRID envíe automáticamente paquetes de AutoSupport, lo cual resulta útil cuando están trabajando activamente en un problema (requiere el protocolo de transmisión HTTPS AutoSupport). Configuración predeterminada: desactivado.
- **Activado por el usuario**: envía manualmente paquetes de AutoSupport en cualquier momento.
- **Recopilación de registros**: "recopilar manualmente archivos de registro y datos del sistema y enviar un paquete de AutoSupport".

Especifica el protocolo para los paquetes de AutoSupport

Puedes utilizar cualquiera de los siguientes protocolos para enviar paquetes AutoSupport:

- **HTTPS**: Esta es la configuración predeterminada y recomendada para las nuevas instalaciones. Este protocolo utiliza el puerto 443. Si quieres habilita la función de AutoSupport on Demand, debes utilizar HTTPS.
- **HTTP**: Si seleccionas HTTP, debes configurar un servidor proxy para que reenvíe los paquetes de AutoSupport como HTTPS. Los servidores de NetApp AutoSupport rechazan los paquetes enviados mediante HTTP. Este protocolo utiliza el puerto 80.
- **SMTP**: usa esta opción si quieres que los paquetes de AutoSupport se envíen por correo electrónico.

El protocolo que configures se utiliza para enviar todo tipo de paquetes de AutoSupport.

Pasos

1. Selecciona **Soporte** > **Herramientas** > **AutoSupport** > **Configuración**.
2. Selecciona el protocolo que deseas utilizar para enviar paquetes AutoSupport.
3. Si has seleccionado **HTTPS**, indica si deseas utilizar un certificado de soporte de NetApp (certificado TLS) para proteger la conexión con el servidor de soporte técnico.
   - **Verificar certificado** (por defecto): garantiza que la transmisión de paquetes AutoSupport sea segura. El certificado de soporte de NetApp ya viene instalado con el software StorageGRID.
   - ${post_edited_translations.segment}
4. Selecciona **Guardar**. Todos los paquetes semanales, activados por el usuario y activados por eventos se envían mediante el protocolo seleccionado.

Desactivar el AutoSupport semanal

De forma predeterminada, el sistema StorageGRID está configurado para enviar un paquete de AutoSupport al soporte técnico una vez a la semana.

Para saber cuándo se enviará el paquete semanal de AutoSupport, ve a la pestaña **AutoSupport** > **Results**.

En la sección **Weekly AutoSupport**, consulta el valor de **Next Scheduled Time**.

Puedes desactivar el envío automático de los paquetes semanales de AutoSupport en cualquier momento.

Pasos

1. Selecciona **Soporte** > **Herramientas** > **AutoSupport** > **Configuración**.
2. Desmarca la casilla **Habilitar AutoSupport semanal**.
3. Selecciona **Guardar**.

Desactivar AutoSupport activado por eventos

De forma predeterminada, el sistema StorageGRID está configurado para enviar un paquete de AutoSupport al soporte técnico cada hora.

Puedes desactivar AutoSupport activado por eventos en cualquier momento.

Pasos

1. Selecciona **Soporte** > **Herramientas** > **AutoSupport** > **Configuración**.
2. Desmarca la casilla de verificación **Habilitar AutoSupport activado por eventos**.
3. Selecciona **Guardar**.

Habilita AutoSupport bajo demanda

AutoSupport on Demand puede ayudarte a resolver los problemas en los que el soporte técnico esté trabajando activamente.

De forma predeterminada, AutoSupport on Demand está desactivado. Activar esta función permite al soporte técnico solicitar que tu sistema StorageGRID envíe paquetes de AutoSupport de forma automática. El soporte técnico también puede establecer el intervalo de tiempo de sondeo para las consultas de AutoSupport on Demand.

El soporte técnico no puede activar ni desactivar AutoSupport on Demand.

Pasos

1. Selecciona **Soporte** > **Herramientas** > **AutoSupport** > **Configuración**.
2. Selecciona **HTTPS** para el protocolo.
3. Selecciona la casilla **Habilitar AutoSupport semanal**.
4. Selecciona la casilla **Enable AutoSupport on Demand**.
5. Selecciona **Guardar**.

   AutoSupport on Demand está activado, y el soporte técnico puede enviar solicitudes de AutoSupport on Demand a StorageGRID.

Desactivar la comprobación de actualizaciones de software

De forma predeterminada, StorageGRID se comunica con NetApp para determinar si hay actualizaciones de software disponibles para tu sistema. Si hay disponible una corrección urgente o una nueva versión de StorageGRID, la nueva versión se muestra en la página de actualización de StorageGRID.

Si lo deseas, puedes desactivar la comprobación de actualizaciones de software. Por ejemplo, si tu sistema no

dispone de acceso a la WAN, deberías desactivar la comprobación para evitar errores de descarga.

Pasos

1. Selecciona **Soporte** > **Herramientas** > **AutoSupport** > **Configuración**.
2. Desmarca la casilla **Buscar actualizaciones de software**.
3. Selecciona **Guardar**.

Añade un destino de AutoSupport adicional

Cuando activas AutoSupport, los paquetes de estado y salud se envían al soporte técnico. Puedes especificar un destino adicional para todos los paquetes de AutoSupport.

Para comprobar o cambiar el protocolo utilizado para enviar paquetes de AutoSupport, consulta las instrucciones para especifica el protocolo para los paquetes de AutoSupport.

> No puedes usar el protocolo SMTP para enviar paquetes de AutoSupport a un destino adicional.

Pasos

1. Selecciona **Soporte** > **Herramientas** > **AutoSupport** > **Configuración**.
2. Selecciona **Activar destino adicional de AutoSupport**.
3. Especifica lo siguiente:

   Nombre de host
   El nombre de host o la dirección IP de un servidor de destino adicional de AutoSupport.

   > Solo puedes introducir un destino adicional.

   Puerto
   El puerto que se utiliza para conectarse a un servidor de destino adicional de AutoSupport. El valor predeterminado es el puerto 80 para HTTP o el puerto 443 para HTTPS.

   Validación del certificado
   Si se utiliza un certificado TLS para proteger la conexión con el destino adicional.

   - Selecciona **Verificar certificado** para usar la validación de certificados.
   - Selecciona **No verificar certificado** para enviar tus paquetes de AutoSupport sin validación del certificado.

     Selecciona esta opción solo cuando tengas una buena razón para no utilizar la validación de certificados, como cuando haya un problema temporal con un certificado.

4. Si seleccionaste **Verificar certificado**, haz lo siguiente:
   a. Busca la ubicación del certificado de la CA.
   b. Sube el archivo del certificado de la CA.

      Aparecen los metadatos del certificado de la CA.

5. Selecciona **Guardar**.

Todos los futuros paquetes semanales, activados por eventos y por el usuario de AutoSupport se enviarán al destino adicional.

Configura AutoSupport para dispositivos

AutoSupport para los dispositivos informa sobre problemas de hardware de StorageGRID, y StorageGRID AutoSupport informa sobre problemas de software de StorageGRID, con una excepción: para el SGF6112, StorageGRID AutoSupport informa tanto de problemas de hardware como de software. Debes configurar AutoSupport en cada dispositivo excepto en el SGF6112, que no requiere configuración adicional. AutoSupport se implementa de forma diferente para los dispositivos de servicios y los dispositivos de almacenamiento.

Usa SANtricity para habilitar AutoSupport en cada dispositivo de almacenamiento. Puedes configurar SANtricity AutoSupport durante la configuración inicial del dispositivo o después de que se haya instalado:

- Para los dispositivos SG6000 y SG5700, "configura AutoSupport en SANtricity System Manager"

Los paquetes de AutoSupport de los dispositivos E-Series se pueden incluir en StorageGRID AutoSupport si configuras la entrega de AutoSupport mediante proxy en "SANtricity System Manager".

StorageGRID AutoSupport no notifica problemas de hardware, como fallos en los módulos DIMM o en las tarjetas de interfaz del host (HIC). Sin embargo, algunos fallos de componentes podrían activar "alertas de hardware". Para los dispositivos StorageGRID con un controlador de gestión de placa base (BMC), puedes configurar notificaciones por correo electrónico y trampas SNMP para informar de fallos de hardware:

- "Configura notificaciones por correo electrónico para alertas de BMC"
- "Configura los ajustes de SNMP para BMC"

Información relacionada

"Soporte de NetApp"

Activar manualmente un paquete de AutoSupport en StorageGRID

Para ayudar al soporte técnico a solucionar problemas con tu sistema StorageGRID, puedes activar manualmente el envío de un paquete de AutoSupport.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes acceso Root u otro permiso de configuración de grid.

Pasos

1. Selecciona **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 tiene éxito, se actualizan los valores de **Resultado más reciente** y **Hora del último éxito** en la pestaña **Resultados**. Si hay algún problema, el valor de **Resultado más reciente** se actualiza a "Fallido" y StorageGRID no vuelve a intentar enviar el paquete de AutoSupport.

3. Después de 1 minuto, actualiza la página AutoSupport en tu navegador para acceder a los resultados más recientes.

Además, puedes "${post_edited_translations.segment}" y enviarlos al sitio de soporte de NetApp.

