



Configurar y administrar

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Configurar y administrar un sistema StorageGRID	1
Administrar StorageGRID	1
Administrar StorageGRID	1
Comience a usar Grid Manager	1
Controlar el acceso a StorageGRID	32
Utilizar la federación de red	84
Gestionar la seguridad	121
Administrar inquilinos	190
Configurar conexiones de cliente	211
Administrar redes y conexiones	253
Utilice AutoSupport	272
Administrar nodos de almacenamiento	287
Administrar nodos de administración	301
Administrar objetos con ILM	304
Administrar objetos con ILM	304
ILM y ciclo de vida de los objetos	305
Crear y asignar grados de almacenamiento	327
Utilice grupos de almacenamiento	330
Utilice grupos de almacenamiento en la nube	338
Administrar perfiles de codificación de borrado	359
Configurar regiones (opcional y solo S3)	362
Crear regla ILM	364
Administrar políticas de ILM	380
Trabajar con políticas y reglas de ILM	397
Usar bloqueo de objetos S3	401
Ejemplo de reglas y políticas de ILM	410
Endurecimiento del sistema	430
Consideraciones generales para el fortalecimiento del sistema	430
Pautas de refuerzo para las actualizaciones de software	431
Pautas de fortalecimiento para redes StorageGRID	432
Pautas de refuerzo para nodos StorageGRID	433
Pautas de refuerzo para TLS y SSH	436
Otras pautas de endurecimiento	437
Configurar StorageGRID para FabricPool	439
Configurar StorageGRID para FabricPool	439
Información necesaria para adjuntar StorageGRID como un nivel de nube	441
Utilice el asistente de configuración de FabricPool	442
Configurar StorageGRID manualmente	456
Configurar el Administrador del sistema ONTAP	466
Configurar el servidor DNS	468
Prácticas recomendadas de StorageGRID para FabricPool	469
Eliminar datos de FabricPool de StorageGRID	473

Configurar y administrar un sistema StorageGRID

Administrar StorageGRID

Administrar StorageGRID

Utilice estas instrucciones para configurar y administrar un sistema StorageGRID .

Acerca de estas instrucciones

Las tareas principales para configurar y administrar StorageGRID le permiten:

- Utilice el Administrador de cuadrícula para configurar grupos y usuarios
- Cree cuentas de inquilino para permitir que las aplicaciones cliente de S3 almacenen y recuperen objetos
- Configurar y administrar redes StorageGRID
- Configurar AutoSupport
- Administrar la configuración del nodo

Antes de empezar

- Tiene una comprensión general del sistema StorageGRID .
- Tienes conocimientos bastante detallados de shells de comandos de Linux, redes y configuración y configuración de hardware de servidor.

Comience a usar Grid Manager

Requisitos del navegador web

Debe utilizar un navegador web compatible.

Navegador web	Versión mínima compatible
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Debes configurar la ventana del navegador a un ancho recomendado.

Ancho del navegador	Píxeles
Mínimo	1024
Óptimo	1280

Sign in en el Administrador de cuadrícula

Puede acceder a la página de inicio de sesión de Grid Manager ingresando 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 cantidad de nodos de administración no principales. Puede iniciar sesión en Grid Manager en cualquier nodo de administración para administrar el sistema StorageGRID. Sin embargo, algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

Conectarse al grupo HA

Si los nodos de administración están incluidos en un grupo de alta disponibilidad (HA), se conectan utilizando la dirección IP virtual del grupo de HA o un nombre de dominio completo que se asigna a la dirección IP virtual. El nodo de administración principal debe seleccionarse como la interfaz principal del grupo, de modo que cuando acceda al Administrador de cuadrícula, lo haga en el nodo de administración principal, a menos que este no esté disponible. Ver ["Administrar grupos de alta disponibilidad"](#).

Usar SSO

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

Sign in en Grid Manager en el primer nodo de administración

Antes de empezar

- Tienes tus credenciales de inicio de sesión.
- Estás usando un ["navegador web compatible"](#).
- Las cookies están habilitadas en su navegador web.
- Pertenece a un grupo de usuarios que tiene al menos un permiso.
- Tienes la URL para el Administrador de Grid:

```
https://FQDN_or_Admin_Node_IP/
```

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

Para acceder al Administrador de cuadrícula en un puerto distinto del puerto predeterminado para HTTPS (443), incluya el número de puerto en la URL:

```
https://FQDN_or_Admin_Node_IP:port/
```



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

Pasos

1. Abra un navegador web compatible.
2. En la barra de direcciones del navegador, ingrese la URL del Administrador de cuadrícula.

3. Si aparece una alerta de seguridad, instale el certificado utilizando el asistente de instalación del navegador. Ver "[Administrar certificados de seguridad](#)".
4. Sign in en el Administrador de cuadrícula.

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

No usar SSO

- a. Introduzca su nombre de usuario y contraseña para el Administrador de Grid.
- b. Seleccione **Iniciar sesión**.



The screenshot shows the login interface for NetApp StorageGRID Grid Manager. At the top, the logo "NetApp StorageGRID®" is displayed, followed by the title "Grid Manager" in a large font. Below the title, there are two input fields: "Username" and "Password". The "Username" field is currently empty with a cursor at the start. Below the "Password" field is a blue "Sign in" button. At the bottom of the form, there are three links: "Tenant sign in", "NetApp support", and "NetApp.com".

Usando SSO

- Si StorageGRID utiliza SSO y esta es la primera vez que accede a la URL en este navegador:
 - i. Seleccionar * Sign in*. Puedes dejar el 0 en el campo Cuenta.



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Ingrese sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización. Por ejemplo:

Sign in with your organizational account

Sign in

- Si StorageGRID usa SSO y usted ha accedido previamente al Administrador de Grid o a una cuenta de inquilino:
 - i. Ingrese **0** (el ID de la cuenta del Administrador de Grid) o seleccione **Administrador de Grid** si aparece en la lista de cuentas recientes.

The image shows a web interface for NetApp StorageGRID. At the top, there is a logo consisting of a square icon with a grid pattern followed by the text "NetApp StorageGRID®". Below the logo, the heading "Sign in" is displayed in a large, bold font. Underneath the heading, there is a section labeled "Recent" with a dropdown menu showing "Grid Manager" and a downward arrow. Below this, there is a section labeled "Account" with a text input field containing the character "0". A blue button with the text "Sign in" is positioned below the input field. At the bottom of the form, there is a link that reads "NetApp support | NetApp.com".

NetApp StorageGRID®

Sign in

Recent

Grid Manager ▼

Account

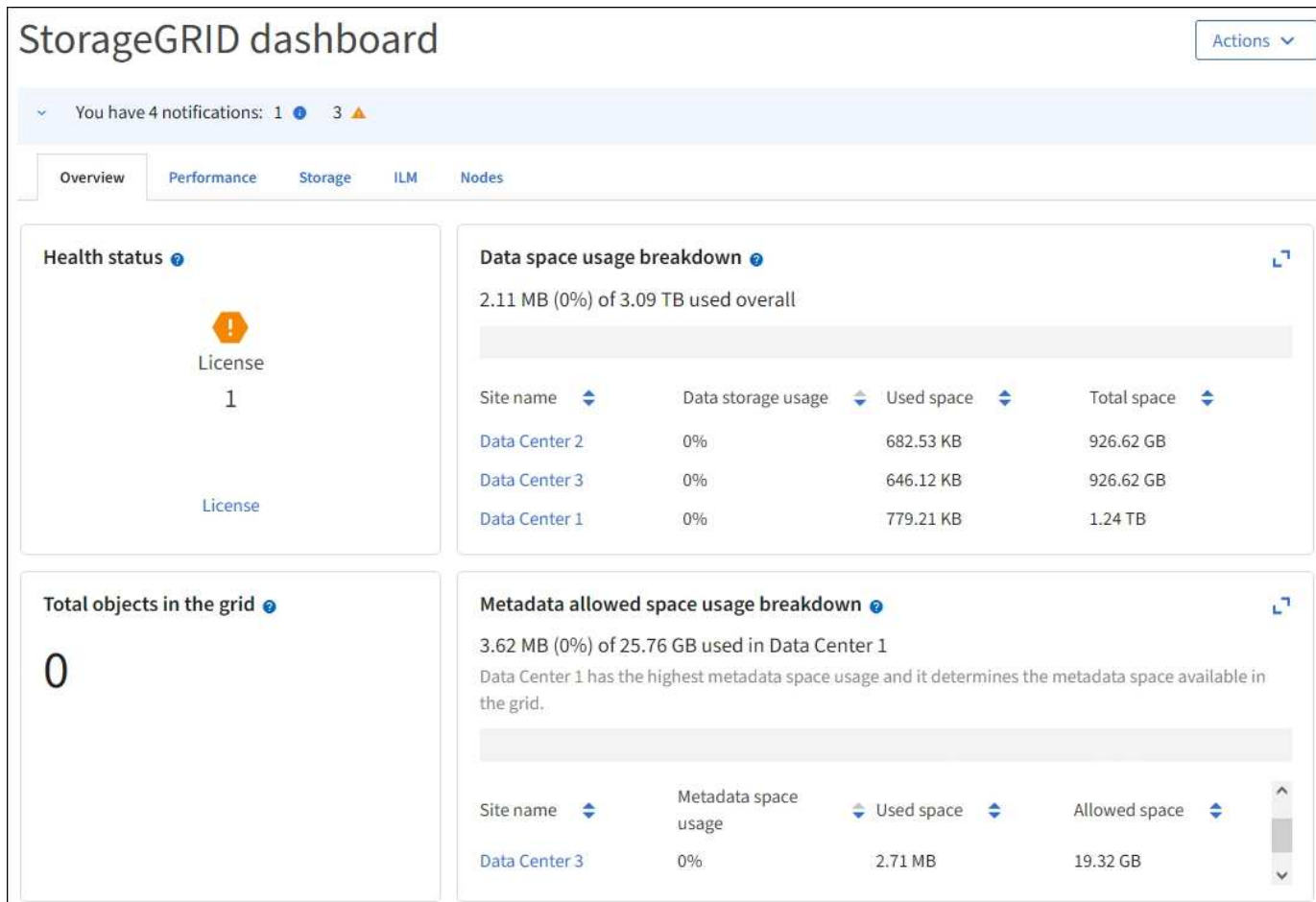
0

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Seleccionar * Sign in*.
- iii. Sign in con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

Cuando haya iniciado sesión, aparecerá la página de inicio del Grid Manager, que incluye el panel de control. Para saber qué información se proporciona, consulte ["Ver y administrar el panel de control"](#) .



Iniciar sesión en otro nodo de administración

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

No usar SSO

Pasos

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

Usando SSO

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

Pasos

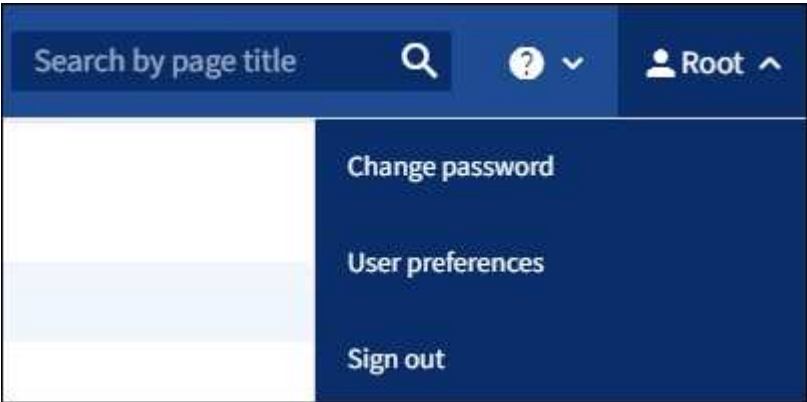
1. Ingrese el nombre de dominio completo o la dirección IP del otro nodo de administración en la barra de direcciones del navegador.
2. Si su sesión SSO ha expirado, ingrese sus credenciales nuevamente.

Cerrar sesión en Grid Manager

Cuando termine de trabajar con Grid Manager, deberá cerrar la sesión para asegurarse de que usuarios no autorizados no puedan acceder al sistema StorageGRID . Es posible que cerrar su navegador no cierre su sesión del sistema, según la configuración de cookies del navegador.

Pasos

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



2. Seleccione **Cerrar sesión**.

Opción	Descripción
SSO no en uso	Has cerrado la sesión del nodo de administración. Se muestra la página de inicio de sesión de Grid Manager. Nota: Si inició sesión en más de un nodo de administración, deberá cerrar sesión en cada nodo.
SSO habilitado	Has cerrado la sesión de todos los nodos de administración a los que estabas accediendo. Se muestra la página de inicio de sesión de StorageGRID . Grid Manager aparece como predeterminado en el menú desplegable Cuentas recientes y el campo ID de cuenta muestra 0. Nota: Si SSO está habilitado y también ha iniciado sesión en el Administrador de inquilinos, también debe "cerrar sesión en la cuenta del inquilino" a "cerrar sesión de SSO" .

Cambiar tu contraseña

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

Antes de empezar

Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .

Acerca de esta tarea

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

Pasos

1. Desde el encabezado del Administrador de cuadrícula, seleccione **su nombre** > **Cambiar contraseña**.
2. Introduzca su contraseña actual.
3. Escriba una nueva contraseña.

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

4. Ingrese nuevamente la nueva contraseña.
5. Seleccione **Guardar**.

Ver la información de la licencia de StorageGRID

Puede ver la información de la licencia de su sistema StorageGRID , como la capacidad máxima de almacenamiento de su red, siempre que sea necesario.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .

Acerca de esta tarea

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



Pasos

1. Acceda a la página de Licencia realizando una de las siguientes acciones:
 - Seleccione **MANTENIMIENTO** > **Sistema** > **Licencia**.
 - Desde la tarjeta de estado de salud en el panel de control, seleccione el ícono de estado de licencia o el enlace **Licencia**.

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

2. Ver los detalles de solo lectura de la licencia actual:

- ID del sistema StorageGRID , que es el número de identificación único para esta instalación de StorageGRID
- Número de serie de la licencia
- Tipo de licencia, ya sea **Perpetua** o **Suscripción**
- Capacidad de almacenamiento licenciada de la red
- Capacidad de almacenamiento admitida
- Fecha de finalización de la licencia. **N/A** aparece para una licencia perpetua.
- Fecha de finalización del soporte

Esta fecha se lee del archivo de licencia actual y podría estar desactualizada si extendió o renovó el contrato de servicio de soporte después de obtener el archivo de licencia. Para actualizar este valor, consulte "[Actualizar la información de la licencia de StorageGRID](#)". También puede ver la fecha de finalización real del contrato utilizando Active IQ.

- Contenido del archivo de texto de la licencia

Actualizar la información de la licencia de StorageGRID

Debe actualizar la información de la licencia de su sistema StorageGRID cada vez que cambien los términos de su licencia. Por ejemplo, debe actualizar la información de la licencia si compra capacidad de almacenamiento adicional para su red.

Antes de empezar

- Tiene un nuevo archivo de licencia para aplicar a su sistema StorageGRID .
- Tienes "[permisos de acceso específicos](#)".
- Tienes la contraseña de aprovisionamiento.

Pasos

1. Seleccione **MANTENIMIENTO > Sistema > Licencia**.
2. En la sección Actualizar licencia, seleccione **Explorar**.
3. Localice y seleccione el nuevo archivo de licencia(.txt).

El nuevo archivo de licencia se valida y se muestra.

4. Introduzca la contraseña de aprovisionamiento.
5. Seleccione **Guardar**.

Utilice la API

Utilice la API de gestión de red

Puede realizar tareas de administración del sistema utilizando la API REST de administración de cuadrícula en lugar de la interfaz de usuario de Grid Manager. Por ejemplo, es posible que desee utilizar la API para automatizar operaciones o crear múltiples entidades, como usuarios, más rápidamente.

Recursos de alto nivel

La API de administración de red proporciona los siguientes recursos de nivel superior:

- `/grid`: El acceso está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados.
- `/org`: El acceso está restringido a los usuarios que pertenecen a un grupo LDAP local o federado para una cuenta de inquilino. Para obtener más información, consulte ["Utilice 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 puntos finales privados de StorageGRID también ignoran la versión API de la solicitud.

Emitir solicitudes de API

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

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

Antes de empezar

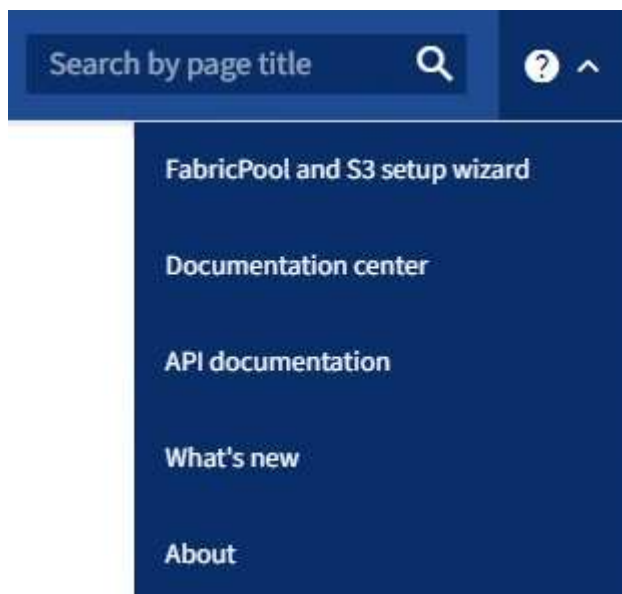
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).



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

Pasos

1. Desde el encabezado de Grid Manager, seleccione el ícono de ayuda y seleccione **Documentación de API**.



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

página API de administración de StorageGRID .

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

3. Seleccione la operación deseada.

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

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

The screenshot shows the API documentation for the `GET /grid/groups` endpoint. The interface is titled "groups Operations on groups". The endpoint is `GET /grid/groups` with the description "Lists Grid Administrator Groups".

Parameters:

Name	Description
<code>type</code> string (query)	filter by group type Available values : local, federated
<code>limit</code> integer (query)	maximum number of results Default value : 25
<code>marker</code> string (query)	marker-style pagination offset (value is Group's URN)
<code>includeMarker</code> boolean (query)	if set, the marker element is also returned
<code>order</code> string (query)	pagination order (desc requires marker) Available values : asc, desc

Responses:

Response content type: `application/json`

Code	Description
200	successfully retrieved

Example Value | Model

```
{
  "responseTime": "2021-03-29T14:22:19.673Z",
  "status": "success",
  "apiVersion": "3.3",
  "deprecated": false,
  "data": [
    {
      "displayName": "Developers",

```

5. Determinar si la solicitud requiere parámetros adicionales, como un ID de grupo o usuario. Luego, obtenga estos valores. Es posible que primero debas emitir una solicitud API diferente para obtener la información que necesitas.
6. Determina si necesitas modificar el cuerpo de la solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.
7. Seleccione **Probarlo**.
8. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.
9. Seleccione **Ejecutar**.
10. Revise el código de respuesta para determinar si la solicitud fue exitosa.

Operaciones de la API de gestión de red

La API de administración de red organiza las operaciones disponibles en las siguientes secciones.



Esta lista solo incluye operaciones disponibles en la API pública.

- **cuentas:** Operaciones para administrar cuentas de inquilinos de almacenamiento, incluida la creación de nuevas cuentas y la recuperación del uso de almacenamiento para una cuenta determinada.
- **alert-history:** Operaciones sobre alertas resueltas.
- **alert-receivers:** Operaciones sobre receptores de notificaciones de alerta (correo electrónico).
- **alert-rules:** Operaciones sobre reglas de alerta.
- **alert-silences:** Operaciones sobre silencios de alerta.
- **alertas:** Operaciones sobre alertas.
- **audit:** Operaciones para listar y actualizar la configuración de auditoría.
- **auth:** Operaciones para realizar la autenticación de la sesión del usuario.

La API de administración de red admite el esquema de autenticación de token de portador. Para iniciar sesión, debe proporcionar 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 proporcionarse en el encabezado de las solicitudes de API posteriores ("Autorización: Bearer *token*"). El token caduca después de 16 horas.



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

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

- **client-certificates:** Operaciones para configurar certificados de cliente para que se pueda acceder a StorageGRID de forma segura mediante herramientas de monitoreo externas.
- **config:** Operaciones relacionadas con el lanzamiento del producto y las versiones de la API de administración de cuadrícula. Puede enumerar la versión de lanzamiento del producto y las versiones principales de la API de administración de cuadrícula compatibles con esa versión, y puede deshabilitar las versiones obsoletas de la API.