Soluciona problemas de los paquetes StorageGRID AutoSupport

Si un intento de enviar un paquete de AutoSupport falla, el sistema StorageGRID realiza diferentes acciones según el tipo de paquete de AutoSupport. Puedes comprobar el estado de los paquetes de AutoSupport seleccionando **Support** > **Tools** > **AutoSupport** > **Results**.

Cuando el paquete AutoSupport no se envía, aparece "Failed" en la pestaña **Resultados** de la página **AutoSupport**.

Si configuraste un servidor proxy para reenviar paquetes de AutoSupport a NetApp, debes "Verifica que los parámetros de configuración del servidor proxy sean correctos".

Fallo del paquete semanal de AutoSupport

Si un paquete semanal de AutoSupport no se envía, el sistema StorageGRID realiza las siguientes acciones:

1. Actualiza el atributo «Resultado más reciente» a «Reintentando».
2. Intenta reenviar el paquete de AutoSupport 15 veces cada cuatro minutos durante una hora.
3. ${post_edited_translations.segment}
4. Intenta enviar de nuevo un paquete de AutoSupport en la siguiente hora programada.
5. Mantiene la programación habitual de AutoSupport si el paquete falla porque el servicio NMS no está disponible, y si se envía un paquete antes de que pasen siete días.
6. Cuando el servicio NMS vuelva a estar disponible, envía inmediatamente un paquete AutoSupport si no se ha enviado ningún paquete durante siete días o más.

Error en el paquete AutoSupport provocado por el usuario o por un evento

Si un paquete de AutoSupport activado por el usuario o por un evento no se envía correctamente, el sistema StorageGRID toma las siguientes acciones:

1. Muestra un mensaje de error si el error es conocido. Por ejemplo, si un usuario selecciona el protocolo SMTP sin introducir los parámetros de configuración de correo electrónico correctos, se muestra el siguiente error: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. ${post_edited_translations.segment}
3. Registra el error en `nms.log`.

Si se produce un fallo y el protocolo seleccionado es SMTP, comprueba que el servidor de correo electrónico del sistema StorageGRID esté correctamente configurado y que tu servidor de correo electrónico esté en funcionamiento (**Soporte** > **Alarmas (heredadas)** > **Configuración de correo electrónico heredada**). Es posible que aparezca 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.`

Aprende cómo "configurar los ajustes del servidor de correo electrónico".

Corrige un fallo de paquete de AutoSupport

Si se produce un fallo y SMTP es el protocolo seleccionado, comprueba que el servidor de correo electrónico del sistema StorageGRID esté configurado correctamente y que tu servidor de correo electrónico esté funcionando. Es posible que aparezca el siguiente mensaje de error en la página de AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envía paquetes de E-Series AutoSupport a través de StorageGRID

Puedes enviar paquetes de AutoSupport de SANtricity System Manager de E-Series al soporte técnico a través de un nodo de administración de StorageGRID en lugar de a través del puerto de gestión del dispositivo de almacenamiento.

Consulta "AutoSupport de hardware de E-Series" para obtener más información sobre cómo utilizar AutoSupport con los dispositivos de la E-Series.

Antes de empezar

- Has iniciado sesión en el Grid Manager utilizando un "navegador web compatible".
- Tienes el "Permiso de administrador de almacenamiento o acceso Root".
- Has configurado SANtricity AutoSupport:
  - Para los dispositivos SG6000 y SG5700, "configura AutoSupport en SANtricity System Manager"

> Debes disponer del firmware 8.70 o superior de SANtricity para acceder a SANtricity System Manager mediante Grid Manager.

Acerca de esta tarea

Los paquetes de E-Series AutoSupport contienen detalles del hardware de almacenamiento y son más específicos que otros paquetes de AutoSupport enviados por el sistema StorageGRID.

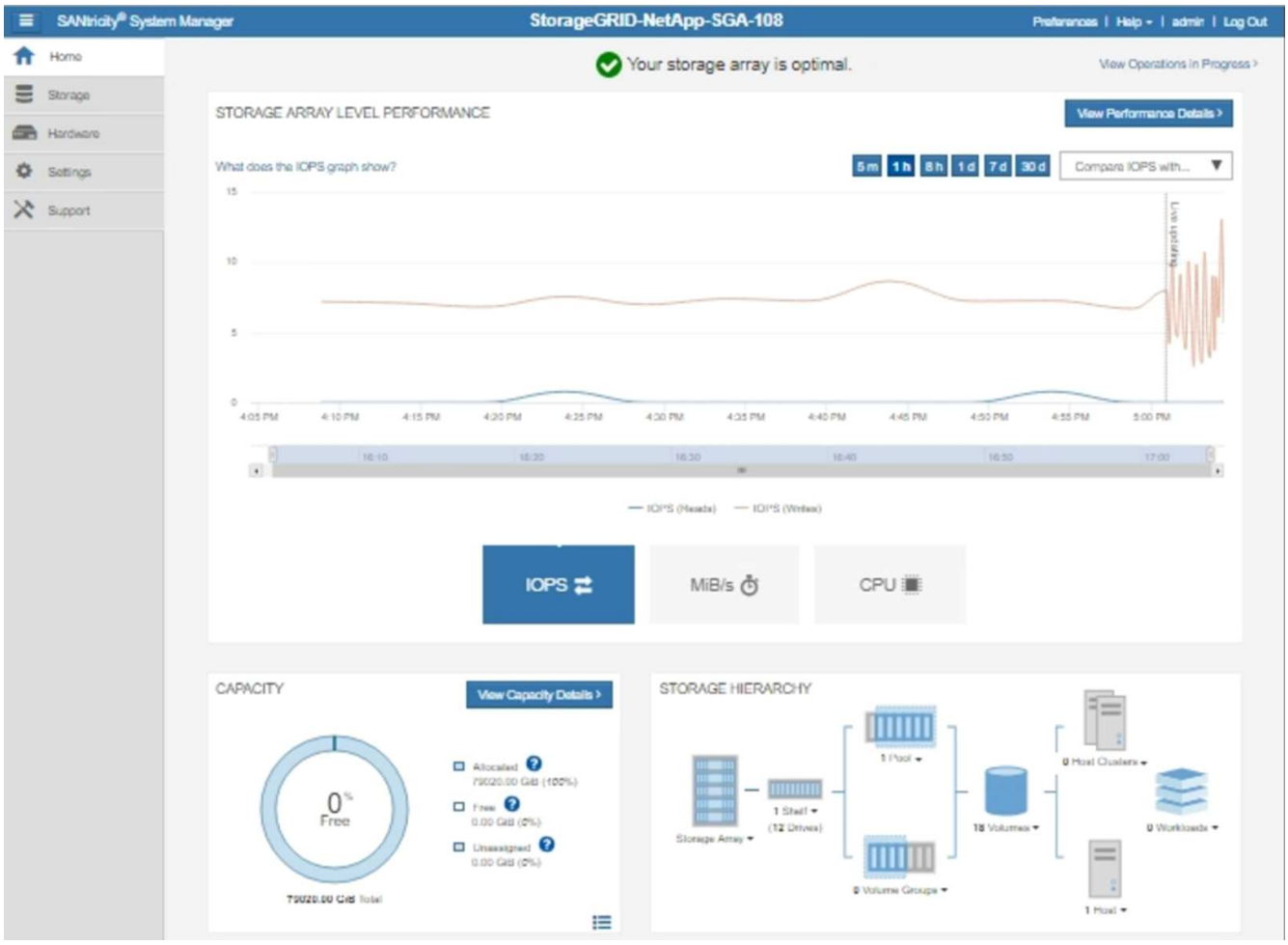
Puedes configurar una dirección de servidor proxy especial en SANtricity System Manager para transmitir paquetes de AutoSupport a través de un nodo de administración de StorageGRID sin usar el puerto de gestión del dispositivo. AutoSupport packages transmitidos de esta manera son enviados por el "Remitente preferido Admin Node" y utilizan cualquier "Configuración del proxy de administrador" que se haya configurado en el Grid Manager.

> Este procedimiento solo es para configurar un servidor proxy de StorageGRID para paquetes de E-Series AutoSupport. Para obtener más detalles sobre la configuración de E-Series AutoSupport, consulta el "NetApp E-Series y documentación de SANtricity".