- **funciones-desactivadas:** Operaciones para ver funciones que podrían haber sido desactivadas.
- **dns-servers:** Operaciones para listar y cambiar servidores DNS externos configurados.
- **drive-details:** Operaciones en unidades para modelos de dispositivos de almacenamiento específicos.
- **endpoint-domain-names:** Operaciones para enumerar y cambiar los nombres de dominio de los puntos finales de S3.
- **erasure-coding:** Operaciones sobre perfiles de codificación de borrado.
- **expansión:** Operaciones de expansión (nivel de procedimiento).
- **expansion-nodes:** Operaciones de expansión (nivel de nodo).
- **sitios-de-expansión:** Operaciones de expansión (a nivel de sitio).
- **grid-networks:** Operaciones para listar y cambiar la lista de redes de cuadrícula.
- **grid-passwords:** Operaciones para la gestión de contraseñas de la red.
- **grupos:** Operaciones para administrar grupos de administradores de grid locales y para recuperar grupos de administradores de grid federados desde un servidor LDAP externo.
- **identity-source:** Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información de usuarios y grupos federados.
- **ilm:** Operaciones sobre la gestión del ciclo de vida de la información (ILM).
- **in-progress-procedures:** recupera los procedimientos de mantenimiento que están actualmente en curso.
- **licencia:** Operaciones para recuperar y actualizar la licencia de StorageGRID .
- **logs:** Operaciones para recopilar y descargar archivos de registro.v
- **métricas:** Operaciones sobre métricas de StorageGRID , incluidas consultas de métricas instantáneas en un único punto en el tiempo y consultas de métricas de rango durante un período de tiempo. La API de administración de red utiliza la herramienta de monitoreo de sistemas Prometheus como fuente de datos de back-end. Para obtener información sobre cómo construir consultas de Prometheus, consulte el sitio web de Prometheus.



Métricas que incluyen *private* en sus nombres están destinados únicamente para uso interno. Estas métricas están sujetas a cambios entre versiones de StorageGRID sin previo aviso.

- **node-details:** Operaciones sobre los detalles del nodo.
- **node-health:** Operaciones sobre el estado de salud del nodo.
- **node-storage-state:** Operaciones sobre el estado de almacenamiento del nodo.
- **ntp-servers:** Operaciones para listar o actualizar servidores externos de Protocolo de tiempo de red (NTP).
- **objetos:** Operaciones sobre objetos y metadatos de objetos.
- **recuperación:** Operaciones para el procedimiento de recuperación.
- **recovery-package:** Operaciones para descargar el paquete de recuperación.
- **regiones:** Operaciones para ver y crear regiones.
- **s3-object-lock:** Operaciones en la configuración global de bloqueo de objetos S3.
- **server-certificate:** Operaciones para ver y actualizar los certificados del servidor de Grid Manager.
- **snmp:** Operaciones en la configuración SNMP actual.

- **storage-watermarks:** Marcas de agua del nodo de almacenamiento.
- **traffic-classes:** Operaciones para políticas de clasificación de tráfico.
- **untrusted-client-network:** Operaciones en la configuración de red de cliente no confiable.
- **usuarios:** Operaciones para ver y administrar usuarios de Grid Manager.

Control de versiones de la API de gestión de red

La API de administración de red utiliza versiones para admitir 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 actualiza cuando se realizan cambios que *no son compatibles* con versiones anteriores. La versión menor de la API se actualiza cuando se realizan cambios que *son compatibles* con versiones anteriores. Los cambios compatibles incluyen la adición de nuevos puntos finales o nuevas propiedades.

El siguiente ejemplo ilustra cómo se actualiza la versión de la API según el tipo de cambios realizados.

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

Cuando instala el software StorageGRID por primera vez, solo se habilita la versión más reciente de la API. Sin embargo, cuando actualiza a una nueva versión de funciones de StorageGRID, continúa teniendo acceso a la versión anterior de API durante al menos una versión de funciones de StorageGRID .



Puede configurar las versiones compatibles. Consulte la sección **config** de la documentación de la API de Swagger para obtener más información. "[API de gestión de red](#)" Para más información. Debe desactivar el soporte para la versión anterior después de actualizar todos los clientes API para usar la versión más nueva.

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

- El encabezado de respuesta es "Obsoleto: verdadero".
- El cuerpo de la respuesta JSON incluye "deprecated": true
- Se agrega una advertencia obsoleta a nms.log. Por ejemplo:

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

Determinar qué versiones de API son compatibles con la versión actual

Utilice el `GET /versions` Solicitud de API para devolver una lista de las principales versiones de 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
  ]
}
```

Especificar una versión de API para una solicitud

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

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

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

Protección contra la falsificación de solicitudes entre sitios (CSRF)

Puede ayudar a protegerse contra ataques de falsificación de solicitud entre sitios (CSRF) contra StorageGRID mediante el uso de tokens CSRF para mejorar la autenticación que utiliza cookies. El administrador de red y el administrador de inquilinos habilitan automáticamente esta función de seguridad; otros clientes de API pueden elegir si habilitarla cuando inician sesión.

Un atacante que puede activar una solicitud a un sitio diferente (por ejemplo, con un formulario HTTP POST) puede provocar que ciertas solicitudes se realicen utilizando las cookies del usuario que inició sesión.

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

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

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:

- El `X-Csrf-Token` encabezado, con el valor del encabezado establecido en el valor de la cookie del token CSRF.
- Para los puntos finales que aceptan un cuerpo codificado por formulario: A `csrfToken` parámetro del cuerpo de la solicitud codificado en formulario.

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



Las solicitudes que tienen una cookie de token CSRF configurada también aplicarán el encabezado "Content-Type: application/json" para cualquier solicitud que espere un cuerpo de solicitud JSON como protección adicional contra ataques CSRF.

Utilice la API si el inicio de sesión único está habilitado

Utilice la API si el inicio de sesión único está habilitado (Active Directory)

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

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

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

Antes de empezar

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

Acerca de esta tarea

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

- El `storagegrid-ssoauth.py` Script de Python, que se encuentra en el directorio de archivos de

instalación de StorageGRID(. /rpms para Red Hat Enterprise Linux, ./debs para Ubuntu o Debian, y ./vsphere para VMware).

- Un ejemplo de flujo de trabajo de solicitudes curl.

El flujo de trabajo curl puede expirar si lo realiza demasiado lento. Es posible que veas el error: A valid SubjectConfirmation was not found on this Response .



El flujo de trabajo curl de ejemplo no protege la contraseña para que otros usuarios no la vean.

Si tiene un problema de codificación de URL, es posible que vea el error: Unsupported SAML version .

Pasos

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

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

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

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

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

El token de autorización de StorageGRID se proporciona en la salida. Ahora puedes usar el token para otras solicitudes, de manera similar a como usarías la API si no se estuviera utilizando SSO.

3. Si desea utilizar solicitudes curl, utilice el siguiente procedimiento.
 - a. Declare las variables necesarias para iniciar sesión.

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



Para acceder a la API de administración de red, utilice 0 como TENANTACCOUNTID.

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

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

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

- c. Guardar el SAMLRequest de la respuesta para su uso en comandos posteriores.

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

- d. Obtenga una URL completa que incluya el ID de 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"'
```

La respuesta incluye el ID de la solicitud del cliente:

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

e. Guarde 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=$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS devuelve una redirección 302, con información adicional en los encabezados.



Si la autenticación multifactor (MFA) está habilitada para su sistema SSO, la publicación 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=fZHRTOMwFIZfhh...UJikvo77sXPw%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. Guardar el MSISAuth cookie de la respuesta.

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

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

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

Los encabezados de respuesta contendrán información de la sesión de AD FS para su uso posterior al cerrar sesión, y el cuerpo de la respuesta contiene SAMLResponse en un campo de formulario oculto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
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. Guardar el SAMLResponse del campo oculto:

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

- j. Usando lo guardado SAMLResponse , crear un StorageGRID/api/saml-response solicitud para

generar un token de autenticación de StorageGRID .

Para RelayState , use el ID de la cuenta del inquilino o use 0 si desea iniciar sesión en la API de administración de Grid.

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

La respuesta incluye el token de autenticación.

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

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

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

Ya puedes utilizar MYTOKEN para otras solicitudes, de forma similar a como usarías la API si no se estuviera utilizando SSO.

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

Si se ha habilitado el inicio de sesión único (SSO), debe emitir una serie de solicitudes de API para cerrar sesión en la API de administración de red o en la API de administración de inquilinos. Estas instrucciones se aplican si está utilizando Active Directory como proveedor de identidad SSO

Acerca de esta tarea

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

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `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%3D",
  "responseTime": "2018-11-20T22:20:30.839Z",
  "status": "success"
}
```

2. Guardar la URL de cierre de sesión.

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

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

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

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de API.

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

4. Eliminar el token portador de StorageGRID .

La eliminación del token portador de StorageGRID funciona de la misma manera que sin SSO. Si no se proporciona la cookie "sso=true", el usuario cierra la sesión 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
```

A 204 No Content La respuesta indica que el usuario ahora ha cerrado la sesión.

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

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

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

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

Estas instrucciones se aplican si utiliza Azure como proveedor de identidad de SSO

Antes de empezar

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

Acerca de esta tarea

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

- El `storagegrid-ssoauth-azure.py` secuencia de comandos de Python
- El `storagegrid-ssoauth-azure.js` Script de Node.js

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

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

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

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

Pasos

1. Instale las dependencias necesarias, de la siguiente manera:

- a. Instalar Node.js (ver "<https://nodejs.org/en/download/>").
- b. Instale los módulos Node.js necesarios (puppeteer y jsdom):

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

2. Pase el script de Python al intérprete de Python para ejecutarlo.

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

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

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

Watch for and approve a 2FA authorization request
*****

StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



El script asume que la MFA se realiza mediante Microsoft Authenticator. Es posible que necesites 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 se proporciona en la salida. Ahora puedes usar el token para otras solicitudes, de manera similar a como usarías la API si no se estuviera utilizando SSO.

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

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

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

Estas instrucciones se aplican si utiliza PingFederate como proveedor de identidad SSO

Antes de empezar

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

Acerca de esta tarea

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

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

El flujo de trabajo curl puede expirar si lo realiza demasiado lento. Es posible que veas el error: `A valid SubjectConfirmation was not found on this Response.`



El flujo de trabajo curl de ejemplo no protege la contraseña para que otros usuarios no la vean.

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

Pasos

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

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

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

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

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

El token de autorización de StorageGRID se proporciona en la salida. Ahora puedes usar el token para otras solicitudes, de manera similar a como usarías la API si no se estuviera utilizando SSO.

3. Si desea utilizar solicitudes curl, utilice el siguiente procedimiento.

- a. Declare las variables necesarias para iniciar sesión.

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



Para acceder a la API de administración de red, utilice 0 como TENANTACCOUNTID.

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

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

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

La respuesta para este ejemplo incluye una URL firmada que está codificada como URL, pero no incluye la capa de codificación JSON adicional.

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

- c. Guardar el SAMLRequest de la respuesta para su uso en comandos posteriores.

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

- d. Exportar la respuesta y la cookie, y hacer eco de 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 repite la respuesta:

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

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

f. Exporta el valor 'href' (elimina la barra diagonal final /) y repite la respuesta:

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

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

g. Exportar el valor de 'acción':

```
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=
$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Guardar el SAMLResponse del campo oculto:

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

j. Usando lo guardado SAMLResponse , crear un StorageGRID/api/saml-response solicitud para generar un token de autenticación de StorageGRID .

Para RelayState , use el ID de la cuenta del inquilino o use 0 si desea iniciar sesión en la API de administración de Grid.

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

La respuesta incluye el token de autenticación.

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

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

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

Ya puedes utilizar MYTOKEN para otras solicitudes, de forma similar a como usarías la API si no se estuviera utilizando SSO.

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

Si se ha habilitado el inicio de sesión único (SSO), debe emitir una serie de solicitudes de API para cerrar sesión en la API de administración de red o en la API de administración de inquilinos. Estas instrucciones se aplican si utiliza PingFederate como proveedor de identidad SSO

Acerca de esta tarea

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

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `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. Guardar la URL de cierre de sesión.

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

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

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

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de 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. Eliminar el token portador de StorageGRID .

La eliminación del token portador de StorageGRID funciona de la misma manera que sin SSO. Si no se proporciona la cookie "sso=true", el usuario cierra la sesión 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
```

A 204 No Content La respuesta indica que el usuario ahora ha cerrado la sesión.

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


Desactivar funciones con la API

Puede utilizar la API de administración de red para desactivar por completo ciertas funciones en el sistema StorageGRID . Cuando una función está desactivada, no se pueden asignar permisos a nadie para realizar las tareas relacionadas con esa función.

Acerca de esta tarea

El sistema de funciones desactivadas le permite evitar el acceso a ciertas funciones en el sistema StorageGRID . Desactivar una función es la única forma de evitar que el usuario root o los usuarios que pertenecen a grupos de administradores con permiso de **acceso root** puedan usar esa función.

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

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 arrendatarios, la Compañía A quiere asegurarse de que sus propios empleados nunca puedan acceder a ninguna cuenta de inquilino después de que la cuenta se haya implementado.

La empresa A puede lograr este objetivo mediante el sistema de desactivación de funciones en la API de administración de la red. Al desactivar por completo la función **Cambiar contraseña de root del inquilino** en el Administrador de Grid (tanto la UI como la API), la Compañía A garantiza que los usuarios administradores, incluido el usuario root y los usuarios que pertenecen a grupos con permiso de **Acceso root**, no puedan cambiar la contraseña de ningún usuario root de la cuenta de inquilino.

Pasos

1. Acceda a la documentación de Swagger para la API de administración de cuadrícula. Ver "[Utilice la API de gestión de red](#)".
2. Localice el punto final Desactivar funciones.
3. Para desactivar una función, como Cambiar la contraseña raíz del inquilino, envíe un cuerpo a la API como este:

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

Cuando se completa la solicitud, la función Cambiar la contraseña raíz del inquilino se deshabilita. El permiso de administración **Cambiar 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 Prohibido".

Reactivar funciones desactivadas

De forma predeterminada, puede utilizar la API de administración de cuadrícula para reactivar una función que se ha desactivado. Sin embargo, si desea evitar que las funciones desactivadas se vuelvan a activar, puede desactivar la función **activateFeatures**.



La función **activateFeatures** no se puede reactivar. Si decide desactivar esta función, tenga en cuenta que perderá permanentemente la capacidad de reactivar cualquier otra función desactivada. Debe ponerse en contacto con el soporte técnico para restaurar cualquier funcionalidad perdida.

Pasos

1. Acceda a la documentación de Swagger para la API de administración de cuadrícula.

2. Localice el punto final Desactivar funciones.
3. Para reactivar todas las funciones, envíe un cuerpo a la API como este:

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

Cuando se completa esta solicitud, se reactivan todas las funciones, incluida la función Cambiar la contraseña raíz del inquilino. El permiso de administración **Cambiar contraseña de root del inquilino** ahora aparece en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña de root de un inquilino tendrá éxito, asumiendo que el usuario tiene el permiso de administración **Acceso de root** o **Cambiar contraseña de root del inquilino**.



El ejemplo anterior hace que *todas* las funciones desactivadas se reactiven. Si se han desactivado otras funciones que deben permanecer desactivadas, deberá especificarlas explícitamente en la solicitud PUT. Por ejemplo, para reactivar la función Cambiar contraseña de root del inquilino y continuar desactivando el permiso de administración de storageAdmin, envíe esta solicitud PUT:

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

Controlar el acceso a StorageGRID

Controlar el acceso a StorageGRID

Usted controla 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, puede habilitar el inicio de sesión único (SSO), crear certificados de cliente y cambiar las contraseñas de la red.

Controlar el acceso al Administrador de Grid

Usted determina quién puede acceder al Administrador de Grid y a la API de Administración de Grid importando grupos y usuarios desde un servicio de federación de identidad o configurando grupos y usuarios locales.

Usando ["federación de identidades"](#) facilita la configuración ["grupos"](#) y ["usuarios"](#) es más rápido y permite a los usuarios iniciar sesión en StorageGRID usando credenciales familiares. Puede configurar la federación de identidad si utiliza Active Directory, OpenLDAP u Oracle Directory Server.



Comuníquese con el soporte técnico si desea utilizar otro servicio LDAP v3.

Usted determina qué tareas puede realizar cada usuario asignándoles diferentes ["permisos"](#) a cada grupo. Por ejemplo, es posible que desee que los usuarios de un grupo puedan administrar las reglas de ILM y que los usuarios de otro grupo puedan realizar tareas de mantenimiento. Un usuario debe pertenecer al menos a un grupo para acceder al sistema.

Opcionalmente, puede configurar un grupo para que sea de solo lectura. Los usuarios de un grupo de solo lectura solo pueden ver configuraciones y funciones. No pueden realizar ningún cambio ni realizar ninguna operación en el Administrador de Grid ni en la API de administración de Grid.

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 usted "[configurar y habilitar SSO](#)" Todos los usuarios deben estar autenticados por un proveedor de identidad externo antes de poder acceder al Administrador de Grid, al Administrador de Inquilinos, a la API de Administración de Grid o a la API de Administración de Inquilinos. Los usuarios locales no pueden iniciar sesión en StorageGRID.

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 de la red y de las claves de cifrado para el sistema StorageGRID . Puede "[cambiar la contraseña](#)" según sea necesario.

Cambiar las contraseñas de la consola del nodo

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

Cambiar la contraseña de aprovisionamiento

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)" .
- Tiene permisos de acceso de mantenimiento o root.
- 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 "[descargando el paquete de recuperación](#)" . La frase de contraseña de aprovisionamiento no aparece en la `Passwords.txt` archivo. Asegúrese de documentar la contraseña de aprovisionamiento y guardarla en un lugar seguro.

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso> Contraseñas de red**.
2. En **Cambiar contraseña de aprovisionamiento**, seleccione **Realizar un cambio**
3. Introduzca su contraseña de aprovisionamiento actual.
4. Introduzca la nueva contraseña. La frase de contraseña debe contener al menos 8 y no más de 32 caracteres. Las frases de contraseña distinguen entre mayúsculas y minúsculas.
5. Guarde la nueva contraseña de aprovisionamiento en una ubicación segura. Es necesario para procedimientos de instalación, expansión y mantenimiento.
6. Vuelva a ingresar la nueva contraseña y seleccione **Guardar**.

El sistema muestra un banner de éxito verde cuando se completa el cambio de contraseña de aprovisionamiento.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

7. Seleccione **Paquete de recuperación**.

8. Ingrese la nueva contraseña de aprovisionamiento para descargar el nuevo paquete de recuperación.



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

Cambiar las contraseñas de la consola del nodo

Cada nodo de su red tiene una contraseña de consola de nodo única, que necesita para iniciar sesión en el nodo. Utilice estos pasos para cambiar la contraseña única de la consola de cada nodo de su red.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Tú tienes el [Permiso de mantenimiento o acceso root](#).
- Tienes la contraseña de aprovisionamiento actual.

Acerca de esta tarea

Utilice la contraseña de la consola del nodo para iniciar sesión en un nodo como "admin" mediante SSH, o como usuario root en una conexión de consola física/VM. El proceso de cambio de contraseña de la consola del nodo crea nuevas contraseñas para cada nodo de su red y almacena las contraseñas en un archivo actualizado. `Passwords.txt` archivo en el paquete de recuperación. Las contraseñas aparecen en la columna Contraseña del archivo `Passwords.txt`.



Hay contraseñas de acceso SSH independientes para las claves SSH utilizadas para la comunicación entre nodos. Las contraseñas de acceso SSH no se modifican con este procedimiento.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Contraseñas de red**.
2. En **Cambiar contraseñas de la consola del nodo**, seleccione **Realizar un cambio**.

Introduzca la contraseña de aprovisionamiento

Pasos

1. Introduzca la contraseña de aprovisionamiento para su red.
2. Seleccione **Continuar**.

Descargar el paquete de recuperación actual

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

Pasos

1. Seleccione **Descargar paquete de recuperación**.
2. Copiar el archivo del paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.



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

3. Seleccione **Continuar**.
4. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para comenzar a cambiar las contraseñas de la consola del nodo.

No puedes cancelar este proceso una vez iniciado.

Cambiar las contraseñas de la consola del nodo

Cuando se inicia el proceso de contraseña de la consola del nodo, se genera un nuevo paquete de recuperación que incluye las nuevas contraseñas. Luego, las contraseñas se actualizan en cada nodo.