Pasos

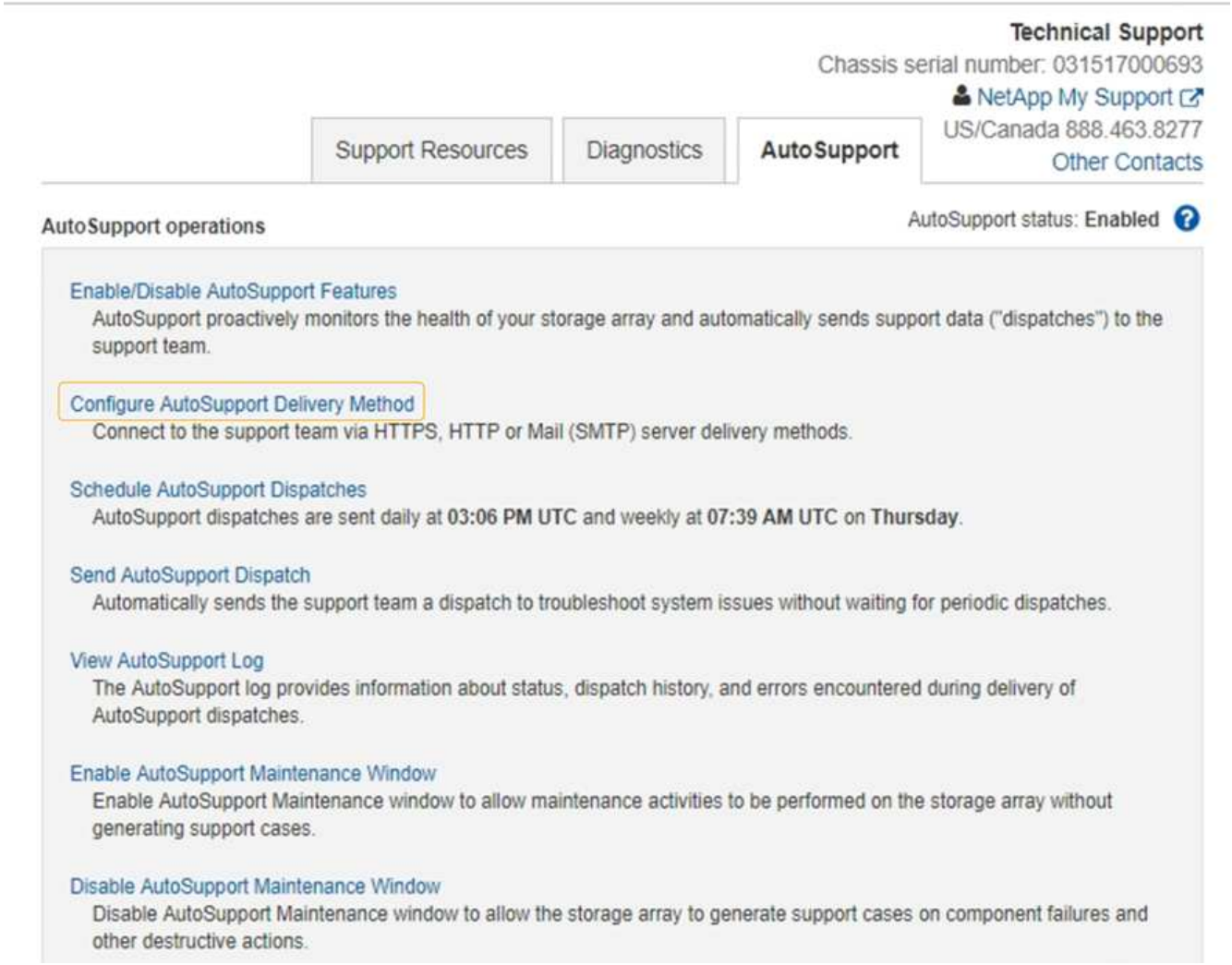
1. En el Grid Manager, selecciona **Nodos**.
2. En la lista de nodos de la izquierda, selecciona el nodo del dispositivo de almacenamiento que quieres configurar.
3. Selecciona **SANtricity System Manager**.

   Aparece la página de inicio de SANtricity System Manager.



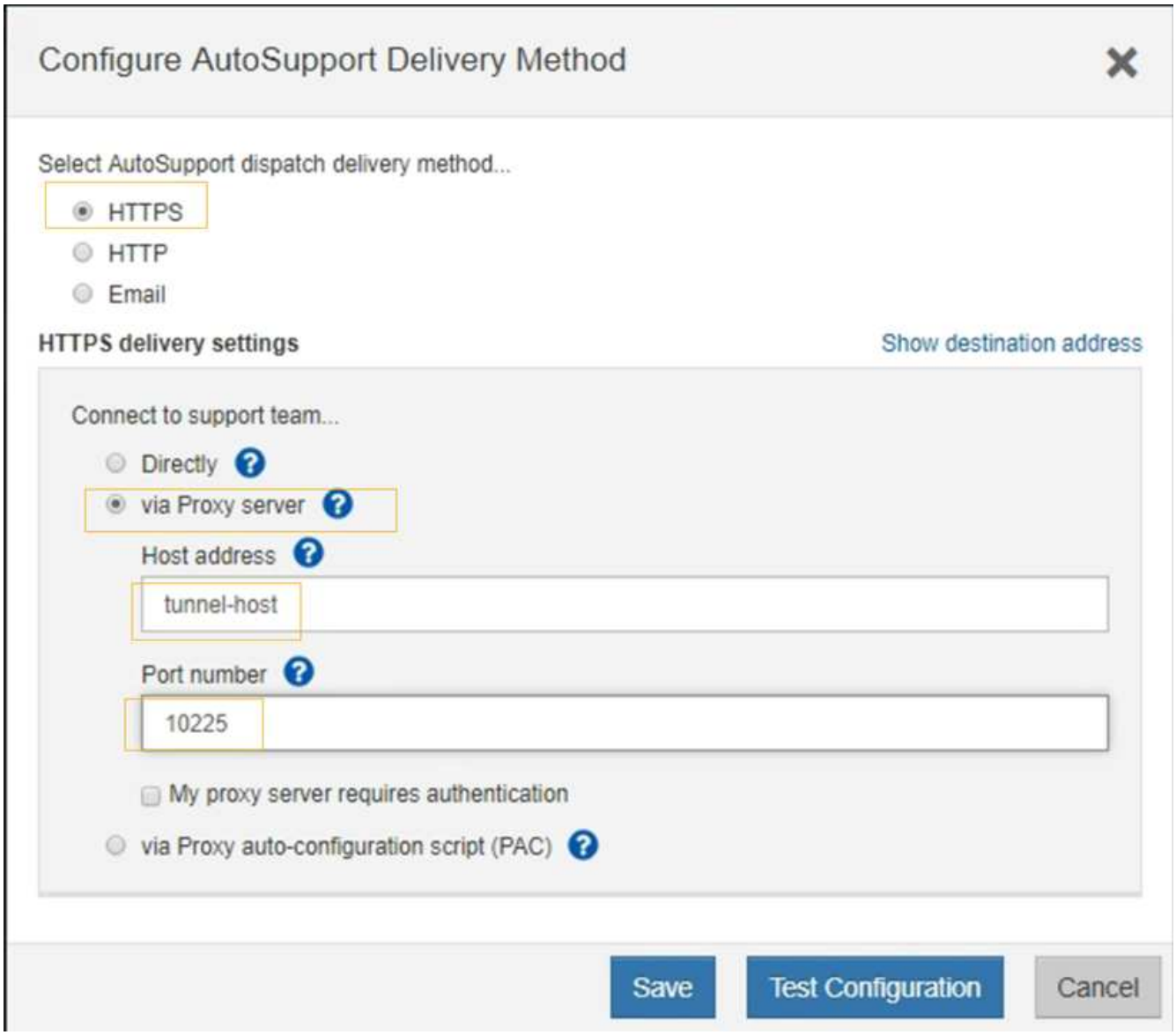
4. Selecciona **Asistencia** > **Centro de asistencia** > **AutoSupport**.

   Aparece la página de operaciones de AutoSupport.



5. Selecciona **Configurar método de entrega de AutoSupport**.

   Aparece la página Configurar el método de entrega de AutoSupport.



6. Selecciona **HTTPS** como método de entrega.

   El certificado que permite HTTPS viene preinstalado.

7. Selecciona **a través de un servidor proxy**.
8. Introduce `tunnel-host` para el campo **Dirección del servidor**.

   `tunnel-host` es la dirección especial que debes usar en un nodo de administración para enviar paquetes E-Series AutoSupport.

9. Introduce `10225` en el campo **Número de puerto**.

   `10225` es el número de puerto en el servidor proxy de StorageGRID que recibe los paquetes de AutoSupport del controlador E-Series en el dispositivo.

10. Selecciona **Test Configuration** para probar el enrutamiento y la configuración de tu servidor proxy de AutoSupport.

Si es correcta, aparece un mensaje en un banner verde: "Tu configuración de AutoSupport ha sido verificada."

Si la prueba falla, aparecerá un mensaje de error en un banner rojo. Comprueba la configuración de DNS y la red de StorageGRID, asegúrate de que "Remitente preferido Admin Node" pueda conectarse al sitio de soporte de NetApp y vuelve a intentar la prueba.

11. Selecciona **Guardar**.

    La configuración se guarda y aparece un mensaje de confirmación: «El método de entrega AutoSupport ha sido configurado.»