Pasos

1. Espere a que se genere el nuevo paquete de recuperación, lo que puede tardar unos minutos.
2. Seleccione **Descargar nuevo paquete de recuperación**.
3. Cuando se complete la descarga:
 - a. Abrir el .zip archivo.
 - b. Confirme que puede acceder al contenido, incluido el Passwords.txt archivo, que contiene las nuevas contraseñas de la consola del nodo.
 - c. Copiar el nuevo archivo del paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.



No sobrescriba el paquete de recuperación antiguo.

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

4. Seleccione la casilla de verificación para indicar que ha descargado el nuevo paquete de recuperación y verificado el contenido.
5. Seleccione **Cambiar contraseñas de la consola del nodo** y espere a que todos los nodos se actualicen con las nuevas contraseñas. Esto podría tardar unos minutos.

Si se cambian las contraseñas de todos los nodos, aparece un banner de éxito verde. Vaya al siguiente paso.

Si se produce un error durante el proceso de actualización, aparecerá un mensaje con la lista de nodos que no pudieron cambiar sus contraseñas. El sistema volverá a intentar automáticamente el proceso en cualquier nodo cuya contraseña no se haya podido cambiar. Si el proceso finaliza con algunos nodos que aún no tienen la contraseña cambiada, aparece el botón **Reintentar**.

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

- a. Revise los mensajes de error enumerados en la tabla.
- b. Resolver los problemas.
- c. Seleccione **Reintentar**.



Al volver a intentarlo solo se cambian las contraseñas de la consola de nodo en los nodos que fallaron durante intentos anteriores de cambio de contraseña.

6. Después de cambiar las contraseñas de la consola de nodo para todos los nodos, elimine el archivo [primer paquete de recuperación que descargaste](#).
7. Opcionalmente, utilice el enlace **Paquete de recuperación** para descargar una copia adicional del nuevo paquete de recuperación.

Cambiar las contraseñas de acceso SSH para los nodos de administración

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

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#).
- 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 para cada nodo se almacenan en el `Passwords.txt` archivo en el paquete de recuperación. Las claves se enumeran en la columna Contraseña de ese archivo.

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

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Contraseñas de red**.
2. En **Cambiar claves SSH**, seleccione **Realizar un cambio**.

Descargar el paquete de recuperación actual

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

Pasos

1. Introduzca la contraseña de aprovisionamiento para su red.
2. Seleccione **Descargar paquete de recuperación**.

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



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

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



No puedes cancelar este proceso una vez iniciado.

Cambiar las claves de acceso SSH

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

Pasos

1. Espere a que se genere el nuevo paquete de recuperación, lo que puede tardar unos minutos.
2. Cuando el botón Descargar nuevo paquete de recuperación esté habilitado, seleccione **Descargar nuevo paquete de recuperación** y guarde el archivo del nuevo paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.
3. Cuando se complete la descarga:
 - a. Abrir el .zip archivo.
 - b. Confirme que puede acceder al contenido, incluido el Passwords.txt archivo, que contiene las nuevas claves de acceso SSH.
 - c. Copiar el nuevo archivo del paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.



No sobrescriba el paquete de recuperación antiguo.

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

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

Si se cambian las claves de todos los nodos, aparece un banner de éxito verde.

Si se produce un error durante el proceso de actualización, un mensaje de banner enumera la cantidad de nodos cuyas claves no se pudieron cambiar. El sistema volverá a intentar automáticamente el proceso en cualquier nodo cuya clave no haya sido cambiada. Si el proceso finaliza con algunos nodos que aún no tienen una clave modificada, aparece el botón **Reintentar**.

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

- a. Revise los mensajes de error enumerados en la tabla.
- b. Resolver los problemas.
- c. Seleccione **Reintentar**.

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

- Después de cambiar las claves de acceso SSH para todos los nodos, elimine el archivo [primer paquete de recuperación que descargaste](#) .
- Opcionalmente, seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación** para descargar una copia adicional del nuevo paquete de recuperación.

Utilizar la federación de identidades

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

Configurar la federación de identidades para Grid Manager

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Está utilizando Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidad.



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

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Ver [Directrices para configurar un servidor OpenLDAP](#) .
- Si planea habilitar el inicio de sesión único (SSO), ha revisado la ["Requisitos y consideraciones para el inicio de sesión único"](#) .
- Si planea utilizar Seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidad utiliza TLS 1.2 o 1.3. Ver ["Cifrados compatibles para conexiones TLS salientes"](#) .

Acerca de esta tarea

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

- Grupos de administración. Los usuarios de los grupos de administración pueden iniciar sesión en Grid Manager y realizar tareas, según los permisos de administración asignados al grupo.
- Grupos de usuarios inquilinos para inquilinos que no utilizan su propia fuente de identidad. Los usuarios de los grupos de inquilinos pueden iniciar sesión en el Administrador de inquilinos y realizar tareas, según los permisos asignados al grupo en el Administrador de inquilinos. Ver ["Crear una cuenta de inquilino"](#) y ["Utilice una cuenta de inquilino"](#) Para más detalles.

Entrar a la configuración

Pasos

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

Ldap service type

Select the type of LDAP service you want to configure.

Active Directory

Azure

OpenLDAP

Other

Seleccione **Otro** para configurar valores para un servidor LDAP que utiliza Oracle Directory Server.

4. Si seleccionó **Otro**, complete los campos en la sección Atributos LDAP. De lo contrario, vaya al siguiente paso.
 - **Nombre único de usuario:** el nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a `sAMAccountName` para Active Directory y `uid` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `uid`.
 - **UUID de usuario:** el nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a `objectGUID` para Active Directory y `entryUUID` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `nsuniqueid`. El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
 - **Nombre único del grupo:** el nombre del atributo que contiene el identificador único de un grupo LDAP. Este atributo es equivalente a `sAMAccountName` para Active Directory y `cn` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `cn`.
 - **UUID de grupo:** el nombre del atributo que contiene el identificador único permanente de un grupo LDAP. Este atributo es equivalente a `objectGUID` para Active Directory y `entryUUID` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
5. Para todos los tipos de servicios LDAP, ingrese la información de conexión de red y servidor LDAP requerida en la sección Configurar 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 utilizar cualquier puerto siempre que tu firewall esté configurado correctamente.

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

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

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

- `sAMAccountName` o `uid`
- `objectGUID`, `entryUUID`, o `nsuniqueid`
- `cn`
- `memberOf` o `isMemberOf`
- **Directorio Activo:** `objectSid`, `primaryGroupID`, `userAccountControl`, y `userPrincipalName`
- **Azur:** `accountEnabled` y `userPrincipalName`

- **Contraseña:** La contraseña asociada al nombre de usuario.



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

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



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

- **DN base de usuario:** la ruta completa del nombre distinguido (DN) de un subárbol LDAP en el que desea buscar usuarios.



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

- **Formato de nombre de usuario vinculado** (opcional): el patrón de nombre de usuario predeterminado que StorageGRID debe usar si el patrón no se puede determinar automáticamente.

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

Introduzca uno de estos patrones:

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

Incluya **[NOMBRE DE USUARIO]** exactamente como está escrito.

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.

- **Usar STARTTLS:** utilice STARTTLS para proteger las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u otros, pero esta opción no es compatible con Azure.

- **Usar LDAPS:** La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Azure.
- **No utilizar TLS:** El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Azure.



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

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.

- **Usar certificado CA del sistema operativo:** utilice el certificado CA de Grid predeterminado instalado en el sistema operativo para proteger las conexiones.
- **Usar certificado CA personalizado:** utilice un certificado de seguridad personalizado.

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

Pruebe la conexión y guarde la configuración

Después de ingresar todos los valores, debe probar la conexión antes de poder guardar la configuración. StorageGRID verifica la configuración de conexión para el servidor LDAP y el formato de nombre de usuario vinculado, si proporcionó uno.

Pasos

1. Seleccione **Probar conexión**.
2. Si no proporcionó un formato de nombre de usuario vinculado:
 - Aparecerá el mensaje "Conexión de prueba exitosa" si la configuración de conexión es válida. Seleccione **Guardar** para guardar la configuración.
 - Aparece el mensaje "No se pudo establecer la conexión de prueba" si la configuración de conexión no es válida. Seleccione **Cerrar**. Luego, resuelva cualquier problema y pruebe la conexión nuevamente.
3. Si proporcionó un formato de nombre de usuario vinculado, ingrese el nombre de usuario y la contraseña de un usuario federado válido.

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

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

Cancel

Test Connection

- Aparecerá el mensaje "Conexión de prueba exitosa" si la configuración de conexión es válida. Seleccione **Guardar** para guardar la configuración.
- Aparece un mensaje de error si la configuración de conexión, el formato de nombre de usuario vinculado o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva cualquier problema y pruebe la conexión nuevamente.

Forzar la sincronización con la fuente de identidad

El sistema StorageGRID sincroniza periódicamente los grupos y usuarios federados desde la fuente de identidad. Puede forzar el inicio de la sincronización si desea habilitar o restringir los permisos de usuario lo más rápido posible.

Pasos

1. Vaya a la página de federación de identidad.
2. Seleccione **Servidor de sincronización** en la parte superior de la página.

El proceso de sincronización puede tardar algún tiempo dependiendo de su entorno.



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

Deshabilitar la federación de identidades

Puede deshabilitar temporal o permanentemente la federación de identidad para grupos y usuarios. Cuando la federación de identidad está deshabilitada, no hay comunicación entre StorageGRID y la fuente de identidad. Sin embargo, cualquier configuración que haya realizado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidad en el futuro.

Acerca de esta tarea

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

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que actualmente hayan iniciado sesión conservarán el acceso al sistema StorageGRID hasta que su sesión expire, pero no podrán iniciar sesión una vez que expire su sesión.

- No se producirá sincronización entre el sistema StorageGRID y la fuente de identidad, y no se generarán alertas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Habilitar federación de identidad** está deshabilitada si el inicio de sesión único (SSO) está configurado en **Habilitado** o **Modo Sandbox**. El estado de SSO en la página de inicio de sesión único debe ser **Deshabilitado** antes de poder deshabilitar la federación de identidad. Ver ["Deshabilitar el inicio de sesión único"](#).

Pasos

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

Directrices para configurar un servidor OpenLDAP

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



Para las fuentes de identidad que no sean ActiveDirectory o Azure, StorageGRID no bloqueará automáticamente el acceso a S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine todas las claves S3 del usuario o elimine el usuario de todos los grupos.

Superposiciones de miembros y refinaciones

Las superposiciones memberof y refint deben estar habilitadas. Para obtener más información, consulte las instrucciones para el mantenimiento inverso de la membresía del grupo en <http://www.openldap.org/doc/admin24/index.html> ["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"].

Indexación

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

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

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

Consulte la información sobre el mantenimiento de la membresía del grupo inverso en <http://www.openldap.org/doc/admin24/index.html> ["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"].

Administrar grupos de administradores

Puede crear grupos de administradores para administrar los permisos de seguridad de uno o más usuarios administradores. Los usuarios deben pertenecer a un grupo para tener acceso al sistema StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Si planea importar un grupo federado, ha configurado la federación de identidad y el grupo federado ya existe en la fuente de identidad configurada.

Crear un grupo de administradores

Los grupos de administradores le permiten determinar qué usuarios pueden acceder a qué funciones y operaciones en el Administrador de Grid y la API de administración de Grid.

Acceder al asistente

Pasos

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

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

- Cree un grupo local si desea asignar permisos a usuarios locales.
- Cree un grupo federado para importar usuarios desde la fuente de identidad.

Grupo local

Pasos

1. Seleccione **Grupo local**.
2. Introduzca un nombre para mostrar para el grupo, que podrá actualizar más tarde según sea necesario. Por ejemplo, "Usuarios de mantenimiento" o "Administradores de ILM".
3. Introduzca un nombre único para el grupo, que no podrá actualizar más tarde.
4. Seleccione **Continuar**.

Grupo federado

Pasos

1. Seleccione **Grupo federado**.
2. Ingrese el nombre del grupo que desea importar, exactamente como aparece en la fuente de identidad configurada.
 - Para Active Directory y Azure, utilice sAMAccountName.
 - Para OpenLDAP, utilice el CN (nombre común).
 - Para otro LDAP, utilice el nombre único apropiado para el servidor LDAP.
3. Seleccione **Continuar**.

Administrar permisos de grupo

Pasos

1. Para **Modo de acceso**, seleccione si los usuarios del grupo pueden cambiar configuraciones y realizar operaciones en el Administrador de cuadrícula y la API de administración de cuadrícula o si solo pueden ver configuraciones y funciones.
 - **Lectura y escritura** (predeterminado): los usuarios pueden cambiar la configuración y realizar las operaciones permitidas por sus permisos de administración.
 - **Solo lectura**: los usuarios solo pueden ver configuraciones y funciones. No pueden realizar ningún cambio ni realizar ninguna operación en el Administrador de Grid ni en la API de administración de Grid. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.



Si un usuario pertenece a varios grupos y alguno de ellos está configurado como **Solo lectura**, el usuario tendrá acceso de solo lectura a todas las configuraciones y funciones seleccionadas.

2. Seleccione uno o más ["permisos del grupo de administradores"](#).

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

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

Agregar usuarios (solo grupos locales)

Pasos

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

Si aún no ha creado usuarios locales, puede guardar el grupo sin agregar usuarios. Puede agregar este grupo al usuario en la página Usuarios. Ver ["Administrar usuarios"](#) Para más detalles.

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

Ver y editar grupos de administradores

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

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

Tarea	Menú de acciones	Página de detalles
Ver detalles del grupo	a. Seleccione la casilla de verificación del grupo. b. Seleccione Acciones > Ver detalles del grupo .	Seleccione el nombre del grupo en la tabla.

Tarea	Menú de acciones	Página de detalles
Editar nombre para mostrar (solo grupos locales)	a. Seleccione la casilla de verificación del grupo. b. Seleccione Acciones > Editar nombre del grupo . c. Introduzca el nuevo nombre. d. Seleccione Guardar cambios .	a. Seleccione el nombre del grupo para mostrar los detalles. b. Seleccione el icono de edición  . c. Introduzca el nuevo nombre. d. Seleccione Guardar cambios .
Editar el modo de acceso o los permisos	a. Seleccione la casilla de verificación del grupo. b. Seleccione Acciones > Ver detalles del grupo . c. Opcionalmente, cambie el modo de acceso del grupo. d. Opcionalmente, seleccione o desmarque " permisos del grupo de administradores ". e. Seleccione Guardar cambios .	a. Seleccione el nombre del grupo para mostrar los detalles. b. Opcionalmente, cambie el modo de acceso del grupo. c. Opcionalmente, seleccione o desmarque " permisos del grupo de administradores ". d. Seleccione Guardar cambios .

Duplicar un grupo

Pasos

1. Seleccione la casilla de verificación del grupo.
2. Seleccione **Acciones > Duplicar grupo**.
3. Complete el asistente para duplicar grupo.

Eliminar un grupo

Puede eliminar un grupo de administradores cuando desee eliminar el grupo del sistema y eliminar todos los permisos asociados con el grupo. Al eliminar un grupo de administradores se eliminan todos los usuarios del grupo, pero no se eliminan los usuarios mismos.

Pasos

1. Desde la página Grupos, seleccione la casilla de verificación de cada grupo que desee eliminar.
2. Seleccione **Acciones > Eliminar grupo**.
3. Seleccione **Eliminar grupos**.

Permisos del grupo de administradores

Al crear grupos de usuarios administradores, selecciona uno o más permisos para controlar el acceso a funciones específicas del Administrador de cuadrícula. Luego puede asignar cada usuario a uno o más de estos grupos de administración para determinar qué tareas puede realizar ese usuario.

Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenecen a ese grupo no

podrán iniciar sesión en Grid Manager ni en la API de administración de Grid.

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

- Sign in en el Administrador de cuadrícula
- Ver el panel de control
- Ver las páginas de Nodos
- Ver alertas actuales y resueltas
- Cambiar su propia contraseña (sólo usuarios locales)
- Ver cierta información proporcionada en las páginas de Configuración y Mantenimiento

Interacción entre permisos y modo de acceso

Para todos los permisos, la configuración **Modo de acceso** del grupo determina si los usuarios pueden cambiar configuraciones y realizar operaciones o si solo pueden ver las configuraciones y funciones relacionadas. Si un usuario pertenece a varios grupos y alguno de ellos está configurado como **Solo lectura**, el usuario tendrá acceso de solo lectura a todas las configuraciones y funciones seleccionadas.

Las siguientes secciones describen los permisos que puede asignar al crear o editar un grupo de administradores. Cualquier funcionalidad no mencionada explícitamente requiere el permiso de **acceso root**.

Acceso root

Este permiso proporciona acceso a todas las funciones de administración de la red.

Cambiar la contraseña raíz del inquilino

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



Para otorgar acceso a la página Inquilinos, que contiene la opción **Cambiar contraseña root**, asigne también el permiso **Cuentas de inquilinos**.

Configuración de la página de topología de cuadrícula

Este permiso proporciona acceso a las pestañas de Configuración en la página **SOPORTE > Herramientas > Topología de cuadrícula**.



La página de topología de cuadrícula ha quedado obsoleta y se eliminará en una versión futura.

ILM

Este permiso proporciona acceso a las siguientes opciones del menú **ILM**:

- Normas
- Políticas
- Etiquetas de política

- Pools de almacenamiento
- Grados de almacenamiento
- Regiones
- Búsqueda de metadatos de objetos



Los usuarios deben tener los permisos **Otra configuración de red** y **Configuración de página de topología de red** para administrar los niveles de almacenamiento.

Mantenimiento

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

- **CONFIGURACIÓN > Control de acceso:**
 - Contraseñas de la red
- **CONFIGURACIÓN > Red:**
 - Nombres de dominio de punto final S3
- **MANTENIMIENTO > Tareas:**
 - Desmantelamiento
 - Expansión
 - Comprobación de existencia de objetos
 - Recuperación
- **MANTENIMIENTO > Sistema:**
 - Paquete de recuperación
 - Actualización de software
- **SOPORTE > Herramientas:**
 - Registros

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

- **MANTENIMIENTO > Red:**
 - servidores DNS
 - Red de cuadrícula
 - servidores NTP
- **MANTENIMIENTO > Sistema:**
 - Licencia
- **CONFIGURACIÓN > Red:**
 - Nombres de dominio de punto final S3
- **CONFIGURACIÓN > Seguridad:**
 - Certificados
- **CONFIGURACIÓN > Monitoreo:**
 - Servidor de auditoría y syslog

Administrar alertas

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

Consulta de métricas

Este permiso proporciona acceso a:

- **SOPORTE > Herramientas > Página Métricas**
- Consultas de métricas de Prometheus personalizadas mediante la sección **Métricas** de la API de administración de cuadrícula
- Tarjetas del panel de control de Grid Manager que contienen métricas

Búsqueda de metadatos de objetos

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

Otra configuración de red

Este permiso proporciona acceso a opciones de configuración de cuadrícula adicionales.



Para ver estas opciones adicionales, los usuarios también deben tener el permiso **Configuración de la página de topología de cuadrícula**.

- **ILM:**
 - Grados de almacenamiento
- **CONFIGURACIÓN > Sistema:**
- **SOPORTE > Otro:**
 - Costo del enlace

Administrador de dispositivos de almacenamiento

Este permiso proporciona:

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

Cuentas de inquilinos

Este permiso proporciona la capacidad de:

- Acceda a la página Inquilinos, donde puede crear, editar y eliminar cuentas de inquilinos
- Ver las políticas de clasificación de tráfico existentes
- Ver las tarjetas del panel de Grid Manager que contienen detalles de los inquilinos

Administrar usuarios

Puede ver usuarios locales y federados. También puede crear usuarios locales y asignarlos a grupos de administradores locales para determinar a qué funciones de Grid Manager pueden acceder estos usuarios.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .

Crear un usuario local

Puede crear uno o más usuarios locales y asignar cada usuario a uno o más grupos locales. Los permisos del grupo controlan a qué funciones de Grid Manager y Grid Management API puede acceder el usuario.

Sólo puedes crear usuarios locales. Utilice la fuente de identidad externa para administrar usuarios y grupos federados.

El administrador de cuadrícula incluye un usuario local predefinido, llamado "root". No puedes eliminar el usuario root.



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

Acceder al asistente

Pasos

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

Ingresa las credenciales de usuario

Pasos

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

Asignar a grupos

Pasos

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

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

Si un usuario pertenece a varios grupos, los permisos son acumulativos. Ver ["Administrar grupos de administradores"](#) Para más detalles.

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

Ver y editar usuarios locales

Puede ver detalles de los usuarios locales y federados existentes. Puede modificar un usuario local para cambiar su nombre completo, contraseña o membresía de grupo. También puede impedir temporalmente que un usuario acceda al Administrador de Grid y a la API de administración de Grid.

Sólo puedes editar usuarios locales. Utilice la fuente de identidad externa para administrar usuarios federados.

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

Cualquier edición se aplicará la próxima vez que el usuario cierre sesión y vuelva a iniciar sesión en el Administrador de cuadrícula.



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

Tarea	Menú de acciones	Página de detalles
Ver detalles del usuario	- Seleccione la casilla de verificación para el usuario. - Seleccione Acciones > Ver detalles del usuario.	Seleccione el nombre del usuario en la tabla.
Editar nombre completo (solo usuarios locales)	- Seleccione la casilla de verificación para el usuario. - Seleccione Acciones > Editar nombre completo. - Introduzca el nuevo nombre. - Seleccione Guardar cambios.	- Seleccione el nombre del usuario para mostrar los detalles. - Seleccione el icono de edición . - Introduzca el nuevo nombre. - Seleccione Guardar cambios.
Denegar o permitir el acceso a StorageGRID	- Seleccione la casilla de verificación para el usuario. - Seleccione Acciones > Ver detalles del usuario. - Seleccione la pestaña Acceso. - Seleccione Sí para evitar que el usuario inicie sesión en Grid Manager o en la API de administración de Grid, o seleccione No para permitir que el usuario inicie sesión. - Seleccione Guardar cambios.	- Seleccione el nombre del usuario para mostrar los detalles. - Seleccione la pestaña Acceso. - Seleccione Sí para evitar que el usuario inicie sesión en Grid Manager o en la API de administración de Grid, o seleccione No para permitir que el usuario inicie sesión. - Seleccione Guardar cambios.

Tarea	Menú de acciones	Página de detalles
Cambiar contraseña (sólo usuarios locales)	a. Seleccione la casilla de verificación para el usuario. b. Seleccione Acciones > Ver detalles del usuario . c. Seleccione la pestaña Contraseña. d. Introduzca una nueva contraseña. e. Seleccione Cambiar contraseña .	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la pestaña Contraseña. c. Introduzca una nueva contraseña. d. Seleccione Cambiar contraseña .
Cambiar grupos (solo usuarios locales)	a. Seleccione la casilla de verificación para el usuario. b. Seleccione Acciones > Ver detalles del usuario . c. Seleccione la pestaña Grupos. d. Opcionalmente, seleccione el enlace después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador. e. Seleccione Editar grupos para seleccionar diferentes grupos. f. Seleccione Guardar cambios .	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la pestaña Grupos. c. Opcionalmente, seleccione el enlace después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador. d. Seleccione Editar grupos para seleccionar diferentes grupos. e. Seleccione Guardar cambios .

Duplicar un usuario

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

Pasos

1. Seleccione la casilla de verificación para el usuario.
2. Seleccione **Acciones > Duplicar usuario**.
3. Complete el asistente para duplicar usuarios.

Eliminar un usuario

Puede eliminar un usuario local para eliminarlo permanentemente del sistema.



No puedes eliminar el usuario root.

Pasos

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

Utilice el inicio de sesión único (SSO)

Configurar el inicio de sesión único

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 su organización. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cómo funciona 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).

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

Sign in cuando el SSO esté habilitado

Cuando SSO está habilitado e inicia sesión en StorageGRID, se lo redirige a la página SSO de su organización para validar sus credenciales.

Pasos

1. Ingrese 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 accede a la URL en este navegador, se le solicitará un ID de cuenta:



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- Si ya ha accedido al Administrador de red o al Administrador de inquilinos, se le solicitará que seleccione una cuenta reciente o que ingrese un ID de cuenta:



Tenant Manager

Recent

Account

Sign in

[NetApp support](#) | [NetApp.com](#)



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

2. Indique si desea acceder al Administrador de red o al Administrador de inquilinos:

- Para acceder al Administrador de cuadrícula, deje el campo **ID de cuenta** en blanco, ingrese **0** como ID de cuenta o seleccione **Administrador de cuadrícula** si aparece en la lista de cuentas recientes.
- Para acceder al Administrador de inquilinos, ingrese el ID de la cuenta del inquilino de 20 dígitos o seleccione un inquilino por nombre si aparece en la lista de cuentas recientes.

3. Seleccionar * Sign in*

StorageGRID lo redirecciona a la página de inicio de sesión SSO de su organización. Por ejemplo:

Sign in with your organizational account

someone@example.com

Password

Sign in

4. Sign in con sus credenciales SSO.

Si sus credenciales de SSO son correctas:

- El proveedor de identidad (IdP) proporciona una respuesta de autenticación a StorageGRID.
- StorageGRID valida la respuesta de autenticación.
- Si la respuesta es válida y usted pertenece a un grupo federado con permisos de acceso a StorageGRID, iniciará sesión en Grid Manager o en Tenant Manager, según la cuenta que haya seleccionado.



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

5. Opcionalmente, acceda a otros nodos de administración, o acceda al Administrador de red o al Administrador de inquilinos, si tiene los permisos adecuados.

No es necesario volver a ingresar sus credenciales SSO.

Cerrar sesión cuando el SSO esté habilitado

Cuando SSO está habilitado para StorageGRID, lo que sucede cuando cierra sesión depende de dónde haya iniciado sesión y desde dónde cierre sesión.

Pasos

1. Localice el enlace **Cerrar sesión** en la esquina superior derecha de la interfaz de usuario.
2. Seleccione **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, para que pueda acceder a estas interfaces de usuario más rápidamente en el futuro.

Si ha iniciado sesión en...	Y cierras sesión en...	Has cerrado sesión en...
Administrador de cuadrícula en uno o más nodos de administración	Administrador de cuadrícula en cualquier nodo de administración	Administrador de cuadrícula en todos los nodos de administración Nota: Si usa Azure para SSO, puede que lleve algunos minutos cerrar sesión en todos los nodos de administración.
Administrador de inquilinos en uno o más nodos de administración	Administrador de inquilinos en cualquier nodo de administración	Administrador de inquilinos en todos los nodos de administración
Tanto Grid Manager como Tenant Manager	Administrador de red	Sólo el administrador de cuadrícula. También debe cerrar sesión en el Administrador de inquilinos para cerrar sesión en SSO.



La tabla resume lo que sucede cuando cierras sesión si estás usando una sola sesión de navegador. Si ha iniciado sesión en StorageGRID en varias sesiones de navegador, deberá cerrar sesión en todas las sesiones de navegador por separado.

Requisitos y consideraciones para el inicio de sesión único

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

Requisitos del proveedor de identidad

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

- Servicio de federación de Active Directory (AD FS)
- Directorio activo de Azure (Azure AD)
- Federación de ping

Debe configurar la federación de identidad para su sistema StorageGRID antes de poder configurar un proveedor de identidad SSO. El tipo de servicio LDAP que utiliza para la federación de identidad controla qué tipo de SSO puede implementar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad SSO
Directorio activo	• Directorio activo • Azur • Federación de ping
Azur	Azur

Requisitos de AD FS

Puede utilizar cualquiera de las siguientes versiones de AD FS:

- ADFS de Windows Server 2022
- Servidor AD FS de Windows 2019
- Servidor AD FS de Windows 2016



Windows Server 2016 debería utilizar el ["Actualización KB3201845"](#) , o superior.

Requisitos adicionales

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

Consideraciones para Azure

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

Requisitos del certificado de servidor

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

Si aún no lo has hecho ["Configuró un certificado personalizado para la interfaz de administración"](#) Deberías hacerlo ahora. Cuando instala un certificado de servidor personalizado, este se utiliza para todos los nodos de administración y puede usarlo en todas las relaciones de confianza de usuarios confiables de StorageGRID , aplicaciones empresariales o conexiones de SP .



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

Puede acceder al certificado de servidor de un nodo de administración iniciando sesión en el shell de comandos del nodo y yendo a `/var/local/mgmt-api` directorio. Un certificado de servidor personalizado se denomina `custom-server.crt`. El certificado de servidor predeterminado del nodo se llama `server.crt`.

Requisitos del puerto

El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autenticuen con inicio de sesión único. Ver "[Controlar el acceso al firewall externo](#)".

Confirmar que los usuarios federados puedan iniciar sesión

Antes de habilitar el inicio de sesión único (SSO), debe confirmar 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

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes "[permisos de acceso específicos](#)".
- Ya ha configurado la federación de identidad.

Pasos

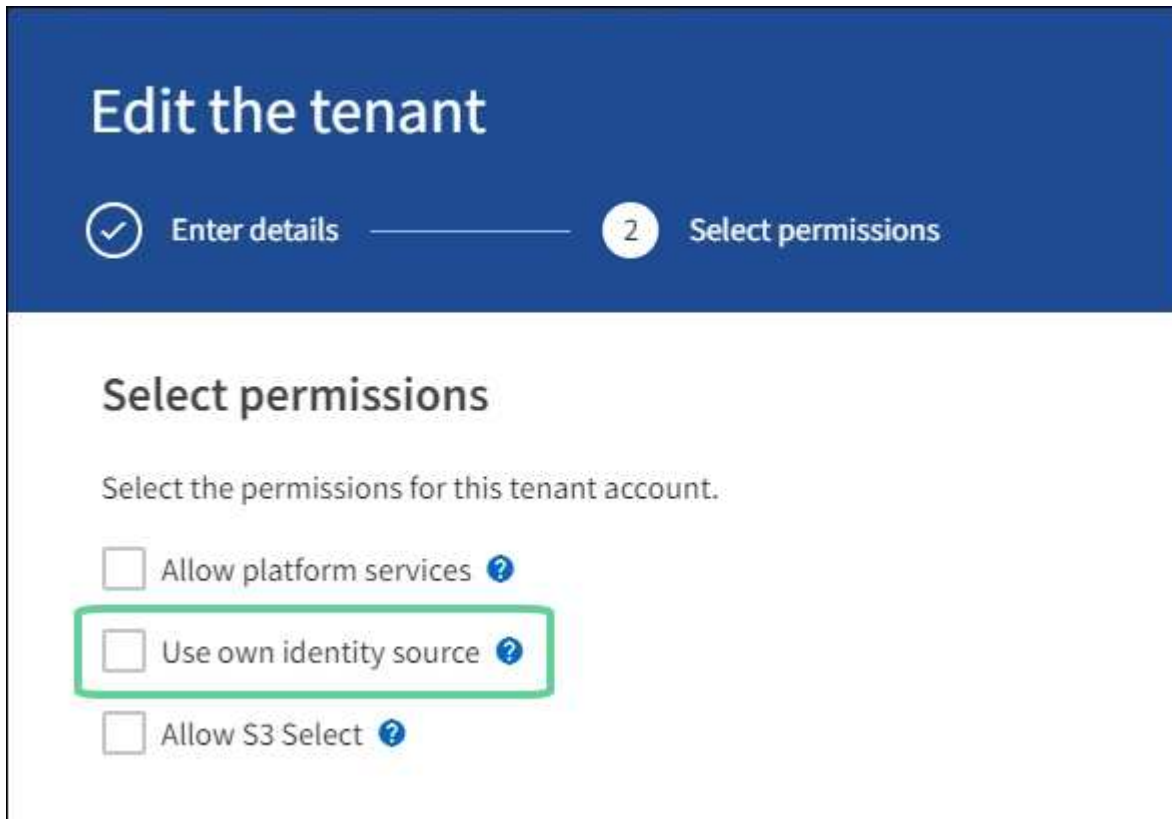
1. Si existen cuentas de inquilinos, confirme que ninguno de ellos esté usando su propia fuente de identidad.



Cuando habilita SSO, una fuente de identidad configurada en Tenant Manager se reemplaza por la fuente de identidad configurada en Grid Manager. Los usuarios que pertenecen a la fuente de identidad del inquilino ya no podrán iniciar sesión a menos que tengan una cuenta con la fuente de identidad de Grid Manager.

- a. Sign in en el Administrador de inquilinos para cada cuenta de inquilino.
 - b. Seleccione **GESTIÓN DE ACCESO > Federación de identidades**.
 - c. Confirme que la casilla de verificación **Habilitar federación de identidad** no esté seleccionada.
 - d. Si es así, confirme que cualquier grupo federado que pueda estar en uso para esta cuenta de inquilino ya no sea necesario, desmarque la casilla de verificación y seleccione **Guardar**.
2. Confirme que un usuario federado puede acceder al Administrador de Grid:
 - a. Desde Grid Manager, seleccione **CONFIGURACIÓN > Control de acceso > Grupos de administración**.
 - b. Asegúrese de que se haya importado al menos un grupo federado desde la fuente de identidad de Active Directory y que se le haya asignado el permiso de acceso raíz.
 - c. Desconectar.

- d. Confirme que puede volver a iniciar sesión en Grid Manager como usuario del grupo federado.
3. Si hay cuentas de inquilino existentes, confirme que un usuario federado que tenga permiso de acceso raíz pueda iniciar sesión:
 - a. Desde el Administrador de red, seleccione **INQUILINOS**.
 - b. Seleccione la cuenta del inquilino y seleccione **Acciones > Editar**.
 - c. En la pestaña Ingresar detalles, seleccione **Continuar**.
 - d. Si la casilla de verificación **Usar fuente de identidad propia** está seleccionada, desmarque la casilla y seleccione **Guardar**.



Aparece la página del inquilino.

- a. Seleccione la cuenta del inquilino, seleccione * Sign in* e inicie sesión en la cuenta del inquilino como usuario raíz local.
- b. Desde el Administrador de inquilinos, seleccione **ADMINISTRACIÓN DE ACCESO > Grupos**.
- c. Asegúrese de que al menos a un grupo federado del Administrador de Grid se le haya asignado el permiso de acceso raíz para este inquilino.
- d. Desconectar.
- e. Confirme que puede volver a iniciar sesión en el inquilino como usuario en el grupo federado.

Información relacionada

- ["Requisitos y consideraciones para el inicio de sesión único"](#)
- ["Administrar grupos de administradores"](#)
- ["Utilice una cuenta de inquilino"](#)

Utilizar el modo sandbox

Puede utilizar el modo sandbox para configurar y probar el inicio de sesión único (SSO) antes de habilitarlo para todos los usuarios de StorageGRID . Una vez habilitado el SSO, puede regresar al modo sandbox siempre que necesite cambiar o volver a probar la configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Ha configurado la federación de identidad para su sistema StorageGRID .
- Para la federación de identidad **tipo de servicio LDAP**, seleccionó Active Directory o Azure, según el proveedor de identidad SSO que planea usar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad SSO
Directorio activo	• Directorio activo • Azur • Federación de ping
Azur	Azur

Acerca de esta tarea

Cuando SSO está habilitado y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidad SSO. A su vez, el proveedor de identidad 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 Azure incluye un nombre principal de usuario (UPN).

Para permitir que StorageGRID (el proveedor de servicios) y el proveedor de identidad SSO se comuniquen de forma segura acerca de las solicitudes de autenticación de usuarios, debe configurar ciertas configuraciones en StorageGRID. A continuación, debe utilizar el software del proveedor de identidad SSO para crear una relación de confianza de usuario confiable (AD FS), una aplicación empresarial (Azure) o un proveedor de servicios (PingFederate) para cada nodo de administración. Por último, debes regresar a StorageGRID para habilitar SSO.

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

Acceder al modo sandbox

Pasos

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

Aparece la página de inicio de sesión único, con la opción **Deshabilitado** seleccionada.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO status ⓘ ☒ Disabled ☐ Sandbox Mode ☐ Enabled

Save



Si las opciones de Estado de SSO no aparecen, confirme que haya configurado el proveedor de identidad como fuente de identidad federada. Ver ["Requisitos y consideraciones para el inicio de sesión único"](#).

2. Seleccione **Modo Sandbox**.

Aparece la sección Proveedor de identidad.

Introduzca los datos del proveedor de identidad

Pasos

1. Seleccione el **tipo de SSO** de la lista desplegable.
2. Complete los campos en la sección Proveedor de identidad según el tipo de SSO que haya seleccionado.

Directorio activo

- a. Ingrese el **Nombre del servicio de federación** para el proveedor de identidad, exactamente como aparece en el Servicio de federación de Active Directory (AD FS).



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

- b. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID .

- **Usar certificado CA del sistema operativo:** utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado:** utilice un certificado CA personalizado para proteger la conexión.

Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

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



Si cambia el certificado de CA, inmediatamente ["reiniciar el servicio mgmt-api en los nodos de administración"](#) y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

- c. En la sección Parte confiada, especifique el **Identificador de parte confiada** para StorageGRID. Este valor controla el nombre que utiliza para cada relación de confianza de usuario confiable en AD FS.

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



Debe crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema StorageGRID . Tener una relación de confianza de parte confiable para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- d. Seleccione **Guardar**.

Aparece una marca de verificación verde en el botón **Guardar** durante unos segundos.



Azur

- a. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID .

- **Usar certificado CA del sistema operativo:** utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado:** utilice un certificado CA personalizado para proteger la conexión.

Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

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



Si cambia el certificado de CA, inmediatamente ["reiniciar el servicio mgmt-api en los nodos de administración"](#) y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

- b. En la sección Aplicación empresarial, especifique el **nombre de la aplicación empresarial** para StorageGRID. Este valor controla el nombre que utiliza para cada aplicación empresarial en Azure AD.

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



Debe crear una aplicación empresarial para cada nodo de administración en su sistema StorageGRID . Tener una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- c. Siga los pasos en ["Crear aplicaciones empresariales en Azure AD"](#) para crear una aplicación empresarial para cada nodo de administración enumerado en la tabla.
- d. Desde Azure AD, copie la URL de metadatos de federación para cada aplicación empresarial. Luego, pegue esta URL en el campo **URL de metadatos de federación** correspondiente en StorageGRID.
- e. Después de haber copiado y pegado una URL de metadatos de federación para todos los nodos de administración, seleccione **Guardar**.

Aparece una marca de verificación verde en el botón **Guardar** durante unos segundos.



Federación de ping

- a. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de

StorageGRID .

- **Usar certificado CA del sistema operativo:** utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado:** utilice un certificado CA personalizado para proteger la conexión.

Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

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



Si cambia el certificado de CA, inmediatamente ["reiniciar el servicio mgmt-api en los nodos de administración"](#) y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

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

- Por ejemplo, si su red tiene solo un nodo de administración y no prevé agregar más nodos de administración en el futuro, ingrese SG o StorageGRID .
- Si su cuadrícula incluye más de un nodo de administración, incluya la cadena [HOSTNAME] en el identificador. Por ejemplo, SG-[HOSTNAME] . Esto genera una tabla que muestra el ID de conexión de SP para cada nodo de administración en su sistema, según el nombre de host del nodo.



Debe crear una conexión SP para cada nodo de administración en su sistema StorageGRID . Tener 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.

- c. Especifique la URL de metadatos de la federación para cada nodo de administración en el campo **URL de metadatos de la federación**.

Utilice el siguiente formato:

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

- d. Seleccione **Guardar**.

Aparece una marca de verificación verde en el botón **Guardar** durante unos segundos.

Save 

Configurar relaciones de confianza entre usuarios, aplicaciones empresariales o conexiones de SP

Cuando se guarda la configuración, aparece el aviso de confirmación del modo Sandbox. Este aviso confirma que el modo sandbox ahora está habilitado y proporciona instrucciones generales.

StorageGRID puede permanecer en modo sandbox tanto tiempo como sea necesario. Sin embargo, cuando se selecciona **Modo Sandbox** en la página de Inicio de sesión único, el SSO se deshabilita para todos los usuarios de StorageGRID . Sólo los usuarios locales pueden iniciar sesión.

Siga estos pasos para configurar relaciones de confianza de usuarios autenticados (Active Directory), completar aplicaciones empresariales (Azure) o configurar conexiones de SP (PingFederate).

Directorio activo

Pasos

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

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

Para obtener instrucciones, vaya a ["Crear relaciones de confianza entre usuarios autenticados en AD FS"](#) .

Azur

Pasos

1. Desde la página de inicio de sesión único del nodo de administración en el que está conectado actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en su red, repita estos pasos:
 - a. Sign in en el nodo.
 - b. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
 - c. Descargue y guarde los metadatos SAML para ese nodo.
3. Vaya al Portal de Azure.
4. Siga los pasos en ["Crear aplicaciones empresariales en Azure AD"](#) para cargar el archivo de metadatos SAML para cada nodo de administración en su aplicación empresarial de Azure correspondiente.