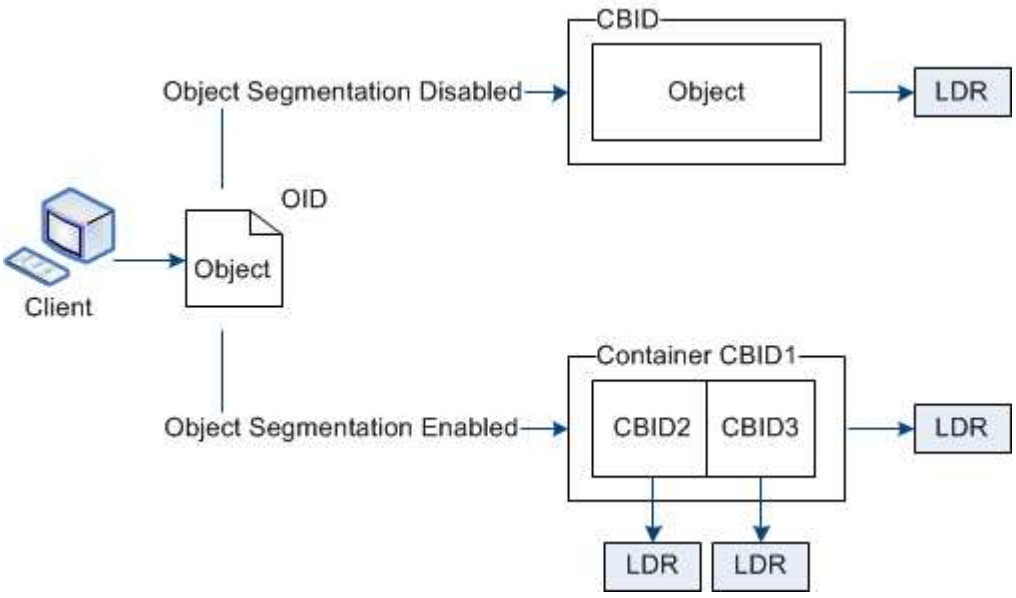
${post_edited_translations.segment}

${post_edited_translations.segment}

Conoce la segmentación de objetos en StorageGRID

La segmentación de objetos es el proceso de dividir un objeto en un conjunto de objetos más pequeños de tamaño fijo para optimizar el almacenamiento y el uso de recursos en objetos grandes. La carga multiparte de S3 también crea objetos segmentados, con un objeto que representa cada parte.

Cuando se incorpora un objeto al sistema StorageGRID, el servicio LDR divide el objeto en segmentos y crea un contenedor de segmentos que incluye como contenido la información de cabecera de todos los segmentos.



Al recuperar un contenedor de segmentos, el servicio LDR reconstruye el objeto original a partir 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 grupo de almacenamiento especificado en la regla de ILM.

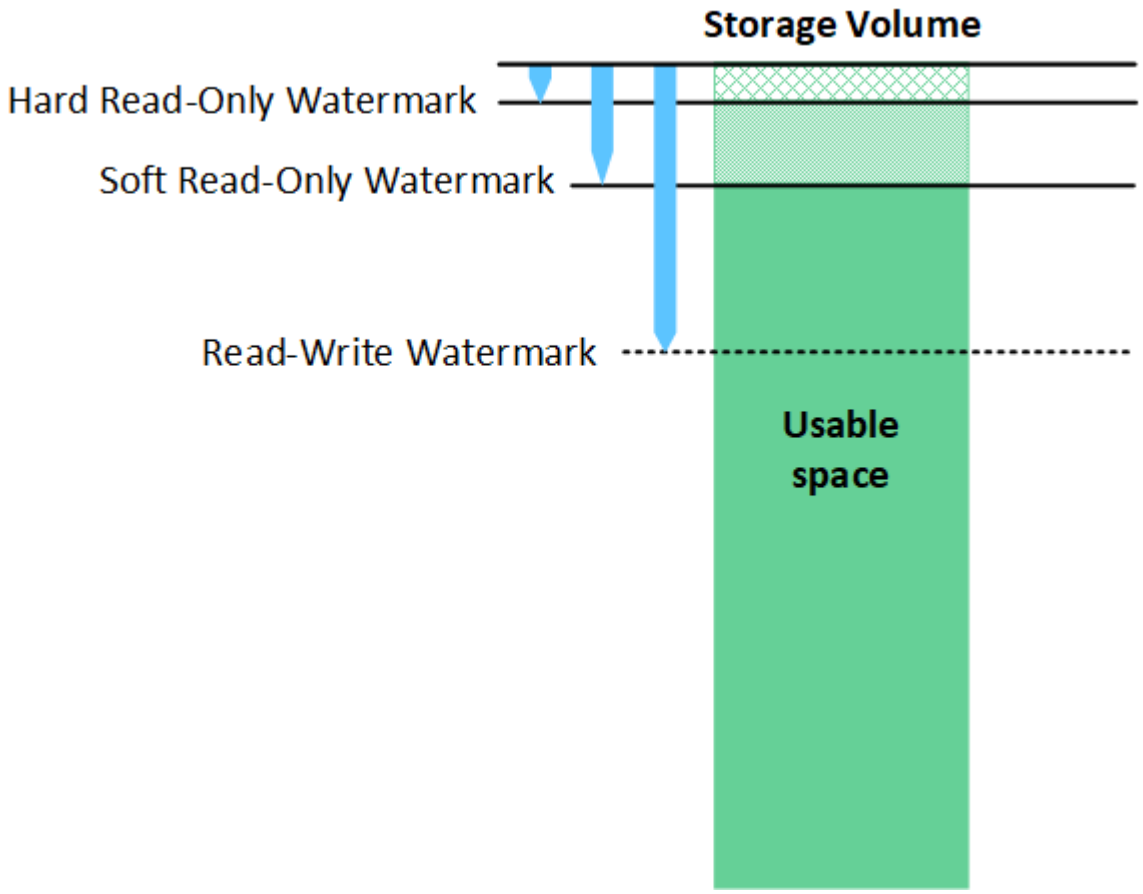
El sistema StorageGRID trata cada segmento de forma independiente y cada uno contribuye al recuento de

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 después de que la ingesta se complete, de la siguiente manera:

```
segment container + segment 1 + segment 2 = three stored objects
```

Conoce las marcas de agua de los volúmenes de almacenamiento en StorageGRID

StorageGRID utiliza tres umbrales de volumen de almacenamiento para garantizar que los nodos de almacenamiento pasen de forma segura a un estado de solo lectura antes de que se queden críticamente sin espacio y para permitir que los nodos de almacenamiento que hayan pasado a un estado de solo lectura vuelvan a estar en modo de lectura/escritura.



> Las marcas de agua de volumen de almacenamiento solo se aplican al espacio utilizado para los datos de objetos replicados y con código de borrado. Para obtener más información sobre el espacio reservado para los metadatos de los objetos en el volumen 0, visita "Gestiona el almacenamiento de metadatos de objetos".

¿Qué es la marca de agua soft de solo lectura?

La **marca de nivel de «solo lectura» del volumen de almacenamiento** es la primera marca que indica que el espacio útil de un Storage Node para datos de objetos se está llenando.

Si cada volumen de un nodo de almacenamiento tiene menos espacio libre que el umbral de solo lectura

flexible de dicho volumen, el nodo de almacenamiento pasa al *modo de solo lectura*. El modo de solo lectura significa que el nodo de almacenamiento ofrece servicios de solo lectura al resto del sistema StorageGRID, pero atiende todas las solicitudes de escritura pendientes.

Por ejemplo, supongamos que cada volumen en un Storage Node tiene un límite flexible de solo lectura de 10 GB. En cuanto cada volumen tenga menos de 10 GB de espacio libre, el Storage Node pasa al modo solo lectura flexible.

¿Qué es la marca de agua de solo lectura estricta?

El **umbral de solo lectura del volumen de almacenamiento** es el siguiente umbral que indica que el espacio utilizable de un nodo para datos de objetos se está llenando.

Si el espacio libre en un volumen es inferior a la marca de agua de solo lectura estricta de ese volumen, las escrituras en el volumen fallarán. Sin embargo, las escrituras en otros volúmenes pueden continuar hasta que el espacio libre en esos volúmenes sea inferior a sus marcas de agua de solo lectura estricta.

Por ejemplo, supongamos que cada volumen en un Storage Node tiene un límite mínimo de solo lectura de 5 GB. En cuanto cada volumen tenga menos de 5 GB de espacio libre, el Storage Node ya no acepta solicitudes de escritura.

El umbral de solo lectura duro siempre es menor que el umbral de solo lectura blando.

¿Qué es la marca de agua de lectura/escritura?

El **nivel de referencia de lectura/escritura del volumen de almacenamiento** solo se aplica a los nodos de almacenamiento que han pasado al modo de solo lectura. Determina cuándo el nodo puede volver a estar en modo de lectura/escritura. Cuando el espacio libre de cualquier volumen de almacenamiento de un nodo de almacenamiento es superior al nivel de referencia de lectura/escritura de ese volumen, el nodo vuelve automáticamente al estado de lectura/escritura.

Por ejemplo, supongamos que el nodo de almacenamiento ha pasado al modo de solo lectura. Supongamos también que cada volumen tiene un watermark de lectura/escritura de 30 GB. En cuanto el espacio libre de cualquier volumen aumenta a 30 GB, el nodo vuelve a estar en modo de lectura/escritura.