Federación de ping

Pasos

1. Desde la página de inicio de sesión único del nodo de administración en el que está conectado actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en su red, repita estos pasos:
 - a. Sign in en el nodo.
 - b. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
 - c. Descargue y guarde los metadatos SAML para ese nodo.
3. Vaya a PingFederate.
4. ["Cree una o más conexiones de proveedor de servicios \(SP\) para StorageGRID"](#) . Utilice el ID de conexión de SP para cada nodo de administración (que se muestra en la tabla de la página de inicio de sesión único de StorageGRID) y los metadatos SAML que descargó para ese nodo de administración.

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

Probar conexiones SSO

Antes de implementar el uso del inicio de sesión único para todo el sistema StorageGRID , debe confirmar que

el inicio de sesión único y el cierre de sesión único estén configurados correctamente para cada nodo de administración.

Directorio activo

Pasos

1. Desde la página de inicio de sesión único de StorageGRID , busque el enlace en el mensaje del modo Sandbox.

La URL se deriva del valor ingresado en el campo **Nombre del servicio de federación**.

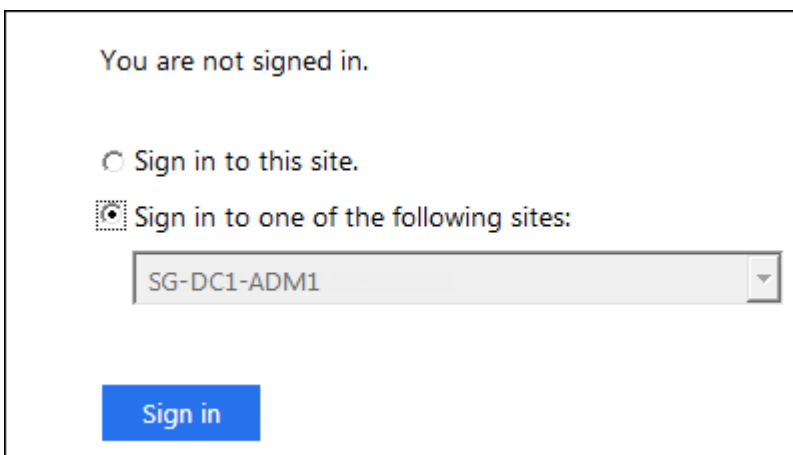
Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

2. Seleccione el enlace o copie y pegue la URL en un navegador para acceder a la página de inicio de sesión de su proveedor de identidad.
3. Para confirmar que puede usar SSO para iniciar sesión en StorageGRID, seleccione * Sign in en uno de los siguientes sitios , **seleccione el identificador de parte confiable para su nodo de administración principal y seleccione * Sign in**.



You are not signed in.

☐ Sign in to this site.

☒ Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

4. Introduzca su nombre de usuario y contraseña federados.
 - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

✓ Single sign-on authentication and logout test completed successfully.

- Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
5. Repita estos pasos para verificar la conexión SSO para cada nodo de administración en su red.

Azur

Pasos

1. Vaya a la página de inicio de sesión único en el portal de Azure.
2. Seleccione **Probar esta aplicación**.
3. Introduzca las credenciales de un usuario federado.
 - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

✓ Single sign-on authentication and logout test completed successfully.

- Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
4. Repita estos pasos para verificar la conexión SSO para cada nodo de administración en su red.

Federación de ping

Pasos

1. Desde la página de inicio de sesión único de StorageGRID , seleccione el primer enlace en el mensaje del modo Sandbox.

Seleccione y pruebe un enlace a la vez.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. Introduzca las credenciales de un usuario federado.
 - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

✓ Single sign-on authentication and logout test completed successfully.

- Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
3. Seleccione el siguiente enlace para verificar la conexión SSO para cada nodo de administración en su red.

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

Habilitar el inicio de sesión único

Cuando haya confirmado que puede usar SSO para iniciar sesión en cada nodo de administración, podrá habilitar SSO para todo su sistema StorageGRID .



Cuando SSO está habilitado, todos los usuarios deben usar SSO para acceder al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos. Los usuarios locales ya no pueden acceder a StorageGRID.

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
2. Cambie el estado de SSO a **Habilitado**.
3. Seleccione **Guardar**.
4. Revise el mensaje de advertencia y seleccione **Aceptar**.

El inicio de sesión único ahora está habilitado.



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

Crear relaciones de confianza entre usuarios autenticados en AD FS

Debe utilizar los Servicios de federación de Active Directory (AD FS) para crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema. Puede crear relaciones de confianza de usuario autenticado mediante comandos de PowerShell, importando metadatos SAML desde StorageGRID o ingresando los datos manualmente.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y seleccionó **AD FS** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver ["Utilizar el modo sandbox"](#) .
- Conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte confiable para cada nodo de administración en su sistema. Puede encontrar estos valores en la tabla de detalles de Nodos de administración en la página de inicio de sesión único de StorageGRID .



Debe crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema StorageGRID . Tener una relación de confianza de parte confiable para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- Tiene experiencia en la creación de relaciones de confianza de usuario autenticado en AD FS o tiene acceso a la documentación de Microsoft AD FS.
- Está utilizando el complemento Administración de AD FS y pertenece al grupo Administradores.
- Si está creando la confianza de usuario confiable manualmente, tiene el certificado personalizado que se

cargó para la interfaz de administración de StorageGRID o sabe cómo iniciar sesión en un nodo de administración desde el shell de comandos.

Acerca de esta tarea

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

Crear una relación de confianza de usuario autenticado mediante Windows PowerShell

Puede utilizar Windows PowerShell para crear rápidamente una o más relaciones de confianza de usuario autenticado.

Pasos

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

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

- Para *Admin_Node_Identifer*, ingrese el Identificador de parte confiable para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único. Por ejemplo, SG-DC1-ADM1 .
- Para *Admin_Node_FQDN*, ingrese el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

3. Desde el Administrador de servidor de Windows, seleccione **Herramientas > Administración de AD FS**.

Aparece la herramienta de administración de AD FS.

4. Seleccione **AD FS > Confianzas de usuario autenticado**.

Aparece la lista de fideicomisos de partes confiantes.

5. Agregue una Política de control de acceso a la confianza de usuario autenticado recién creada:

- a. Localice el fideicomiso de parte confiante que acaba de crear.
- b. Haga clic derecho en la confianza y seleccione **Editar política de control de acceso**.
- c. Seleccione una política de control de acceso.
- d. Seleccione **Aplicar** y seleccione **Aceptar**

6. Agregue una Política de emisión de reclamaciones al fideicomiso de parte confiada recién creado:

- a. Localice el fideicomiso de parte confiante que acaba de crear.
- b. Haga clic derecho en el fideicomiso y seleccione **Editar política de emisión de reclamaciones**.
- c. Seleccione **Agregar regla**.
- d. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** de la lista y seleccione **Siguiente**.
- e. En la página Configurar regla, ingrese 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, seleccione **Active Directory**.
 - g. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.
 - h. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.
 - i. Seleccione **Finalizar** y seleccione **Aceptar**.
7. Confirme que los metadatos se importaron correctamente.
- a. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
 - b. Confirme que los campos en las pestañas **Puntos finales**, **Identificadores** y **Firma** estén completos.
- Si faltan los metadatos, confirme que la dirección de metadatos de la Federación sea correcta o ingrese los valores manualmente.
8. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .
9. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver "[Utilizar el modo Sandbox](#)" para obtener instrucciones.

Cree una relación de confianza entre usuarios autenticados mediante la importación de metadatos de la federación

Puede importar los valores para cada entidad de confianza accediendo a los metadatos SAML de cada nodo de administración.

Pasos

1. En el Administrador de servidor de Windows, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En Acciones, seleccione **Agregar confianza de usuario autenticado**.
3. En la página de bienvenida, seleccione **Reclamos conscientes** y seleccione **Iniciar**.
4. Seleccione **Importar datos sobre la parte confiante publicados en línea o en una red local**.
5. En **Dirección de metadatos de la federación (nombre de host o URL)**, escriba la ubicación de los metadatos SAML para este nodo de administración:

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

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

6. Complete el asistente de confianza de usuario autenticado, guarde la confianza de usuario autenticado y cierre el asistente.



Al ingresar el nombre para mostrar, utilice el Identificador de usuario confiado para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único en el Administrador de Grid. Por ejemplo, SG-DC1-ADM1 .

7. Agregar una regla de reclamación:

- a. Haga clic derecho en el fideicomiso y seleccione **Editar política de emisión de reclamaciones**.
- b. Seleccione **Agregar regla**:
- c. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** de la lista y seleccione **Siguiente**.
- d. En la página Configurar regla, ingrese 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, seleccione **Active Directory**.
- f. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.
- g. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.
- h. Seleccione **Finalizar** y seleccione **Aceptar**.

8. Confirme que los metadatos se importaron correctamente.

- a. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
- b. Confirme que los campos en las pestañas **Puntos finales**, **Identificadores** y **Firma** estén completos.

Si faltan los metadatos, confirme que la dirección de metadatos de la Federación sea correcta o ingrese los valores manualmente.

9. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .

10. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver "[Utilizar el modo Sandbox](#)" para obtener instrucciones.

Crear una relación de confianza de usuario confiado manualmente

Si decide no importar los datos de las confianzas de las partes confiables, puede ingresar los valores manualmente.

Pasos

1. En el Administrador de servidor de Windows, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En Acciones, seleccione **Agregar confianza de usuario autenticado**.
3. En la página de bienvenida, seleccione **Reclamos conscientes** y seleccione **Iniciar**.
4. Seleccione **Ingresar datos sobre la parte confiada manualmente** y seleccione **Siguiente**.
5. Complete el Asistente de confianza de usuario autenticado:
 - a. Introduzca un nombre para mostrar para este nodo de administración.

Para mantener la coherencia, utilice el Identificador de usuario autenticado para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único en el Administrador de Grid. Por ejemplo, SG-DC1-ADM1 .

- b. Omita el paso para configurar un certificado de cifrado de token opcional.
- c. En la página Configurar URL, seleccione la casilla de verificación **Habilitar soporte para el protocolo SAML 2.0 WebSSO**.
- d. Escriba la URL del punto final del servicio SAML para el nodo de administración:

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

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

- e. En la página Configurar identificadores, especifique el identificador de usuario de confianza para el mismo nodo de administración:

Admin_Node_Identifier

Para *Admin_Node_Identifier*, ingrese el Identificador de parte confiable para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único. Por ejemplo, SG-DC1-ADM1 .

- f. Revise la configuración, guarde la confianza del usuario autenticado y cierre el asistente.

Aparece el cuadro de diálogo Editar política de emisión de reclamaciones.



Si el cuadro de diálogo no aparece, haga clic con el botón derecho en el fideicomiso y seleccione **Editar política de emisión de reclamaciones**.

6. Para iniciar el asistente de reglas de reclamación, seleccione **Agregar regla**:
 - a. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** de la lista y seleccione **Siguiente**.
 - b. En la página Configurar regla, ingrese 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, seleccione **Active Directory**.
 - d. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.
 - e. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.
 - f. Seleccione **Finalizar** y seleccione **Aceptar**.
7. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
8. En la pestaña **Puntos finales**, configure el punto final para el cierre de sesión único (SLO):
 - a. Seleccione **Agregar SAML**.
 - b. Seleccione **Tipo de punto final > Cerrar sesión SAML**.
 - c. Seleccione **Enlace > Redireccionar**.
 - d. En el campo **URL de confianza**, ingrese la URL utilizada para el cierre de sesión único (SLO) desde

este nodo de administración:

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

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

a. Seleccione **Aceptar**.

9. En la pestaña **Firma**, especifique el certificado de firma para esta relación de confianza de usuario autenticado:

a. Agregue el certificado personalizado:

- Si tiene el certificado de administración personalizado que cargó en StorageGRID, seleccione ese certificado.
- Si no tiene el certificado personalizado, inicie sesión en el Nodo de administración, vaya a `/var/local/mgmt-api` directorio del nodo de administración y agregue el `custom-server.crt` archivo de certificado.



Uso del certificado predeterminado del nodo de administración(`server.crt`) no se recomienda. Si el nodo de administración falla, se regenerará el certificado predeterminado cuando recupere el nodo y deberá actualizar la confianza de la parte confiable.

b. Seleccione **Aplicar** y seleccione **Aceptar**.

Las propiedades de la parte confiada se guardan y cierran.

10. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .
11. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver "[Utilizar el modo sandbox](#)" para obtener instrucciones.

Crear aplicaciones empresariales en Azure AD

Utilice Azure AD para crear una aplicación empresarial para cada nodo de administración en su sistema.

Antes de empezar

- Ha comenzado a configurar el inicio de sesión único para StorageGRID y seleccionó **Azure** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver "[Utilizar el modo sandbox](#)".
- Tiene el **nombre de la aplicación empresarial** para cada nodo de administración en su sistema. Puede copiar estos valores de la tabla de detalles del nodo de administración en la página de inicio de sesión único de StorageGRID .



Debe crear una aplicación empresarial para cada nodo de administración en su sistema StorageGRID . Tener una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- Tiene experiencia en la creación de aplicaciones empresariales en Azure Active Directory.
- Tiene una cuenta de Azure con una suscripción activa.
- Tiene uno de los siguientes roles en la cuenta de Azure: Administrador global, Administrador de aplicaciones en la nube, Administrador de aplicaciones o propietario de la entidad de servicio.

Acceder a Azure AD

Pasos

1. Iniciar sesión en el "[Portal de Azure](#)" .
2. Navegar a "[Directorio activo de Azure](#)" .
3. Seleccionar "[Aplicaciones empresariales](#)" .

Cree aplicaciones empresariales y guarde la configuración de SSO de StorageGRID

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

Pasos

1. Repita los siguientes pasos para cada nodo de administración.
 - a. En el panel de aplicaciones empresariales de Azure, seleccione **Nueva aplicación**.
 - b. Seleccione **Crea tu propia aplicación**.
 - c. Para el nombre, ingrese el **nombre de la aplicación empresarial** que copió de la tabla de detalles del nodo de administración en la página de inicio de sesión único de StorageGRID .
 - d. Deje seleccionado el botón de opción **Integrar cualquier otra aplicación que no encuentre en la galería (No galería)**.
 - e. Seleccione **Crear**.
 - f. Seleccione el enlace **Comenzar** en el **2. Configurar el cuadro de inicio de sesión único** o seleccione el enlace **Inicio de sesión único** en el margen izquierdo.
 - g. Seleccione la casilla **SAML**.
 - h. Copie la **URL de metadatos de federación de aplicaciones**, que puede encontrar en el **Paso 3 Certificado de firma SAML**.
 - i. Vaya a la página de inicio de sesión único de StorageGRID y pegue en el campo **URL de metadatos de federación** la URL que corresponde al **nombre de la aplicación empresarial** que utilizó.
2. Después de haber pegado una URL de metadatos de federación para cada nodo de administración y realizado todos los demás cambios necesarios en la configuración de SSO, seleccione **Guardar** en la página de inicio de sesión único de StorageGRID .

Descargar metadatos SAML para cada nodo de administración

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

Pasos

1. Repita estos pasos para cada nodo de administración.
 - a. Sign in en StorageGRID desde el nodo de administración.
 - b. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
 - c. Seleccione el botón para descargar los metadatos SAML para ese nodo de administración.
 - d. Guarde el archivo que cargará en Azure AD.

Cargar metadatos SAML a cada aplicación empresarial

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

Pasos

1. Regresar al Portal de Azure.
2. Repita estos pasos para cada aplicación empresarial:



Es posible que necesites actualizar la página de aplicaciones empresariales para ver las aplicaciones que agregaste previamente a la lista.

- a. Vaya a la página Propiedades de la aplicación empresarial.
 - b. Establezca **Tarea requerida** en **No** (a menos que desee configurar las asignaciones por separado).
 - c. Vaya a la página de inicio de sesión único.
 - d. Complete la configuración de SAML.
 - e. Seleccione el botón **Cargar archivo de metadatos** y seleccione el archivo de metadatos SAML que descargó para el nodo de administración correspondiente.
 - f. Después de cargar el archivo, seleccione **Guardar** y luego seleccione **X** para cerrar el panel. Regresará a la página Configurar inicio de sesión único con SAML.
3. Siga los pasos en "[Utilizar el modo sandbox](#)" para probar cada aplicación.

Crear conexiones de proveedor de servicios (SP) en PingFederate

Utilice PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración en su sistema. Para acelerar el proceso, importará los metadatos SAML desde StorageGRID.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y seleccionó **Ping Federate** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver "[Utilizar el modo sandbox](#)".
- Tienes el *ID de conexión SP * para cada nodo de administración en tu sistema. Puede encontrar estos valores en la tabla de detalles de Nodos de administración en la página de inicio de sesión único de

StorageGRID .

- Ha descargado los **metadatos SAML** para cada nodo de administración en su sistema.
- Tiene experiencia en la creación de conexiones SP en PingFederate Server.
- Tú tienes el https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html ["Guía de referencia del administrador"] para el servidor PingFederate. La documentación de PingFederate proporciona instrucciones y explicaciones detalladas paso a paso.
- Tú tienes el "[Permiso de administrador](#)" para el servidor PingFederate.

Acerca de esta tarea

Estas instrucciones resumen cómo configurar PingFederate Server versión 10.3 como proveedor de SSO para StorageGRID. Si está utilizando otra versión de PingFederate, es posible que deba adaptar estas instrucciones. Consulte la documentación del servidor PingFederate para obtener instrucciones detalladas para su versión.

Requisitos previos completos en PingFederate

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

Crear almacén de datos[[almacén de datos]]

Si aún no lo ha hecho, cree un almacén de datos para conectar PingFederate al servidor LDAP de AD FS. Utilice los valores que utilizó cuando "[configuración de la federación de identidades](#)" en StorageGRID.

- **Tipo:** Directorio (LDAP)
- **Tipo LDAP:** Directorio activo
- **Nombre del atributo binario:** Ingrese **objectGUID** en la pestaña Atributos binarios LDAP exactamente como se muestra.

Crear un validador de credenciales de contraseña

Si aún no lo ha hecho, cree un validador de credenciales de contraseña.

- **Tipo:** LDAP Nombre de usuario Contraseña Credencial Validador
- **Almacén de datos:** seleccione el almacén de datos que creó.
- **Base de búsqueda:** Ingrese información de LDAP (por ejemplo, DC=saml,DC=sgws).
- **Filtro de búsqueda:** sAMAccountName=\${username}
- **Alcance:** Subárbol

Crear una instancia de adaptador de IdP

Si aún no lo ha hecho, cree una instancia de adaptador IdP.

Pasos

1. Vaya a **Autenticación > Integración > Adaptadores IdP**.
2. Seleccione **Crear nueva instancia**.

3. En la pestaña Tipo, seleccione **Adaptador IdP de formulario HTML**.
4. En la pestaña Adaptador IdP, seleccione **Agregar una nueva fila a 'Validadores de credenciales'**.
5. Seleccione el [validador de credenciales de contraseña](#) tu creaste
6. En la pestaña Atributos del adaptador, seleccione el atributo **nombre de usuario** para **Seudónimo**.
7. Seleccione **Guardar**.

Crear o importar certificado de firma

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

Pasos

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

Crear una conexión SP en PingFederate

Cuando crea una conexión SP en PingFederate, importa los metadatos SAML que descargó de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos que necesita.



Debe crear una conexión SP para cada nodo de administración en su sistema StorageGRID , de modo que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo. Utilice estas instrucciones para crear la primera conexión SP . Luego, ve a [Crear conexiones SP adicionales](#) para crear cualquier conexión adicional que necesites.

Elija el tipo de conexión SP

Pasos

1. Vaya a **Aplicaciones > Integración > *Conexiones SP ***.
2. Seleccione **Crear conexión**.
3. Seleccione **No utilizar una plantilla para esta conexión**.
4. Seleccione **Perfiles SSO del navegador y SAML 2.0** como protocolo.

Importar metadatos de SP

Pasos

1. En la pestaña Importar metadatos, seleccione **Archivo**.
2. Elija el archivo de metadatos SAML que descargó de la página de inicio de sesión único de StorageGRID para el nodo de administración.
3. Revise el Resumen de metadatos y la información proporcionada en la pestaña Información general.