La marca de agua de lectura/escritura siempre es mayor que tanto la marca de agua blanda de solo lectura como la marca de agua dura de solo lectura.

Ver marcas de nivel de agua del volumen de almacenamiento

Puedes consultar la configuración actual de las marcas de agua y los valores optimizados por el sistema. Si no se están utilizando marcas de agua optimizadas, puedes determinar si puedes o debes ajustar la configuración.

Antes de empezar

- Has completado la actualización a StorageGRID 11.6 o una versión posterior.
- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso raíz".

Ver la configuración actual de la marca de agua

${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}
2. En la página de marcas de agua de almacenamiento, fíjate en la casilla de selección Usar valores optimizados.
   - Si se marca la casilla, 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 modifiques estos valores. Si lo deseas, puedes Ver marcas de agua de almacenamiento optimizadas.

   - Si la casilla «Usar valores optimizados» no está marcada, se están utilizando marcas de agua personalizadas (no optimizadas). No se recomienda utilizar ajustes de marcas de agua personalizadas. Sigue las instrucciones de "Solución de problemas de alertas de anulación de marcas de agua de solo lectura bajas" para determinar si puedes o debes ajustar la configuración.

     Al especificar ajustes personalizados para la marca de agua, debes introducir valores superiores a 0.

${post_edited_translations.segment}

StorageGRID utiliza dos métricas de Prometheus para mostrar los valores optimizados que ha calculado para el umbral de solo lectura (soft) del volumen de almacenamiento. Puedes consultar los valores optimizados mínimos y máximos para cada Storage Node en tu grid.

1. Selecciona **Soporte** > **Herramientas** > **Métricas**.
2. ${post_edited_translations.segment}
3. Para ver la marca de agua mínima recomendada de solo lectura, introduce la siguiente métrica de Prometheus y selecciona **Ejecutar**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   La última columna muestra el valor mínimo optimizado de la marca de agua de solo lectura flexible para todos los volúmenes de almacenamiento de cada Storage Node. Si este valor es mayor que el ajuste personalizado de la marca de agua de solo lectura flexible del volumen de almacenamiento, se activa la alerta **Low read-only watermark override** para el Storage Node.

4. ${post_edited_translations.segment}

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   ${post_edited_translations.segment}

Administra el almacenamiento de metadatos de objetos en StorageGRID

La capacidad de metadatos de objetos de un sistema StorageGRID controla el número máximo de objetos que se pueden almacenar en ese sistema. Para asegurarte de que tu sistema StorageGRID tenga espacio suficiente para almacenar objetos nuevos, debes comprender dónde y cómo almacena StorageGRID los metadatos de objetos.

¿Qué son los metadatos de un objeto?

Los metadatos de objetos son cualquier información que describe un objeto. StorageGRID utiliza los metadatos de objetos para realizar el seguimiento de las ubicaciones de todos los objetos en todo el grid y gestionar el ciclo de vida de cada objeto a lo largo del tiempo.

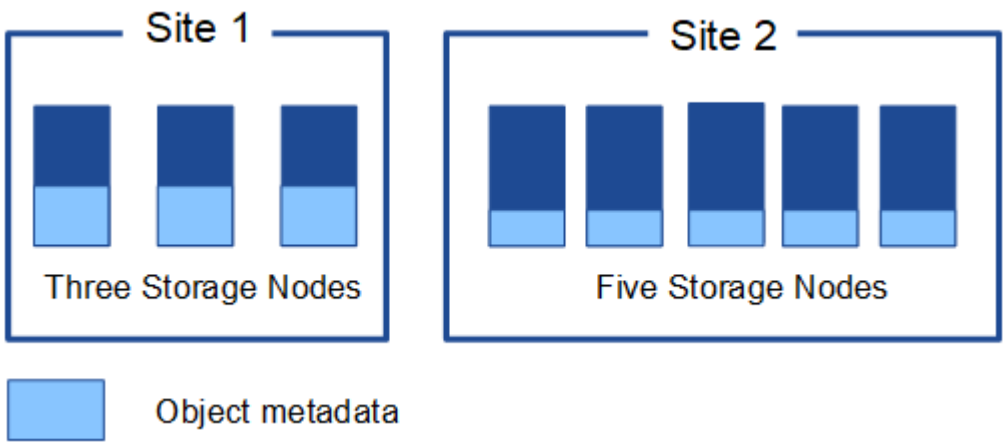
${post_edited_translations.segment}

- ${post_edited_translations.segment}
- Cualquier par clave-valor de metadatos de usuario personalizados asociados al objeto.
- Para los objetos de S3, cualquier par clave-valor de etiquetas asociado con el objeto.
- En el caso de las copias replicadas de objetos, la ubicación de almacenamiento actual de cada copia.
- ${post_edited_translations.segment}
- Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluyendo el nombre del bucket externo y el identificador único del objeto.
- ${post_edited_translations.segment}

${post_edited_translations.segment}

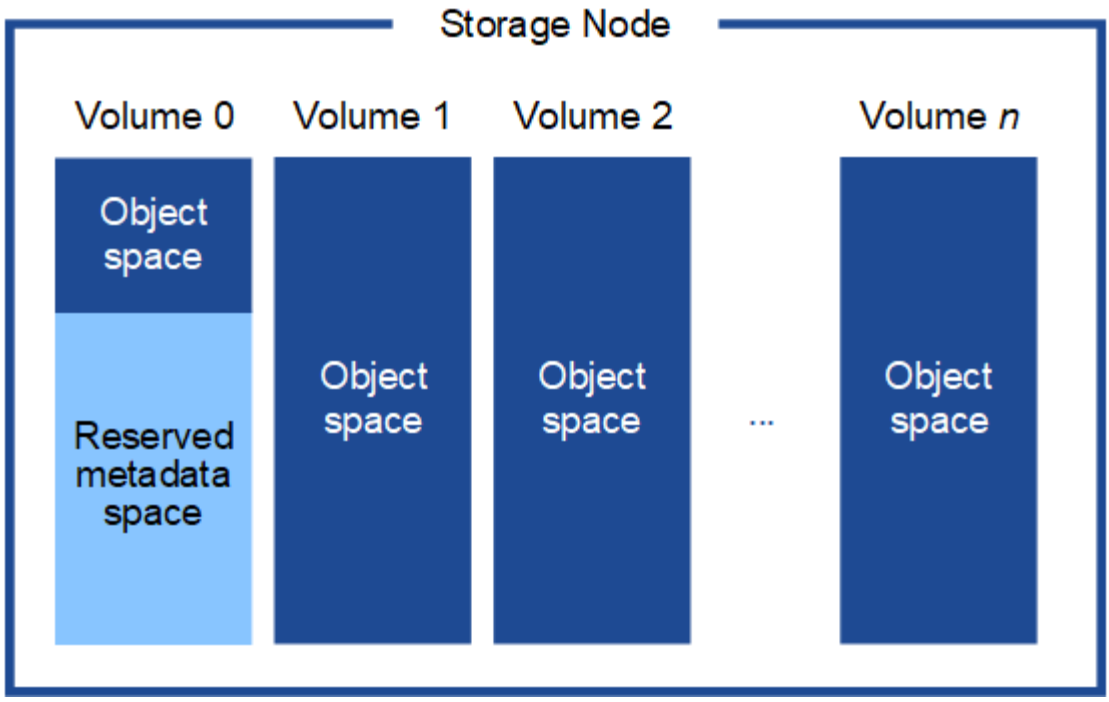
StorageGRID mantiene los metadatos de los objetos en una base de datos Cassandra, que se almacena de forma independiente de los datos de los objetos. Para proporcionar redundancia y proteger los metadatos de los objetos frente a pérdidas, StorageGRID almacena tres copias de los metadatos de todos los objetos del sistema en cada sitio.

Esta figura representa los nodos de almacenamiento en dos sitios. Cada sitio tiene la misma cantidad de metadatos de objetos, y los metadatos de cada sitio se subdividen entre todos los nodos de almacenamiento de ese sitio.



${post_edited_translations.segment}

Esta figura representa los volúmenes de almacenamiento de un único nodo de almacenamiento.



Como se muestra en la figura, StorageGRID reserva espacio para los metadatos de objetos en el volumen de almacenamiento 0 de cada Storage Node. Utiliza el espacio reservado para almacenar metadatos de objetos y realizar operaciones esenciales de la base de datos. El espacio restante en el volumen de almacenamiento 0 y todos los demás volúmenes de almacenamiento del Storage Node se utilizan exclusivamente para datos de objetos (copias replicadas y fragmentos con codificación de borrado).

${post_edited_translations.segment}

${post_edited_translations.segment}

El *espacio reservado para metadatos* es un ajuste de 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 este ajuste se basa en:

- La versión del software que utilizabas cuando instalaste StorageGRID por primera vez.
- ${post_edited_translations.segment}

${post_edited_translations.segment}	**Cantidad de RAM en los nodos de almacenamiento**	**${post_edited_translations.segment}**
11,5 a 12,0	${post_edited_translations.segment}	8 TB (8.000 GB)
	${post_edited_translations.segment}	3 TB (3.000 GB)
${post_edited_translations.segment}	128 GB o más en cada nodo de almacenamiento en cualquier centro	${post_edited_translations.segment}

${post_edited_translations.segment}	Cantidad de RAM en los nodos de almacenamiento	${post_edited_translations.segment}
	Menos de 128 GB en cualquier nodo de almacenamiento de cada emplazamiento	3 TB (3.000 GB)
${post_edited_translations.segment}	Cualquier cantidad	2 TB (2.000 GB)

Ver la configuración de espacio reservado para metadatos

Sigue estos pasos para consultar la configuración del espacio reservado para metadatos de tu sistema StorageGRID.

Pasos

1. Selecciona **Configuración** > **Sistema** > **Ajustes de almacenamiento**.
2. ${post_edited_translations.segment}

${post_edited_translations.segment}

La configuración predeterminada para una nueva instalación de StorageGRID 11.6 o superior en la que cada Storage Node tenga 128 GB o más de RAM es 8,000 GB (8 TB).

Espacio realmente reservado para metadatos

A diferencia de la configuración de espacio reservado para metadatos a nivel de sistema, el *espacio reservado real* para los metadatos de los objetos se determina para cada Storage Node. Para cualquier Storage Node, el espacio reservado real para metadatos depende del tamaño del volumen 0 de ese nodo y de la configuración de espacio reservado para metadatos a nivel de sistema.

${post_edited_translations.segment}	Espacio realmente reservado para metadatos
${post_edited_translations.segment}	10% del volumen 0
${post_edited_translations.segment}	El menor de estos valores: • ${post_edited_translations.segment} • ${post_edited_translations.segment} **Nota**: Solo se requiere un rangedb para los nodos de almacenamiento que contienen únicamente metadatos.

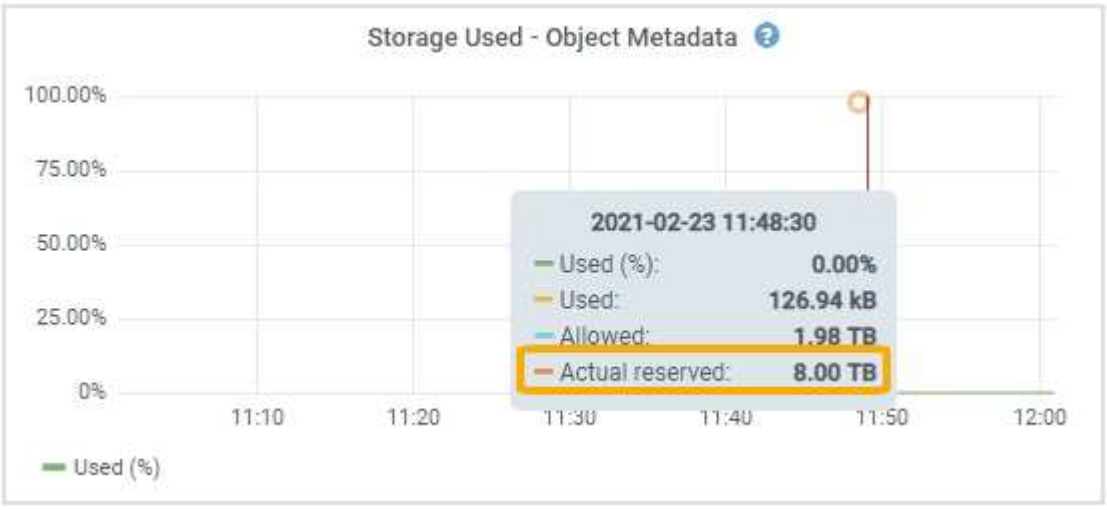
Ver el espacio realmente reservado para metadatos

${post_edited_translations.segment}

Pasos

1. Desde el Grid Manager, selecciona **Nodes** > ***Storage Node***.

2. Selecciona la pestaña **Storage**.
3. Coloca el cursor sobre el gráfico «Almacenamiento utilizado - metadatos de objetos» y busca el valor **espacio reservado real**.



En la captura de pantalla, el valor **Reservado real** es de 8 TB. Esta captura de pantalla corresponde a un Storage Node grande en una nueva instalación de StorageGRID 11.6. Como la configuración de espacio reservado para metadatos a nivel de sistema es menor que el volumen 0 de este Storage Node, el espacio reservado real para este nodo es igual a la configuración de espacio reservado para metadatos.

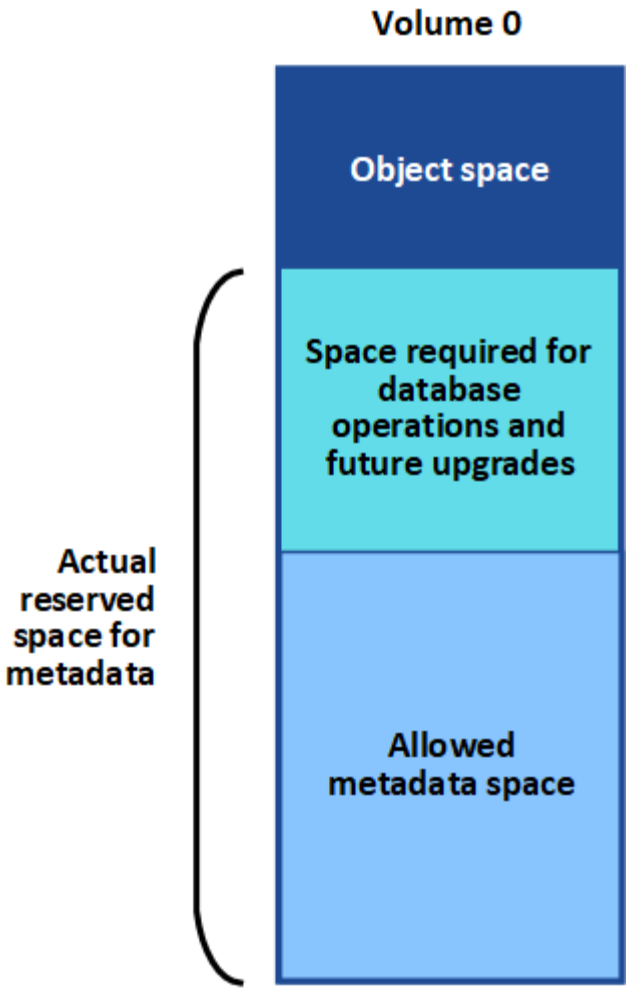
Ejemplo de espacio real reservado para metadatos

Supongamos que instalas un nuevo sistema StorageGRID con la versión 11.7 o posterior. Para este ejemplo, supón que cada Storage Node tiene más de 128 GB de RAM y que el volumen 0 de Storage Node 1 (SN1) es de 6 TB. Según estos valores:

- El **espacio reservado para metadatos** de todo el sistema está configurado en 8 TB. (Este es el valor predeterminado para una nueva instalación de StorageGRID 11.6 o superior si cada Storage Node tiene más de 128 GB de RAM).
- El espacio realmente reservado para los metadatos de SN1 es de 6 TB. (Se reserva todo el volumen porque el volumen 0 es más pequeño que la configuración de **Espacio reservado para metadatos**.)

${post_edited_translations.segment}

El espacio real reservado para los metadatos en cada nodo de almacenamiento se subdivide en el espacio disponible para los metadatos de los objetos (el espacio de metadatos permitido) y el espacio necesario para las operaciones esenciales de la base de datos (como la compactación y la reparación) y las futuras actualizaciones de hardware y software. El espacio de metadatos permitido determina la capacidad total de los objetos.



${post_edited_translations.segment}

		${post_edited_translations.segment}	
	${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment}
⇐ 4 TB	60 % del espacio reservado para metadatos, hasta un máximo de 1,32 TB	60 % del espacio reservado para metadatos, hasta un máximo de 1,98 TB	${post_edited_translations.segment}

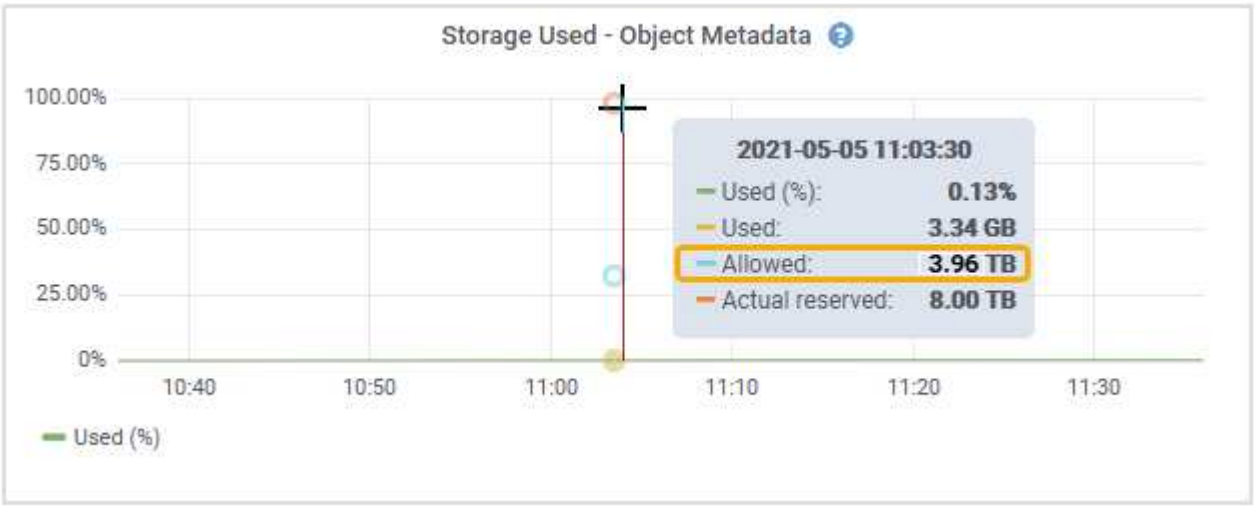
Ver el espacio de metadatos permitido

Sigue estos pasos para consultar el espacio de metadatos permitido para un Storage Node.