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

4. Seleccione **Siguiente**.

Configurar el inicio de sesión único (SSO) del navegador IdP

Pasos

1. Desde la pestaña SSO del navegador, seleccione **Configurar SSO del navegador**.
2. En la pestaña Perfiles SAML, seleccione las opciones * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** y **IdP-initiated SLO**.
3. Seleccione **Siguiente**.
4. En la pestaña Duración de la afirmación, no realice cambios.
5. En la pestaña Creación de aserciones, seleccione **Configurar creación de aserciones**.
 - a. En la pestaña Asignación de identidad, seleccione **Estándar**.
 - b. En la pestaña Contrato de atributo, utilice **SAML_SUBJECT** como Contrato de atributo y el formato de nombre no especificado que se importó.
6. Para extender el contrato, seleccione **Eliminar** para quitar el `urn:oid`, que no se utiliza.

Instancia del adaptador de mapas

Pasos

1. En la pestaña Mapeo de origen de autenticación, seleccione **Asignar nueva instancia de adaptador**.
2. En la pestaña Instancia del adaptador, seleccione la [instancia de adaptador](#) que creaste.
3. En la pestaña Método de mapeo, seleccione **Recuperar atributos adicionales de un almacén de datos**.
4. En la pestaña Origen de atributos y búsqueda de usuarios, seleccione **Agregar origen de atributos**.
5. En la pestaña Almacén de datos, proporcione una descripción y seleccione el [almacén de datos](#) que usted agregó.
6. En la pestaña Búsqueda de directorio LDAP:
 - Ingrese el **DN base**, que debe coincidir exactamente con el valor ingresado en StorageGRID para el servidor LDAP.
 - Para el ámbito de búsqueda, seleccione **Subárbol**.
 - Para la clase de objeto raíz, busque y agregue cualquiera de estos atributos: **objectGUID** o **userPrincipalName**.
7. En la pestaña Tipos de codificación de atributos binarios LDAP, seleccione **Base64** para el atributo **objectGUID**.
8. En la pestaña Filtro LDAP, ingrese **sAMAccountName=\${username}**.
9. En la pestaña Cumplimiento de contrato de atributo, seleccione **LDAP (atributo)** en el menú desplegable Fuente y seleccione **objectGUID** o **userPrincipalName** en el menú desplegable Valor.
10. Revise y luego guarde la fuente del atributo.
11. En la pestaña Origen del atributo de guardado fallido, seleccione **Anular la transacción SSO**.
12. Revise el resumen y seleccione **Listo**.
13. Seleccione **Listo**.

Configurar los ajustes del protocolo

Pasos

1. En la pestaña **Conexión SP * > *SSO del navegador > Configuración del protocolo**, seleccione

Configurar configuración del protocolo.

2. En la pestaña URL del servicio de consumidor de aserciones, acepte los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**POST** para enlace y `/api/saml-response` para la URL del punto final).
3. En la pestaña URL del servicio SLO, acepte los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**REDIRECT** para enlace y `/api/saml-logout` para URL de punto final).
4. En la pestaña Enlaces SAML permitidos, desactive **ARTIFACT** y **SOAP**. Sólo se requieren **POST** y **REDIRECT**.
5. En la pestaña Política de firma, deje seleccionadas las casillas de verificación **Requerir que las solicitudes de autenticación estén firmadas** y **Firmar siempre la afirmación**.
6. En la pestaña Política de cifrado, seleccione **Ninguno**.
7. Revise el resumen y seleccione **Listo** para guardar la configuración del protocolo.
8. Revise el resumen y seleccione **Listo** para guardar la configuración de SSO del navegador.

Configurar credenciales

Pasos

1. Desde la pestaña Conexión SP , seleccione **Credenciales**.
2. Desde la pestaña Credenciales, seleccione **Configurar credenciales**.
3. Seleccione el [certificado de firma](#) usted creó o importó.
4. Seleccione **Siguiente** para ir a **Administrar configuración de verificación de firma**.
 - a. En la pestaña Modelo de confianza, seleccione **Sin ancla**.
 - b. En la pestaña Certificado de verificación de firma, revise la información del certificado de firma, que se importó de los metadatos SAML de StorageGRID .
5. Revise las pantallas de resumen y seleccione **Guardar** para guardar la conexión SP .

Crear conexiones SP adicionales

Puede copiar la primera conexión SP para crear las conexiones SP que necesita para cada nodo de administración en su red. Carga nuevos metadatos para cada copia.



Las conexiones SP para diferentes nodos de administración utilizan configuraciones idénticas, con la excepción del ID de entidad del socio, la URL base, el ID de conexión, el nombre de la conexión, la verificación de firma y la URL de respuesta de SLO.

Pasos

1. Seleccione **Acción** > **Copiar** para crear una copia de la conexión SP inicial para cada nodo de administración adicional.
2. Ingrese el ID de conexión y el nombre de conexión para la copia y seleccione **Guardar**.
3. Seleccione el archivo de metadatos correspondiente al Nodo de Administración:
 - a. Seleccione **Acción** > **Actualizar con metadatos**.
 - b. Seleccione **Elegir archivo** y cargue los metadatos.
 - c. Seleccione **Siguiente**.

- d. Seleccione **Guardar**.
4. Resuelva el error debido al atributo no utilizado:
 - a. Seleccione la nueva conexión.
 - b. Seleccione **Configurar SSO del navegador > Configurar creación de afirmaciones > Contrato de atributos**.
 - c. Eliminar la entrada para **urn:oid**.
 - d. Seleccione **Guardar**.

Deshabilitar el inicio de sesión único

Puede desactivar el inicio de sesión único (SSO) si ya no desea utilizar esta funcionalidad. Debe deshabilitar el inicio de sesión único antes de poder deshabilitar la federación de identidad.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).

Pasos

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

Aparece la página de inicio de sesión único.

2. Seleccione la opción **Deshabilitado**.
3. Seleccione **Guardar**.

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

4. Seleccione **Aceptar**.

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

Deshabilitar temporalmente y volver a habilitar el inicio de sesión único para un nodo de administración

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

Antes de empezar

- Tienes ["permisos de acceso específicos"](#).
- Tú tienes el `Passwords.txt` archivo.
- Conoces la contraseña del usuario root local.

Acerca de esta tarea

Después de deshabilitar SSO para un nodo de administración, puede iniciar sesión en Grid Manager como usuario raíz local. Para proteger su sistema StorageGRID, debe usar el shell de comandos del nodo para

volver a habilitar SSO en el nodo de administración tan pronto como cierre la sesión.



Deshabilitar SSO para un nodo de administración no afecta la configuración de SSO de ningún otro nodo de administración en la red. La casilla de verificación **Habilitar SSO** en la página de Inicio de sesión único en el Administrador de Grid permanece seleccionada y todas las configuraciones de SSO existentes se mantienen a menos que las actualice.

Pasos

1. Inicie sesión en un nodo de administración:

- Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- Introduzca el siguiente comando para cambiar a root: `su -`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de \$ a # .

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

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

3. Confirme que desea deshabilitar SSO.

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

4. Desde un navegador web, acceda al Administrador de cuadrícula en el mismo nodo de administración.

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

5. Sign in con el nombre de usuario root y la contraseña del usuario root local.

6. Si deshabilitó SSO temporalmente porque necesitaba corregir la configuración de SSO:

- Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
- Cambie la configuración de SSO incorrecta o desactualizada.
- Seleccione **Guardar**.

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

7. Si deshabilitó el SSO temporalmente porque necesitaba acceder al Administrador de Grid por algún otro motivo:

- Realice cualquier tarea o tareas que necesite realizar.
- Seleccione **Cerrar sesión** y cierre el Administrador de cuadrícula.
- Vuelva a habilitar SSO en el nodo de administración. Puede realizar cualquiera de los siguientes pasos:

- Ejecute el siguiente comando: `enable-saml`

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

Confirme que desea habilitar SSO.

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

- Reiniciar el nodo de la red: `reboot`

8. Desde un navegador web, acceda al Administrador de cuadrícula desde el mismo nodo de administración.
9. Confirme que aparezca la página de Sign in de StorageGRID y que debe ingresar sus credenciales de SSO para acceder al Administrador de Grid.

Utilizar la federación de red

¿Qué es la federación de red?

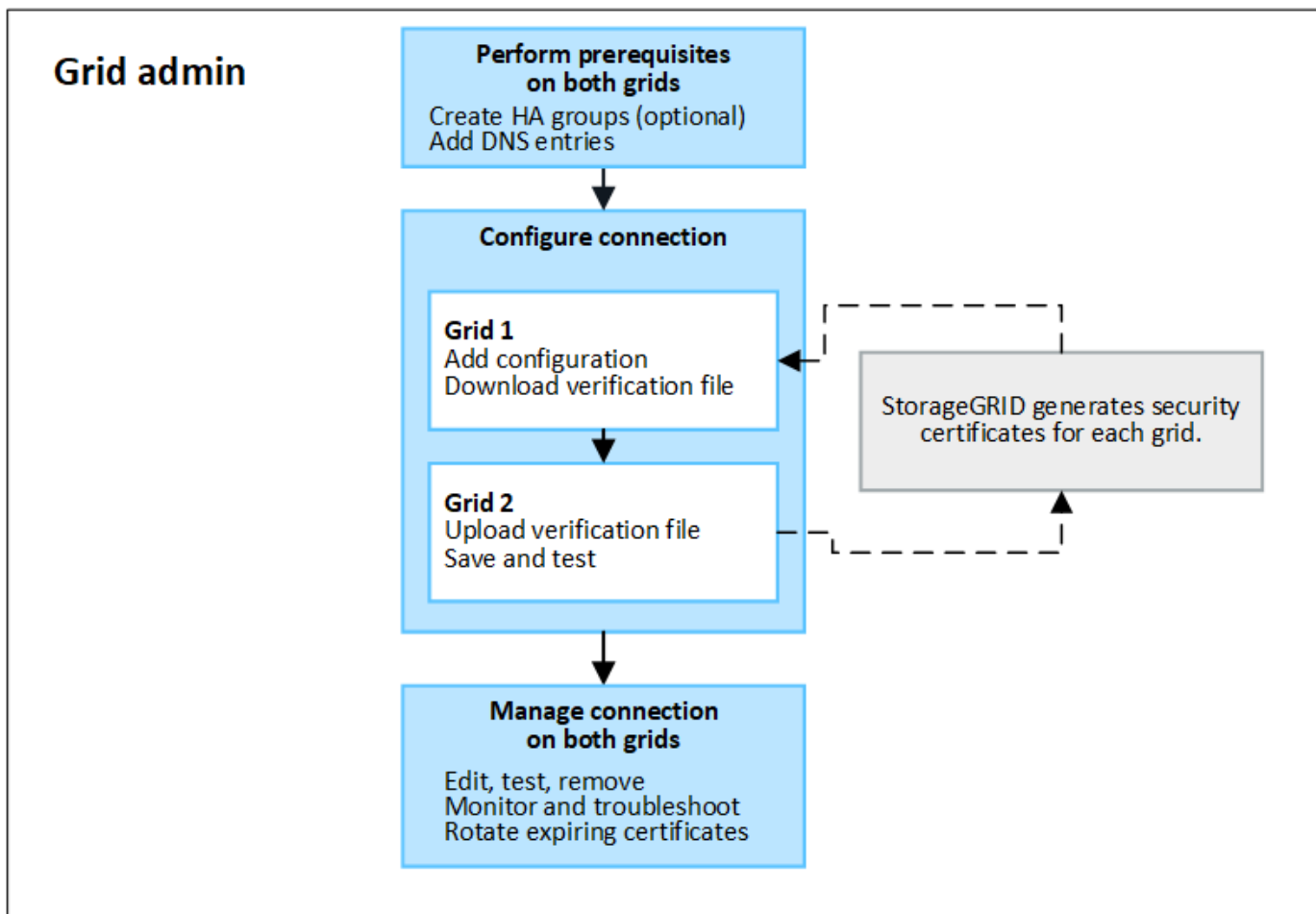
Puede utilizar la federación de red para clonar inquilinos y replicar sus objetos entre dos sistemas StorageGRID para la recuperación ante desastres.

¿Qué es una conexión de federación de red?

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

Flujo de trabajo para la federación de redes

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



Consideraciones y requisitos para las conexiones de federación de red

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

Para obtener detalles sobre los requisitos de la versión, consulte la ["Notas de la versión"](#).

- Una red puede tener una o más conexiones de federación de redes a otras redes. Cada conexión de federación de red es independiente de cualquier otra conexión. Por ejemplo, si la Red 1 tiene una conexión con la Red 2 y una segunda conexión con la Red 3, no hay ninguna conexión implícita entre la Red 2 y la Red 3.
- Las conexiones de la federación de red son bidireccionales. Una vez establecida la conexión, puedes supervisarla y administrarla desde cualquiera de las redes.
- Debe existir al menos una conexión de federación de red antes de poder usar ["clon de cuenta"](#) o ["replicación entre redes"](#).

Requisitos de red y dirección IP

- Las conexiones de federación de red pueden ocurrir en la red de red, la red de administración o la red de cliente.
- Una conexión de federación de red conecta una red con otra red. La configuración de cada red especifica un punto final de federación de red en la otra red que consta de nodos de administración, nodos de puerta de enlace o ambos.
- La mejor práctica es conectar ["grupos de alta disponibilidad \(HA\)"](#) de nodos de puerta de enlace y de

administración en cada red. El uso de grupos de alta disponibilidad ayuda a garantizar que las conexiones de la federación de red permanecerán en línea si los nodos no están disponibles. Si falla la interfaz activa en cualquiera de los grupos HA, la conexión puede usar una interfaz de respaldo.

- No se recomienda crear una conexión de federación de red que utilice la dirección IP de un solo nodo de administración o nodo de puerta de enlace. Si el nodo deja de estar disponible, la conexión de la federación de red también dejará de estar disponible.
- **"Replicación entre redes"** La creación de objetos requiere que los nodos de almacenamiento en cada red puedan acceder a los nodos de administración y de puerta de enlace configurados en la otra red. Para cada cuadrícula, confirme que todos los nodos de almacenamiento tengan una ruta de alto ancho de banda como los nodos de administración o los nodos de puerta de enlace utilizados para la conexión.

Utilice FQDN para equilibrar la carga de la conexión

Para un entorno de producción, utilice nombres de dominio completos (FQDN) para identificar cada cuadrícula en la conexión. Luego, crea las entradas DNS apropiadas, de la siguiente manera:

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

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

- Las entradas DNS que se asignan a las direcciones VIP de varios grupos de HA se equilibran entre los nodos activos en los grupos de HA.
- Las entradas DNS que se asignan a las direcciones IP de varios nodos de administración o nodos de puerta de enlace se equilibran entre los nodos asignados.

Requisitos del puerto

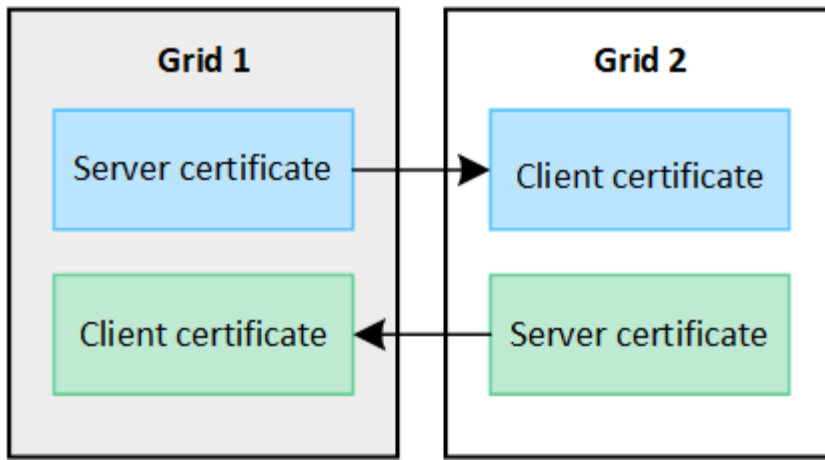
Al crear una conexión de federación de red, puede especificar cualquier número de puerto no utilizado del 23000 al 23999. Ambas redes en esta conexión utilizarán el mismo puerto.

Debe asegurarse de que ningún nodo de ninguna de las redes utilice este puerto para otras conexiones.

Requisitos del certificado

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

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



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



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

Más información

- ["Crear conexiones de federación de red"](#)
- ["Administrar conexiones de federación de red"](#)
- ["Solucionar errores de federación de red"](#)

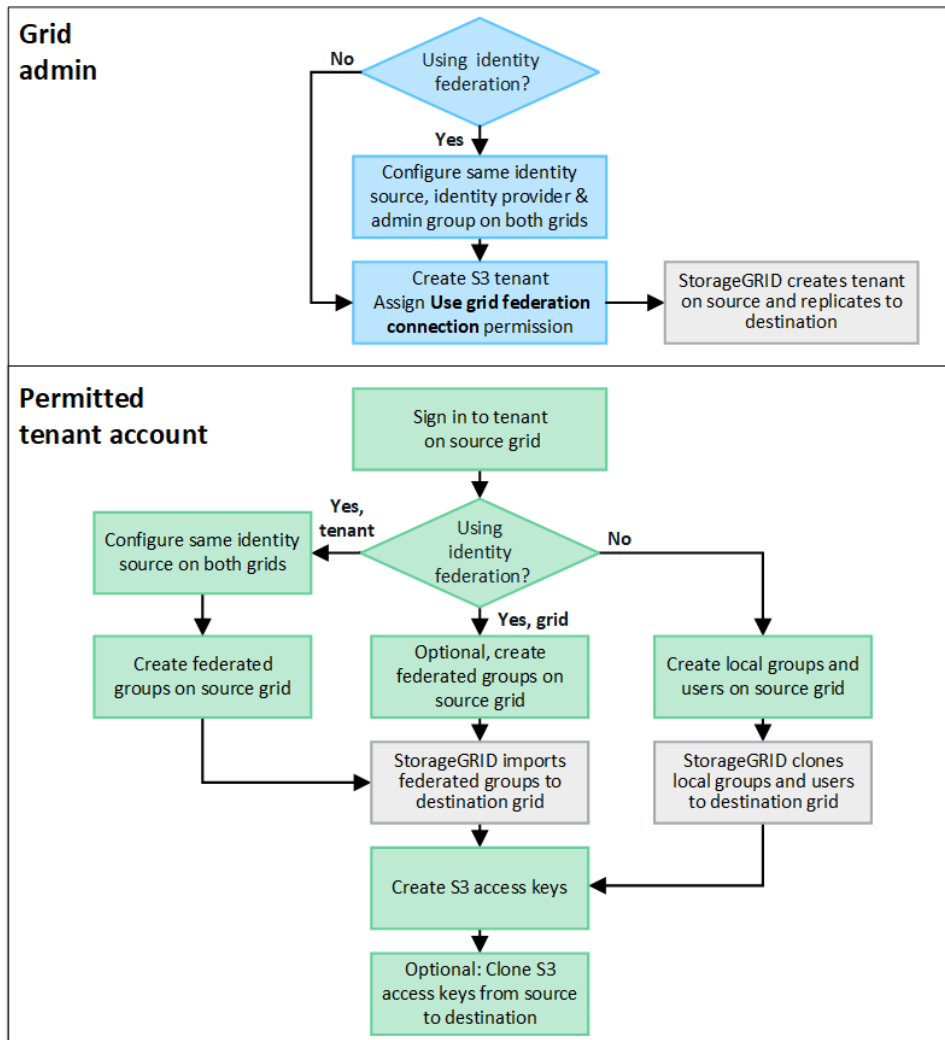
¿Qué es la clonación de cuenta?

La clonación de cuenta es la replicación automática de una cuenta de inquilino, grupos de inquilinos, usuarios de inquilinos y, opcionalmente, claves de acceso S3 entre los sistemas StorageGRID en un ["conexión de federación de red"](#).

Se requiere clonar la cuenta para ["replicación entre redes"](#). La clonación de información de cuentas desde un sistema StorageGRID de origen a un sistema StorageGRID de destino garantiza que los usuarios y grupos de inquilinos puedan acceder a los depósitos y objetos correspondientes en cualquiera de las redes.

Flujo de trabajo para clonar cuentas

El diagrama de flujo de trabajo muestra los pasos que los administradores de la red y los inquilinos permitidos realizarán para configurar la clonación de cuenta. Estos pasos se realizan después de la ["La conexión de la federación de red está configurada"](#).



Flujo de trabajo de administración de la red

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

Configurar SSO para clonar cuenta (opcional)

Si alguno de los sistemas StorageGRID en la conexión de federación de red usa SSO, ambas redes deben usar SSO. Antes de crear las cuentas de inquilino para la federación de red, los administradores de red para las redes de origen y destino del inquilino deben realizar estos pasos.