Pasos

1. Desde el Grid Manager, selecciona **Nodes**.

2. Selecciona el nodo de almacenamiento.
3. Selecciona la pestaña **Storage**.
4. Coloca el cursor sobre el gráfico "Almacenamiento utilizado - metadatos del objeto" y busca el valor **Allowed**.



${post_edited_translations.segment}

El valor **Permitido** se corresponde con esta métrica de Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

${post_edited_translations.segment}

Supongamos que instalas un sistema StorageGRID con la versión 11.6. Para este ejemplo, supón 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 para metadatos** de todo el sistema está configurado en 8 TB. (Este es el valor predeterminado para StorageGRID 11.6 o superior cuando cada Storage Node tiene más de 128 GB de RAM.)
- El espacio realmente reservado para los metadatos de SN1 es de 6 TB. (Se reserva todo el volumen porque el volumen 0 es más pequeño que la configuración de **Espacio reservado para metadatos**.)
- El espacio permitido para metadatos en SN1 es de 3 TB, según el cálculo que se muestra en la tabla con el espacio permitido para los metadatos: (espacio reservado para metadatos − 1 TB) × 60 %, hasta un máximo de 3,96 TB.

Cómo influyen los nodos de almacenamiento de distintos tamaños en la capacidad de los objetos

Como se describió anteriormente, StorageGRID distribuye de manera uniforme los metadatos de objetos entre los nodos de almacenamiento de cada sitio. Por este motivo, si un sitio contiene nodos de almacenamiento de diferentes tamaños, el nodo más pequeño del sitio determina la capacidad de metadatos del sitio.

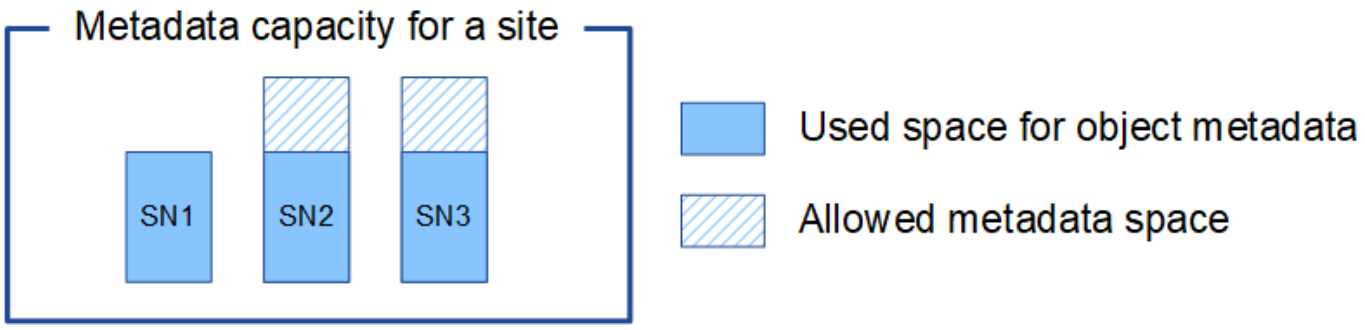
${post_edited_translations.segment}

- Tienes una red de un único sitio que contiene tres nodos de almacenamiento de distintos tamaños.

- La opción **Espacio reservado para metadatos** está configurada en 4 TB.
- ${post_edited_translations.segment}

Nodo de almacenamiento	${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment}
SN1	2,2 TB	2,2 TB	1,32 TB
SN2	5 TB	4 TB	1,98 TB
SN3	6 TB	4 TB	1,98 TB

Como los metadatos de objetos se distribuyen de manera uniforme entre los nodos de almacenamiento de un sitio, cada nodo de este ejemplo solo puede albergar 1,32 TB de metadatos. No se pueden usar los 0,66 TB adicionales de espacio de metadatos permitido para SN2 y SN3.



Del mismo modo, porque StorageGRID mantiene todos los metadatos de los objetos de un sistema StorageGRID en cada sitio, la capacidad total de metadatos de un sistema StorageGRID se determina por la capacidad de metadatos de objetos del sitio más pequeño.

Y dado que la capacidad de metadatos de los objetos determina el número máximo de objetos, cuando un nodo agota su capacidad de metadatos, la grid está, en efecto, llena.

Información relacionada

- Para saber cómo supervisar la capacidad de metadatos de los objetos de cada Storage Node, consulta las instrucciones para "Supervisión de StorageGRID".
- Para aumentar la capacidad de metadatos de objetos de tu sistema, "expandir una grid" añadiendo nuevos Storage Nodes.

Aumenta la configuración de espacio reservado para metadatos en StorageGRID

Es posible que puedas aumentar el parámetro del sistema Espacio reservado para metadatos si tus Storage Nodes cumplen requisitos específicos de RAM y espacio disponible.

Lo que necesitas

- Has iniciado sesión en Grid Manager usando una "navegador web compatible".
- Tienes el "Permiso de acceso root o el permiso de otra configuración de grid".

Acerca de esta tarea

Es posible que puedas aumentar manualmente el valor de Espacio reservado para metadatos a nivel de sistema hasta 8 TB.

Solo puedes aumentar el valor de la configuración de Espacio reservado para metadatos a nivel del sistema si ambas afirmaciones son verdaderas:

- Los nodos de almacenamiento de cualquier sitio de tu sistema cuentan cada uno con 128 GB o más de RAM.
- Los nodos de almacenamiento de cualquier sitio en tu sistema tienen suficiente espacio disponible en el volumen de almacenamiento 0.

Ten en cuenta que, si aumentas este parámetro, reducirás al mismo tiempo el espacio disponible para el almacenamiento de objetos en el volumen de almacenamiento 0 de todos los Storage Nodes. Por este motivo, es posible que prefieras establecer el espacio reservado para metadatos en un valor inferior a 8 TB, según tus necesidades previstas de metadatos de objetos.

> En general, es mejor utilizar un valor más alto que uno más bajo. Si el valor de «Espacio reservado para metadatos» es demasiado alto, puedes reducirlo más adelante. Por el contrario, si aumentas el valor más adelante, es posible que el sistema tenga que mover datos de objetos para liberar espacio.

Para obtener una explicación detallada de cómo la configuración «Espacio reservado para metadatos» afecta al espacio permitido para el almacenamiento de metadatos de objetos en un Storage Node concreto, consulta "Gestiona el almacenamiento de metadatos de objetos".

Pasos

1. ${post_edited_translations.segment}
   a. Selecciona **Configuración** > **Sistema** > **Ajustes de almacenamiento**.
   b. Toma nota del valor de **Espacio reservado para metadatos**.
2. Asegúrate de que tienes suficiente espacio disponible en el volumen de almacenamiento 0 de cada Storage Node para aumentar este valor.
   a. Selecciona **Nodos**.
   b. Selecciona el primer nodo de almacenamiento en la cuadrícula.
   c. Selecciona la pestaña Storage.
   d. ${post_edited_translations.segment}
   e. Comprueba que el valor Disponible sea igual o superior a la diferencia entre el nuevo valor que deseas utilizar y el valor actual de Espacio reservado para metadatos.

      Por ejemplo, si el valor actual de la opción «Espacio reservado para metadatos» es de 4 TB y quieres aumentarlo a 6 TB, el valor de «Disponible» debe ser de 2 TB o más.

   f. Repite 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 continúes con este procedimiento.
      - Si cada nodo de almacenamiento tiene suficiente espacio disponible en el volumen 0, pasa al siguiente paso.
3. Asegúrate de que cada nodo de almacenamiento cuente con al menos 128 GB de RAM.

a. Selecciona **Nodos**.

b. Selecciona el primer nodo de almacenamiento en la cuadrícula.

c. Selecciona la pestaña **Hardware**.

d. Pasa el cursor sobre el gráfico de uso de memoria. Asegúrate de que **Total Memory** sea de al menos 128 GB.

e. Repite estos pasos para todos los nodos de almacenamiento.