Pasos

1. Configure la misma fuente de identidad para ambas cuadrículas. Ver "[Utilizar la federación de identidades](#)".
2. Configure el mismo proveedor de identidad SSO (IdP) para ambas redes. Ver "[Configurar el inicio de sesión único](#)".
3. "[Crea el mismo grupo de administradores](#)" en ambas cuadrículas importando el mismo grupo federado.

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



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

Configurar la federación de identidad a nivel de cuadrícula para la clonación de cuentas (opcional)

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

Pasos

1. Configure la misma fuente de identidad para ambas cuadrículas. Ver "[Utilizar la federación de identidades](#)".
2. Opcionalmente, si un grupo federado tendrá permiso de acceso raíz inicial tanto para las cuentas de inquilino de origen como de destino, "[crear el mismo grupo de administradores](#)" en ambas cuadrículas importando el mismo grupo federado.



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

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

Crear una cuenta de inquilino S3 permitida

Después de configurar opcionalmente SSO o la federación de identidad, un administrador de red realiza estos pasos para determinar qué inquilinos pueden replicar objetos de depósito en otros sistemas StorageGRID.

Pasos

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

La cuadrícula donde se crea originalmente el inquilino se conoce como la *cuadrícula de origen* del inquilino. La cuadrícula donde se replica el inquilino se conoce como la *cuadrícula de destino* del inquilino.

2. En esa cuadrícula, cree una nueva cuenta de inquilino S3 o edite una cuenta existente.
3. Asignar el permiso **Usar conexión de federación de red**.
4. Si la cuenta del inquilino administrará sus propios usuarios federados, asigne el permiso **Usar fuente de identidad propia**.

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

5. Seleccione una conexión de federación de red específica.
6. Guardar el inquilino nuevo o modificado.

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

- Ambas cuentas de inquilino tienen el mismo ID de cuenta, nombre, cuota de almacenamiento y

permisos asignados.

- Si seleccionó un grupo federado para tener permiso de acceso raíz para el inquilino, ese grupo se clona en el inquilino de destino.
- Si seleccionó un usuario local para que tenga permiso de acceso raíz para el inquilino, ese usuario se clonará en el inquilino de destino. Sin embargo, la contraseña de ese usuario no se clona.

Para obtener más información, consulte ["Administrar inquilinos permitidos para la federación de red"](#) .

Flujo de trabajo de cuentas de inquilinos permitidos

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

Pasos

1. Sign in en la cuenta del inquilino en la cuadrícula de origen del inquilino.
2. Si está permitido, configure la federación de identidad en las cuentas de inquilino de origen y de destino.
3. Cree grupos y usuarios en el inquilino de origen.

Cuando se crean nuevos grupos o usuarios en el inquilino de origen, StorageGRID los clona automáticamente en el inquilino de destino, pero no se produce ninguna clonación desde el destino hasta el origen.

4. Crear claves de acceso S3.
5. Opcionalmente, clone las claves de acceso S3 del inquilino de origen al inquilino de destino.

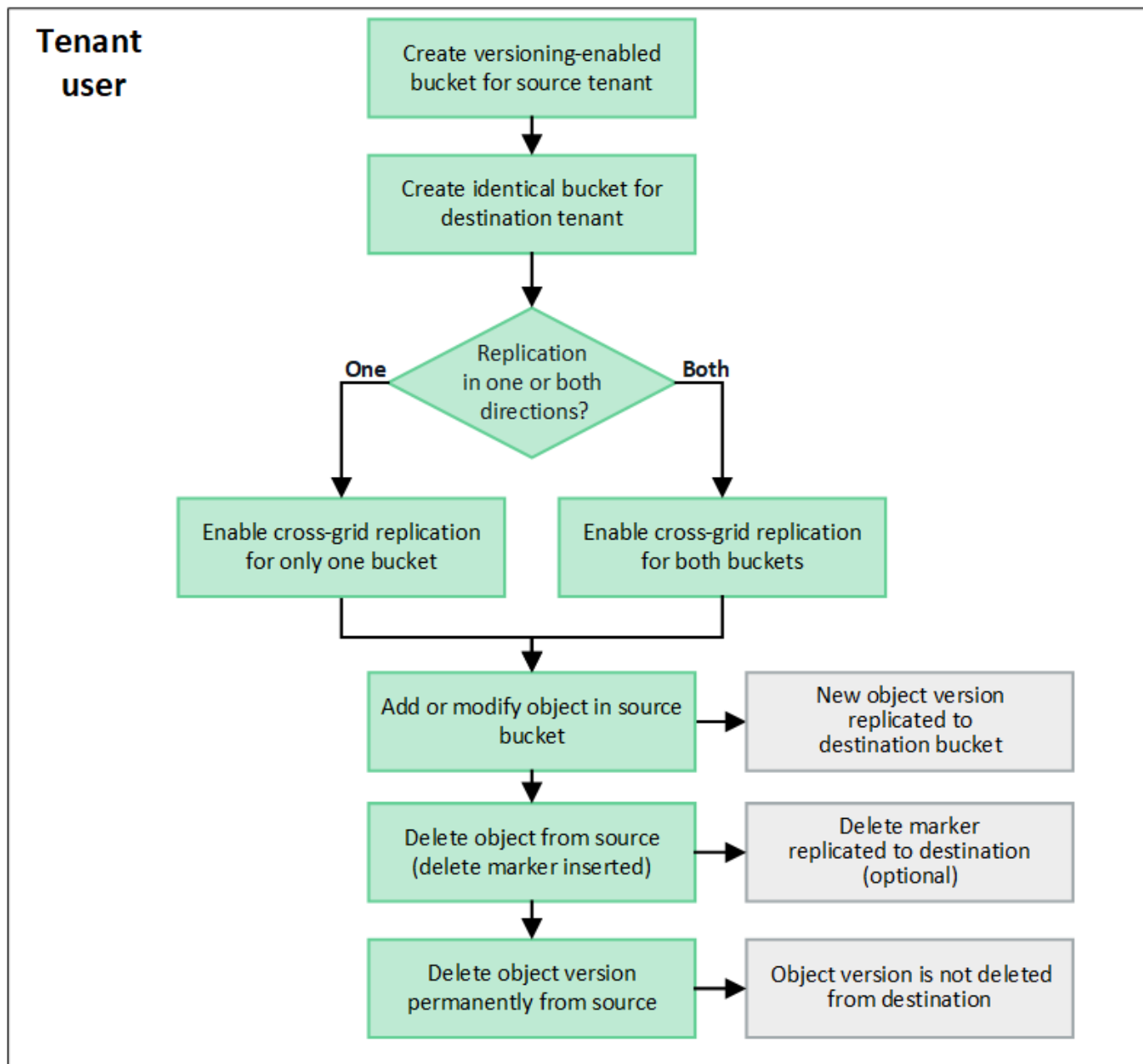
Para obtener detalles sobre el flujo de trabajo de la cuenta de inquilino permitida y para aprender cómo se clonan los grupos, los usuarios y las claves de acceso de S3, consulte ["Clonar grupos de inquilinos y usuarios"](#) y ["Clonar claves de acceso S3 usando la API"](#) .

¿Qué es la replicación entre redes?

La replicación entre redes es la replicación automática de objetos entre depósitos S3 seleccionados en dos sistemas StorageGRID que están conectados en una ["conexión de federación de red"](#) . ["Clon de cuenta"](#) es necesario para la replicación entre redes.

Flujo de trabajo para la replicación entre redes

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



Requisitos para la replicación entre redes

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

- Debe tener el mismo nombre pero puede tener diferentes regiones
- Debe tener habilitada la versión
- Debe tener el bloqueo de objetos S3 deshabilitado
- Debe estar vacío

Una vez creados ambos buckets, se puede configurar la replicación entre redes para uno o ambos buckets.

Más información

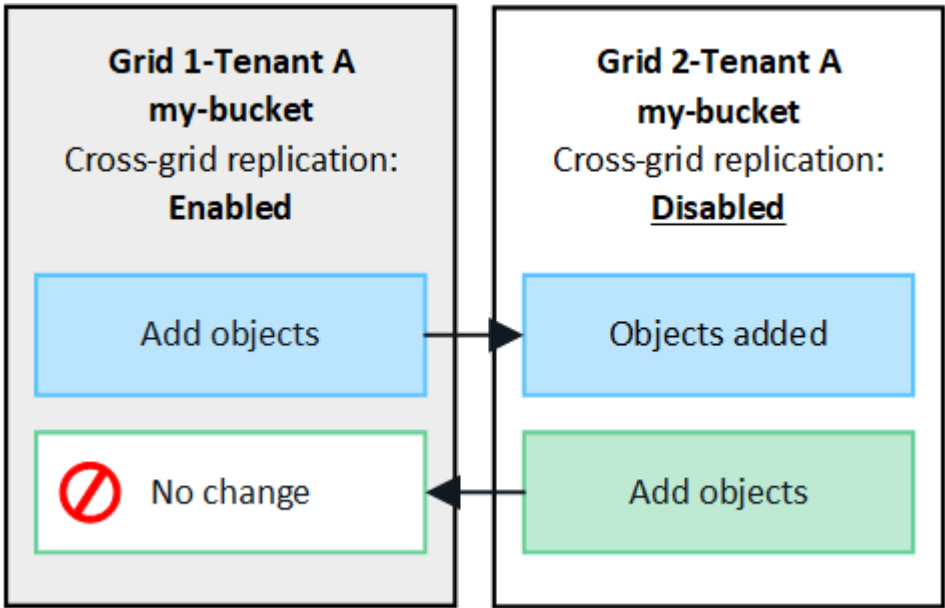
["Administrar la replicación entre redes"](#)

Cómo funciona la replicación entre redes

La replicación entre redes se puede configurar para que ocurra en una dirección o en ambas direcciones.

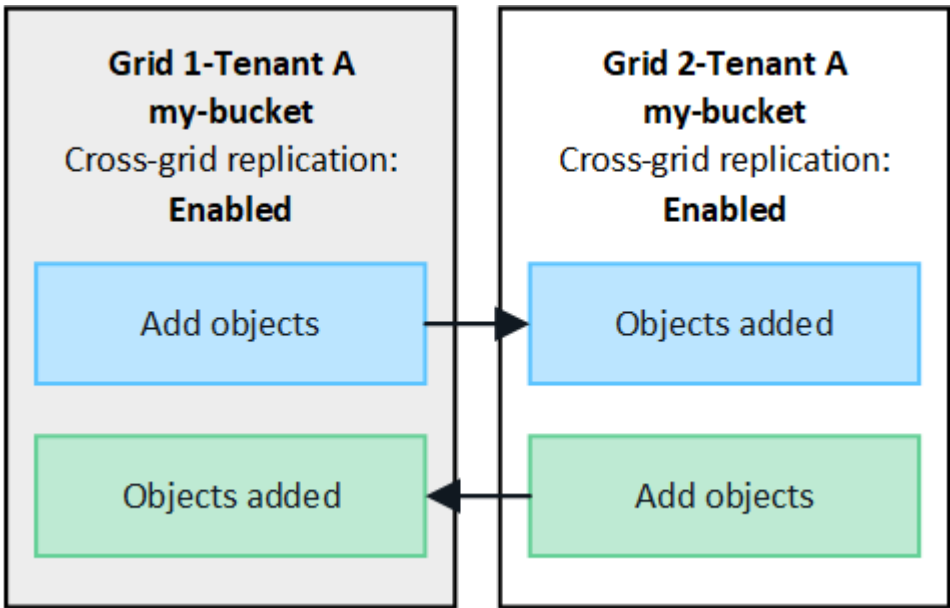
Replicación en una dirección

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



Replicación en ambas direcciones

Si habilita la replicación entre cuadrículas para el mismo depósito en ambas cuadrículas, los objetos agregados a cualquiera de los depósitos se replicarán en la otra cuadrícula. En la figura, la replicación entre redes está habilitada para my-bucket en ambas direcciones.



¿Qué sucede cuando se ingieren objetos?

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

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

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

Red	Estado de replicación
Fuente	• COMPLETADO: La replicación fue exitosa para todas las conexiones de red. • PENDIENTE: El objeto no se ha replicado a al menos una conexión de red. • FALLA: La replicación no está pendiente para ninguna conexión a la red y al menos una falló con una falla permanente. Un usuario debe resolver el error.
Destino	RÉPLICA: El objeto fue replicado desde la cuadrícula de origen.



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

2. StorageGRID utiliza las políticas ILM activas de cada red para administrar los objetos, tal como lo haría con cualquier otro objeto. Por ejemplo, el Objeto A en la Cuadrícula 1 podría almacenarse como dos copias replicadas y conservarse para siempre, mientras que la copia del Objeto A que se replicó en la Cuadrícula 2 podría almacenarse utilizando una codificación de borrado 2+1 y eliminarse después de tres años.

¿Qué sucede cuando se eliminan objetos?

Como se describe en ["Eliminar flujo de datos"](#) StorageGRID puede eliminar un objeto por cualquiera de estos motivos:

- El cliente S3 emite una solicitud de eliminación.
- Un usuario de administrador de inquilinos selecciona el ["Eliminar objetos en el depósito"](#) Opción para eliminar todos los objetos de un depósito.
- El bucket tiene una configuración de ciclo de vida que expira.
- Finaliza el último período de tiempo de la regla ILM para el objeto y no se especifican más ubicaciones.

Cuando StorageGRID elimina un objeto debido a una operación Eliminar objetos en el depósito, vencimiento del ciclo de vida del depósito o vencimiento de la ubicación de ILM, el objeto replicado nunca se elimina de la otra red en una conexión de federación de redes. Sin embargo, los marcadores de eliminación agregados al depósito de origen mediante eliminaciones del cliente S3 se pueden replicar opcionalmente en el depósito de

destino.

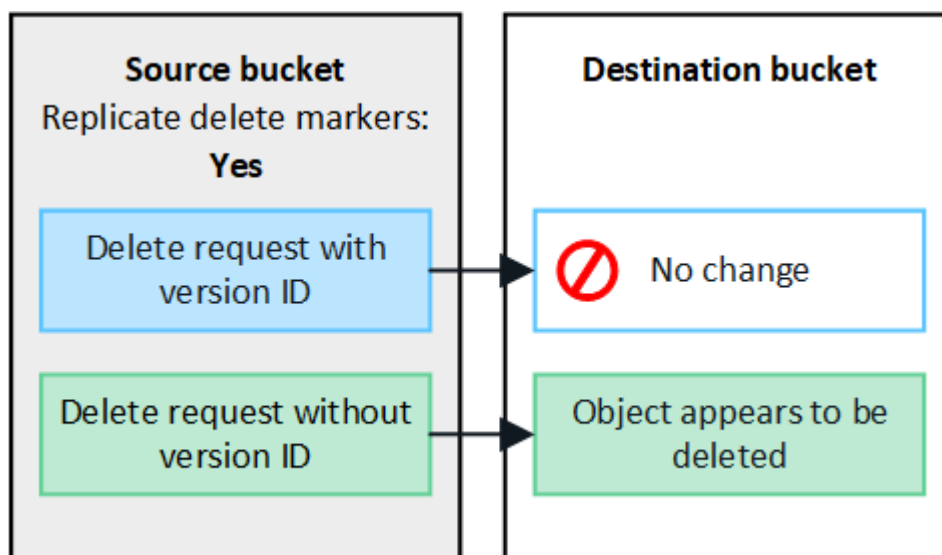
Para comprender qué sucede cuando un cliente S3 elimina objetos de un depósito que tiene habilitada la replicación entre cuadrículas, revise cómo los clientes S3 eliminan objetos de depósitos que tienen habilitada la gestión de versiones, de la siguiente manera:

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

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

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

En la figura, **Replicar marcadores de eliminación** se configuró en **Sí** cuando "[Se habilitó la replicación entre redes](#)". Las solicitudes de eliminación del depósito de origen que incluyen un ID de versión no eliminarán objetos del depósito de destino. Las solicitudes de eliminación del depósito de origen que no incluyen un ID de versión parecerán eliminar objetos en el depósito de destino.





Si desea mantener las eliminaciones de objetos sincronizadas entre cuadrículas, cree las correspondientes ["Configuraciones del ciclo de vida de S3"](#) para los cubos en ambas cuadrículas.

Cómo se replican los objetos cifrados

Cuando utiliza la replicación entre cuadrículas para replicar objetos entre cuadrículas, puede cifrar objetos individuales, usar el cifrado de depósito predeterminado o configurar el cifrado de toda la cuadrícula. Puede agregar, modificar o eliminar configuraciones de cifrado predeterminadas de toda la red o del bucket antes o después de habilitar la replicación entre redes para un bucket.

Para cifrar objetos individuales, puede utilizar SSE (cifrado del lado del servidor con claves administradas StorageGRID) al agregar los objetos al depósito de origen. Utilice el `x-amz-server-side-encryption` encabezado de solicitud y especifique AES256. Ver ["Utilice cifrado del lado del servidor"](#).



No se admite el uso de SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente) para la replicación entre redes. La operación de ingesta fallará.

Para utilizar el cifrado predeterminado para un depósito, utilice una solicitud `PutBucketEncryption` y configure el `SSEAlgorithm` parámetro a AES256. El cifrado a nivel de depósito se aplica a cualquier objeto ingerido sin la `x-amz-server-side-encryption` encabezado de solicitud. Ver ["Operaciones en buckets"](#).

Para utilizar el cifrado a nivel de cuadrícula, configure la opción **Cifrado de objetos almacenados en AES-256**. El cifrado a nivel de red se aplica a cualquier objeto que no esté cifrado a nivel de depósito o que se ingiera sin el `x-amz-server-side-encryption` encabezado de solicitud. Ver ["Configurar opciones de red y objetos"](#).



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

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

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

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

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

PutObjectTagging y DeleteObjectTagging no son compatibles

Las solicitudes PutObjectTagging y DeleteObjectTagging no se admiten para objetos en depósitos que tienen habilitada la replicación entre cuadrículas.

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

Cómo se replican los objetos segmentados

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

Comparar la replicación entre redes y la replicación de CloudMirror

A medida que comience a utilizar la federación de red, revise las similitudes y diferencias entre "[replicación entre redes](#)" y el "[Servicio de replicación StorageGRID CloudMirror](#)".

	Replicación entre redes	Servicio de replicación CloudMirror
¿Cuál es el propósito principal?	Un sistema StorageGRID actúa como un sistema de recuperación ante desastres. Los objetos de un bucket se pueden replicar entre las cuadrículas en una o ambas direcciones.	Permite que un inquilino replique automáticamente objetos desde un depósito en StorageGRID (origen) a un depósito S3 externo (destino). La replicación de CloudMirror crea una copia independiente de un objeto en una infraestructura S3 independiente. Esta copia independiente no se utiliza como copia de seguridad, sino que a menudo se procesa en la nube.
¿Cómo está configurado?	1. Configurar una conexión de federación de red entre dos redes. 2. Agregue nuevas cuentas de inquilinos, que se clonarán automáticamente en la otra red. 3. Agregue nuevos grupos de inquilinos y usuarios, que también se clonan. 4. Cree depósitos correspondientes en cada cuadrícula y habilite la replicación entre cuadrículas para que se produzca en una o ambas direcciones.	1. Un usuario inquilino configura la replicación de CloudMirror definiendo un punto final de CloudMirror (dirección IP, credenciales, etc.) mediante el Administrador de inquilinos o la API S3. 2. Cualquier depósito propiedad de esa cuenta de inquilino se puede configurar para apuntar al punto final de CloudMirror.