- Si uno o más nodos de almacenamiento no tienen suficiente memoria total disponible, no se puede aumentar el valor de Espacio reservado para metadatos. No continúes con este procedimiento.
- Si cada nodo de almacenamiento tiene al menos 128 GB de memoria total, pasa al siguiente paso.

4. Actualiza la configuración del Espacio reservado para metadatos.

a. Selecciona **Configuración** > **Sistema** > **Ajustes de almacenamiento**.

b. ${post_edited_translations.segment}

c. ${post_edited_translations.segment}

${post_edited_translations.segment}

d. Selecciona **Guardar**.

Comprime objetos almacenados en StorageGRID

${post_edited_translations.segment}

Antes de empezar

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

Acerca de esta tarea

De forma predeterminada, la compresión de objetos está desactivada. Si activas la compresión, StorageGRID intenta comprimir cada objeto al guardarlo, utilizando una compresión sin pérdidas.

> Si modificas esta configuración, la nueva configuración tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para mejorar el rendimiento y la escalabilidad.

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- 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, seleccionar esta opción no reducirá aún más el tamaño del objeto.
- No selecciones **Comprimir objetos almacenados** si estás usando NetApp FabricPool con StorageGRID.
- Si se selecciona **Comprimir objetos almacenados**, las aplicaciones cliente de S3 deben evitar realizar operaciones GetObject que especifiquen que se devuelva un rango de bytes. Estas operaciones de "lectura de rango" son ineficientes porque StorageGRID debe descomprimir los objetos 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, resulta ineficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si los rangos se leen de objetos comprimidos, las solicitudes de los clientes pueden agotar el tiempo de espera.

${post_edited_translations.segment}

Pasos

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Selecciona **Guardar**.

Gestiona nodos de almacenamiento completos en StorageGRID

A medida que los nodos de almacenamiento alcanzan su capacidad, debes ampliar el sistema StorageGRID añadiendo nuevo almacenamiento. Hay tres opciones disponibles: añadir volúmenes de almacenamiento, añadir bandejas de expansión de almacenamiento y añadir nodos de almacenamiento.

Agregar volúmenes de almacenamiento

Cada nodo de almacenamiento admite un número máximo de volúmenes de almacenamiento. El máximo definido varía según la plataforma. Si un nodo de almacenamiento tiene menos volúmenes de almacenamiento que el número máximo, puedes añadir volúmenes para aumentar su capacidad. Consulta las instrucciones para "Ampliar un sistema StorageGRID".

Agrega bandejas de expansión de almacenamiento

Algunos nodos de almacenamiento de los dispositivos StorageGRID, como el SG6060 o el SG6160, pueden admitir bandejas de almacenamiento adicionales. Si tienes dispositivos StorageGRID con capacidad de expansión que aún no se han ampliado a la capacidad máxima, puedes añadir bandejas de almacenamiento para aumentar la capacidad. Consulta las instrucciones para "Ampliar un sistema StorageGRID".

${post_edited_translations.segment}

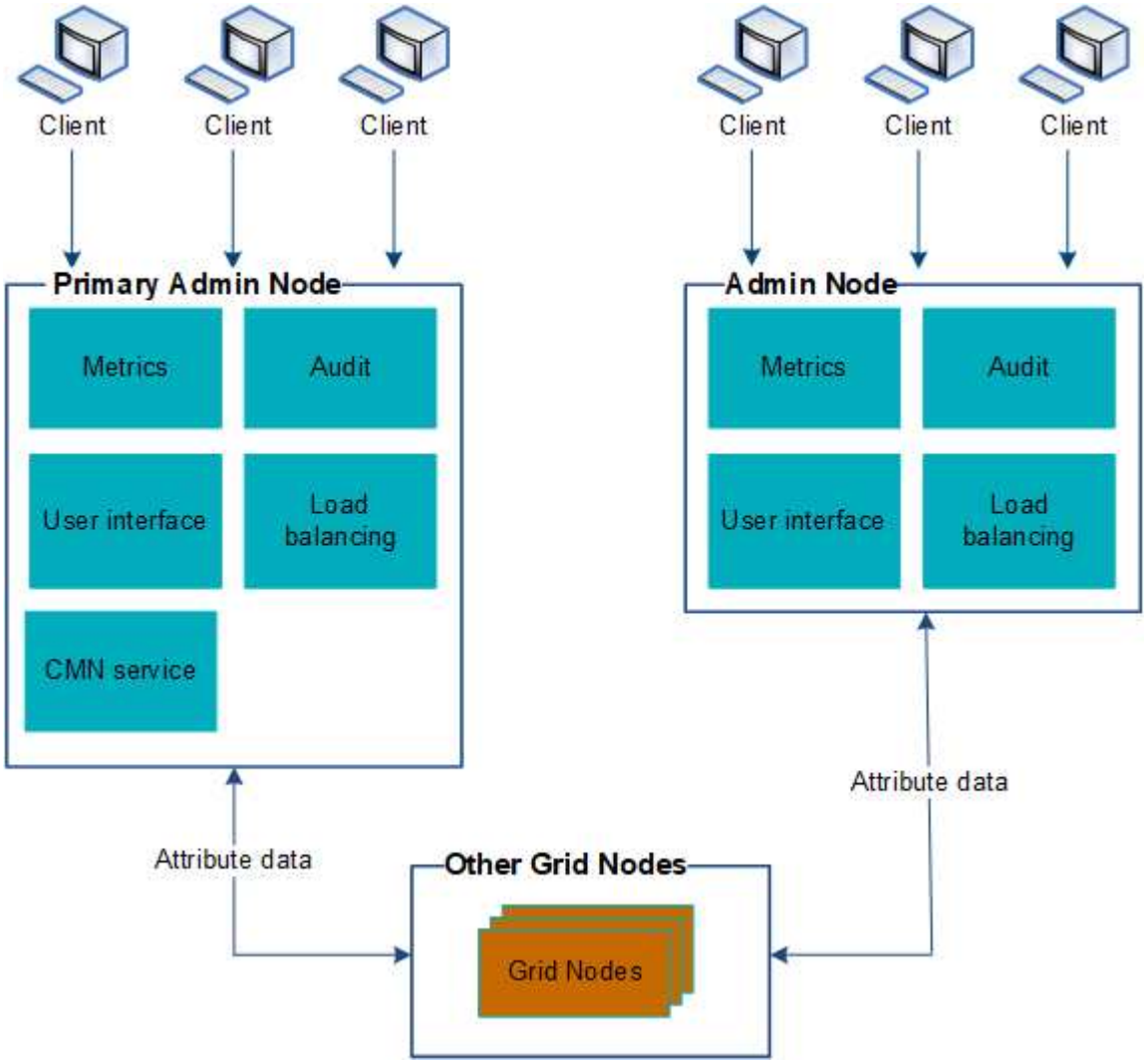
Puedes aumentar la capacidad de almacenamiento añadiendo Storage Nodes. Al añadir almacenamiento, debes tener muy en cuenta las reglas de ILM actualmente activas y los requisitos de capacidad. Consulta las instrucciones para "Ampliar un sistema StorageGRID".

Gestionar nodos de administración

Usa varios nodos de administración en StorageGRID

Un sistema StorageGRID puede incluir varios nodos de administración para que puedas supervisar y configurar tu sistema StorageGRID de forma continua, incluso si falla uno de los nodos 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 siguen enviándose. Sin embargo, disponer de varios nodos de administración no ofrece protección frente a fallos, salvo en lo que respecta a las notificaciones y a los paquetes de AutoSupport.



Existen dos opciones para seguir visualizando y configurando el sistema StorageGRID en caso de que falle un nodo de administración:

- Los clientes web pueden volver a conectarse a cualquier otro nodo de administración disponible.
- Si un administrador del sistema ha configurado un grupo de alta disponibilidad de nodos de administración, los clientes web pueden seguir accediendo al Grid Manager o al Tenant Manager usando la dirección IP virtual del grupo de alta disponibilidad. Consulta "Gestiona grupos de alta disponibilidad".

> Cuando se utiliza un grupo de alta disponibilidad (HA), 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 de alta disponibilidad falle y pase a otro nodo de administración del grupo.

Algunas tareas de mantenimiento solo pueden realizarse mediante el nodo de administración principal. Si el nodo de administración principal falla, debe recuperarse antes de que el sistema StorageGRID vuelva a estar plenamente operativo.

Identifica el nodo de administración principal en StorageGRID

El nodo de administración principal ofrece más funcionalidades que los nodos de

administración no principales. Por ejemplo, algunos procedimientos de mantenimiento deben realizarse utilizando el nodo de administración principal.

Para obtener más información sobre los nodos de administración, consulta "¿Qué es un nodo de administración?".

Antes de empezar

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

Pasos

1. Selecciona **Nodos**.
2. Escribe **primario** en el cuadro de búsqueda.

   En los resultados de la búsqueda, identifica el nodo que aparece como "Primary Admin Node" en la columna Tipo. Debería aparecer un único Primary Admin Node.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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