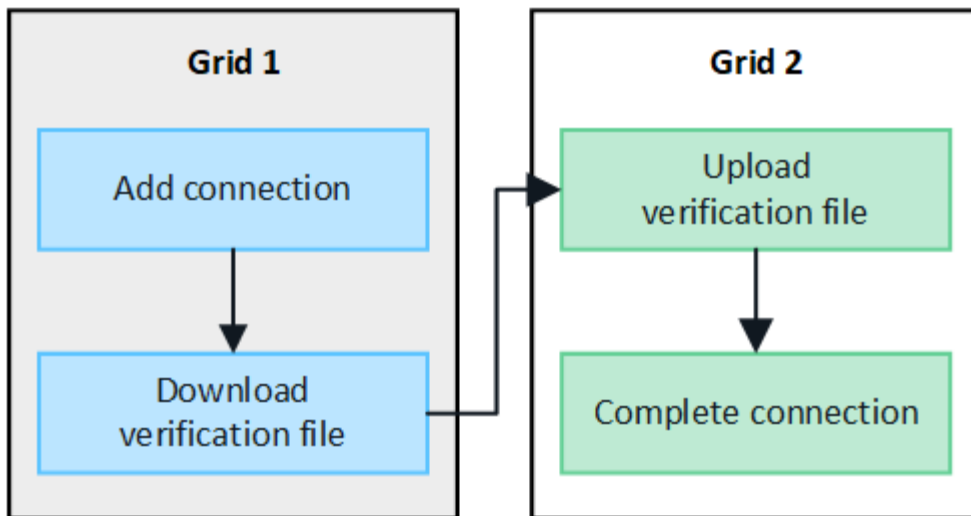
	Replicación entre redes	Servicio de replicación CloudMirror
¿Quién es responsable de configurarlo?	• Un administrador de red configura la conexión y los inquilinos. • Los usuarios inquilinos configuran los grupos, usuarios, claves y depósitos.	Normalmente, un usuario inquilino.
¿Cual es el destino?	Un bucket S3 correspondiente e idéntico en el otro sistema StorageGRID en la conexión de federación de red.	• Cualquier infraestructura S3 compatible (incluido Amazon S3). • Plataforma de Google Cloud (GCP)
¿Es necesario el control de versiones de objetos?	Sí, tanto los depósitos de origen como los de destino deben tener habilitada la versión de objetos.	No, la replicación de CloudMirror admite cualquier combinación de depósitos versionados y no versionados tanto en el origen como en el destino.
¿Qué hace que los objetos se muevan al destino?	Los objetos se replican automáticamente cuando se agregan a un depósito que tiene habilitada la replicación entre cuadrículas.	Los objetos se replican automáticamente cuando se agregan a un depósito que se ha configurado con un punto final de CloudMirror. Los objetos que existían en el depósito de origen antes de que este se configurara con el punto final de CloudMirror no se replican, a menos que se modifiquen.
¿Cómo se replican los objetos?	La replicación entre cuadrículas crea objetos versionados y replica el ID de la versión del depósito de origen al depósito de destino. Esto permite mantener el orden de las versiones en ambas cuadrículas.	La replicación de CloudMirror no requiere depósitos con control de versiones habilitado, por lo que CloudMirror solo puede mantener el orden de una clave dentro de un sitio. No hay garantías de que se mantenga el orden para las solicitudes de un objeto en un sitio diferente.
¿Qué pasa si un objeto no se puede replicar?	El objeto se pone en cola para su replicación, sujeto a los límites de almacenamiento de metadatos.	El objeto se pone en cola para la replicación, sujeto a los límites de los servicios de la plataforma (consulte "Recomendaciones para el uso de los servicios de la plataforma").
¿Se replican los metadatos del sistema del objeto?	Sí, cuando un objeto se replica en la otra red, sus metadatos del sistema también se replican. Los metadatos serán idénticos en ambas cuadrículas.	No, cuando un objeto se replica en el depósito externo, se actualizan sus metadatos del sistema. Los metadatos variarán según la ubicación, dependiendo del momento de la ingesta y del comportamiento de la infraestructura S3 independiente.

	Replicación entre redes	Servicio de replicación CloudMirror
¿Cómo se recuperan los objetos?	Las aplicaciones pueden recuperar o leer objetos realizando una solicitud al depósito en cualquiera de las cuadrículas.	Las aplicaciones pueden recuperar o leer objetos realizando una solicitud a StorageGRID o al destino S3. Por ejemplo, supongamos que utiliza la replicación de CloudMirror para reflejar objetos en una organización asociada. El socio puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario utilizar StorageGRID .
¿Qué pasa si se elimina un objeto?	- Las solicitudes de eliminación que incluyen un ID de versión nunca se replican en la cuadrícula de destino. - Las solicitudes de eliminación que no incluyen un ID de versión agregan un marcador de eliminación al depósito de origen, que opcionalmente se puede replicar en la cuadrícula de destino. - Si la replicación entre redes está configurada para una sola dirección, los objetos en el depósito de destino se pueden eliminar sin afectar el origen.	Los resultados variarán según el estado de la versión de los depósitos de origen y destino (que no necesitan ser los mismos): - Si ambos depósitos están versionados, una solicitud de eliminación agregará un marcador de eliminación en ambas ubicaciones. - Si solo está versionado el depósito de origen, una solicitud de eliminación agregará un marcador de eliminación al origen, pero no al destino. - Si ninguno de los buckets tiene versión, una solicitud de eliminación eliminará el objeto del origen pero no del destino. De manera similar, los objetos en el depósito de destino se pueden eliminar sin afectar el origen.

Crear conexiones de federación de red

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

Como se muestra en la figura, la creación de una conexión de federación de red incluye pasos en ambas redes. Añade la conexión en una cuadrícula y complétala en la otra cuadrícula. Puedes empezar desde cualquiera de las cuadrículas.



Antes de empezar

- Usted ha revisado el "[Consideraciones y requisitos](#)" para configurar conexiones de federación de red.
- Si planea utilizar nombres de dominio completos (FQDN) para cada cuadrícula en lugar de direcciones IP o VIP, sabe qué nombres usar y ha confirmado que el servidor DNS de cada cuadrícula tiene las entradas adecuadas.
- Está usando un "[navegador web compatible](#)".
- Tiene permiso de acceso de root y la contraseña de aprovisionamiento para ambas redes.

Agregar conexión

Realice estos pasos en cualquiera de los dos sistemas StorageGRID .

Pasos

1. Sign in en el Administrador de cuadrícula desde el nodo de administración principal en cualquiera de las cuadrículas.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione **Agregar conexión**.
4. Introduzca detalles para la conexión.

Campo	Descripción
Nombre de la conexión	Un nombre único para ayudarle a reconocer esta conexión, por ejemplo, "Cuadrícula 1-Cuadrícula 2".
FQDN o IP para esta cuadrícula	Uno de los siguientes: • El FQDN de la red en la que está conectado actualmente • Una dirección VIP de un grupo HA en esta red • Una dirección IP de un nodo de administración o de puerta de enlace en esta red. La IP puede estar en cualquier red a la que pueda acceder la red de destino.

Campo	Descripción
Puerto	El puerto que desea utilizar para esta conexión. Puede ingresar cualquier número de puerto no utilizado del 23000 al 23999. Ambas redes en esta conexión utilizarán el mismo puerto. Debe asegurarse de que ningún nodo de ninguna de las redes utilice este puerto para otras conexiones.
Días de validez del certificado para esta red	El número de días que desea que los certificados de seguridad para esta red en la conexión sean válidos. El valor predeterminado es 730 días (2 años), pero puede ingresar cualquier valor entre 1 y 762 días. StorageGRID genera automáticamente certificados de cliente y servidor para cada cuadrícula cuando guarda la conexión.
Frase de contraseña de aprovisionamiento para esta red	La contraseña de aprovisionamiento para la red en la que ha iniciado sesión.
FQDN o IP para la otra red	Uno de los siguientes: • El FQDN de la red a la que desea conectarse • Una dirección VIP de un grupo HA en la otra red • Una dirección IP de un nodo de administración o de puerta de enlace en la otra red. La IP puede estar en cualquier red a la que la red de origen pueda acceder.

5. Seleccione **Guardar y continuar**.

6. Para el paso Descargar archivo de verificación, seleccione **Descargar archivo de verificación**.

Una vez completada la conexión en la otra red, ya no podrás descargar el archivo de verificación de ninguna de las redes.

7. Localice el archivo descargado(*connection-name.grid-federation*) y guárdelo en un lugar seguro.



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

8. Seleccione **Cerrar** para regresar a la página de federación de Grid.

9. Confirme que se muestra la nueva conexión y que su **Estado de conexión** es **Esperando para conectar**.

10. Proporcionar el *connection-name.grid-federation* archivo al administrador de la red para la otra red.

Conexión completa

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

Pasos

1. Sign in en Grid Manager desde el nodo de administración principal.

2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione **Cargar archivo de verificación** para acceder a la página de carga.
4. Seleccione **Subir archivo de verificación**. Luego, busque y seleccione el archivo que se descargó de la primera cuadrícula.(*connection-name.grid-federation*).

Se muestran los detalles de la conexión.

5. Opcionalmente, ingrese un número diferente de días válidos para los certificados de seguridad de esta cuadrícula. La entrada **Días de validez del certificado** tiene como valor predeterminado el que ingresó en la primera cuadrícula, pero cada cuadrícula puede usar fechas de vencimiento diferentes.

En general, utilice la misma cantidad de días para los certificados en ambos lados de la conexión.



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

6. Ingrese la contraseña de aprovisionamiento para la red en la que está conectado actualmente.
7. Seleccione **Guardar y probar**.

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

Si aparece un mensaje de error, solucione cualquier problema. Ver "[Solucionar errores de federación de red](#)".

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

Si edita esta conexión, se creará un nuevo archivo de verificación. El archivo original no se puede reutilizar.

Después de terminar

- Revise las consideraciones para "[gestión de inquilinos permitidos](#)".
- "[Crear una o más cuentas de inquilino nuevas](#)", asigne el permiso **Usar conexión de federación de red** y seleccione la nueva conexión.
- "[Administrar la conexión](#)" según sea necesario. Puede editar valores de conexión, probar una conexión, rotar certificados de conexión o eliminar una conexión.
- "[Monitorizar la conexión](#)" como parte de sus actividades normales de monitoreo de StorageGRID.
- "[Solucionar problemas de conexión](#)", incluida la resolución de alertas y errores relacionados con la clonación de cuentas y la replicación entre redes.

Administrar conexiones de federación de red

La administración de las conexiones de federación de red entre sistemas StorageGRID incluye editar los detalles de conexión, rotar los certificados, eliminar los permisos de inquilinos y eliminar las conexiones no utilizadas.

Antes de empezar

- Ha iniciado sesión en el Administrador de cuadrícula en cualquiera de las cuadrículas mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#) para la red en la que ha iniciado sesión.

Editar una conexión de federación de red

Puede editar una conexión de federación de red iniciando sesión en el nodo de administración principal en cualquiera de las redes de la conexión. Después de realizar cambios en la primera cuadrícula, deberá descargar un nuevo archivo de verificación y cargarlo en la otra cuadrícula.



Mientras se edita la conexión, las solicitudes de clonación de cuenta o replicación entre redes continuarán usando las configuraciones de conexión existentes. Cualquier modificación que realice en la primera cuadrícula se guarda localmente, pero no se utiliza hasta que se haya cargado en la segunda cuadrícula, se haya guardado y se haya probado.

Comience a editar la conexión

Pasos

1. Sign in en el Administrador de cuadrícula desde el nodo de administración principal en cualquiera de las cuadrículas.
2. Seleccione **NODOS** y confirme que todos los demás nodos de administración en su sistema estén en línea.



Cuando edita una conexión de federación de red, StorageGRID intenta guardar un archivo de "configuración candidata" en todos los nodos de administración de la primera red. Si este archivo no se puede guardar en todos los nodos de administración, aparecerá un mensaje de advertencia cuando seleccione **Guardar y probar**.

3. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
4. Edite los detalles de la conexión utilizando el menú **Acciones** en la página de federación de Grid o la página de detalles de una conexión específica. Ver ["Crear conexiones de federación de red"](#) para qué entrar.

Menú de acciones

- a. Seleccione el botón de opción para la conexión.
- b. Seleccione **Acciones > Editar**.
- c. Introduzca la nueva información.

Página de detalles

- a. Seleccione un nombre de conexión para mostrar sus detalles.
- b. Seleccione **Editar**.
- c. Introduzca la nueva información.

5. Introduzca la contraseña de aprovisionamiento para la red en la que ha iniciado sesión.
6. Seleccione **Guardar y continuar**.

Los nuevos valores se guardan, pero no se aplicarán a la conexión hasta que haya cargado el nuevo archivo de verificación en la otra cuadrícula.

7. Seleccione **Descargar archivo de verificación**.

Para descargar este archivo más tarde, vaya a la página de detalles de la conexión.

8. Localice el archivo descargado(*connection-name.grid-federation*) y guárdelo en un lugar seguro.



El archivo de verificación contiene secretos y debe almacenarse y transmitirse de forma segura.

9. Seleccione **Cerrar** para regresar a la página de federación de Grid.

10. Confirme que el **Estado de conexión** sea **Pendiente de edición**.



Si el estado de la conexión era distinto de **Conectado** cuando comenzó a editar la conexión, no cambiará a **Pendiente de edición**.

11. Proporcionar el *connection-name.grid-federation* archivo al administrador de la red para la otra red.

Terminar de editar la conexión

Termine de editar la conexión cargando el archivo de verificación en la otra cuadrícula.

Pasos

1. Sign in en Grid Manager desde el nodo de administración principal.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione **Cargar archivo de verificación** para acceder a la página de carga.
4. Seleccione **Subir archivo de verificación**. Luego, busque y seleccione el archivo que se descargó de la primera cuadrícula.
5. Ingrese la contraseña de aprovisionamiento para la red en la que está conectado actualmente.
6. Seleccione **Guardar y probar**.

Si se puede establecer la conexión utilizando los valores editados, aparecerá un mensaje de éxito. De lo contrario, aparecerá un mensaje de error. Revise el mensaje y solucione cualquier problema.

7. Cierre el asistente para regresar a la página de federación de Grid.
8. Confirme que el **Estado de conexión** sea **Conectado**.
9. Vaya a la página de federación de Grid en la primera cuadrícula y actualice el navegador. Confirme que el **Estado de conexión** ahora es **Conectado**.
10. Una vez establecida la conexión, elimine de forma segura todas las copias del archivo de verificación.

Pruebe una conexión de federación de red

Pasos

1. Sign in en Grid Manager desde el nodo de administración principal.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.

3. Pruebe la conexión utilizando el menú **Acciones** en la página de federación de Grid o la página de detalles de una conexión específica.

Menú de acciones

- a. Seleccione el botón de opción para la conexión.
- b. Seleccione **Acciones > Prueba**.

Página de detalles

- a. Seleccione un nombre de conexión para mostrar sus detalles.
- b. Seleccione **Probar conexión**.

4. Revisar el estado de la conexión:

Estado de la conexión	Descripción
Conectado	Ambas redes están conectadas y se comunican normalmente.
Error	La conexión está en un estado de error. Por ejemplo, un certificado ha expirado o un valor de configuración ya no es válido.
Pendiente de edición	Ha editado la conexión en esta cuadrícula, pero la conexión aún utiliza la configuración existente. Para completar la edición, cargue el nuevo archivo de verificación en la otra cuadrícula.
Esperando para conectar	Ha configurado la conexión en esta red, pero la conexión no se ha completado en la otra red. Descargue el archivo de verificación de esta cuadrícula y cárguelo en la otra cuadrícula.
Desconocido	La conexión está en un estado desconocido, posiblemente debido a un problema de red o un nodo fuera de línea.

5. Si el estado de la conexión es **Error**, resuelva cualquier problema. Luego, seleccione **Probar conexión** nuevamente para confirmar que el problema se ha solucionado.

Rotar certificados de conexión

Cada conexión de federación de red utiliza cuatro certificados SSL generados automáticamente para proteger la conexión. Cuando los dos certificados de cada red se acercan a su fecha de vencimiento, la alerta **Vencimiento del certificado de federación de red** le recuerda que debe rotar los certificados.



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

Pasos

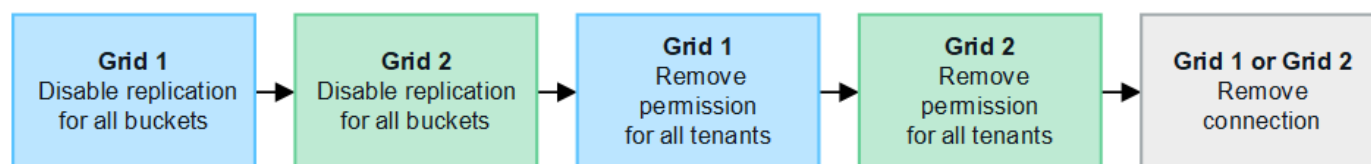
1. Sign in en el Administrador de cuadrícula desde el nodo de administración principal en cualquiera de las cuadrículas.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.

3. Desde cualquiera de las pestañas de la página de federación de Grid, seleccione el nombre de la conexión para mostrar sus detalles.
4. Seleccione la pestaña **Certificados**.
5. Seleccione **Rotar certificados**.
6. Especifique cuántos días deben ser válidos los nuevos certificados.
7. Introduzca la contraseña de aprovisionamiento para la red en la que ha iniciado sesión.
8. Seleccione **Rotar certificados**.
9. Según sea necesario, repita estos pasos en la otra cuadrícula de la conexión.

En general, utilice la misma cantidad de días para los certificados en ambos lados de la conexión.

Eliminar una conexión de federación de red

Puede eliminar una conexión de federación de red de cualquiera de las redes en la conexión. Como se muestra en la figura, debe realizar los pasos previos necesarios en ambas redes para confirmar que ningún inquilino en ninguna de las redes esté utilizando la conexión.



Antes de eliminar una conexión, tenga en cuenta lo siguiente:

- Eliminar una conexión no elimina ningún elemento que ya se haya copiado entre cuadrículas. Por ejemplo, los usuarios, grupos y objetos del inquilino que existen en ambas cuadrículas no se eliminan de ninguna de las cuadrículas cuando se elimina el permiso del inquilino. Si desea eliminar estos elementos, deberá eliminarlos manualmente de ambas cuadrículas.
- Cuando elimina una conexión, todos los objetos que estén pendientes de replicación (ingeridos pero aún no replicados en la otra red) tendrán una falla permanente en su replicación.

Deshabilitar la replicación para todos los depósitos de inquilinos

Pasos

1. Para comenzar desde cualquiera de las cuadrículas, inicie sesión en el Administrador de cuadrícula desde el nodo de administración principal.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione el nombre de la conexión para mostrar sus detalles.
4. En la pestaña **Inquilinos permitidos**, determine si algún inquilino está utilizando la conexión.
5. Si hay inquilinos en la lista, instruya a todos los inquilinos a "[Deshabilitar la replicación entre redes](#)" para todos sus cubos en ambas redes en la conexión.



No puedes eliminar el permiso **Usar conexión de federación de red** si alguno de los depósitos de inquilinos tiene habilitada la replicación entre redes. Cada cuenta de inquilino debe deshabilitar la replicación entre redes para sus depósitos en ambas redes.

Eliminar el permiso para cada inquilino

Una vez que se haya deshabilitado la replicación entre redes para todos los grupos de inquilinos, elimine el **permiso de uso de federación de red** de todos los inquilinos en ambas redes.

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
2. Seleccione el nombre de la conexión para mostrar sus detalles.
3. Para cada inquilino en la pestaña **Inquilinos permitidos**, elimine el permiso **Usar conexión de federación de red** de cada inquilino. Ver "[Gestionar inquilinos permitidos](#)".
4. Repita estos pasos para los inquilinos permitidos en la otra cuadrícula.

Eliminar conexión

Pasos

1. Cuando ningún inquilino en ninguna de las redes esté usando la conexión, seleccione **Eliminar**.
2. Revise el mensaje de confirmación y seleccione **Eliminar**.
 - Si se puede eliminar la conexión, se muestra un mensaje de éxito. La conexión de federación de red ahora se elimina de ambas redes.
 - Si no se puede eliminar la conexión (por ejemplo, todavía está en uso o hay un error de conexión), se muestra un mensaje de error. Puede realizar cualquiera de las siguientes acciones:
 - Resolver el error (recomendado). Ver "[Solucionar errores de federación de red](#)".
 - Retire la conexión a la fuerza. Vea la siguiente sección.

Eliminar una conexión de federación de red por la fuerza

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

La eliminación forzada solo elimina la conexión de la red local. Para eliminar completamente la conexión, realice los mismos pasos en ambas rejillas.

Pasos

1. Desde el cuadro de diálogo de confirmación, seleccione **Forzar eliminación**.

Aparece un mensaje de éxito. Esta conexión de federación de red ya no se puede utilizar. Sin embargo, es posible que los depósitos de inquilinos aún tengan habilitada la replicación entre redes y que algunas copias de objetos ya se hayan replicado entre las redes de la conexión.
2. Desde la otra cuadrícula en la conexión, inicie sesión en el Administrador de cuadrícula desde el nodo de administración principal.
3. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
4. Seleccione el nombre de la conexión para mostrar sus detalles.
5. Seleccione **Eliminar y Sí**.
6. Seleccione **Eliminar forzosamente** para eliminar la conexión de esta red.

Gestionar los inquilinos permitidos para la federación de red

Puede permitir que las cuentas de inquilinos de S3 utilicen una conexión de federación

de red entre dos sistemas StorageGRID . Cuando a los inquilinos se les permite usar una conexión, se requieren pasos especiales para editar los detalles del inquilino o eliminar de forma permanente el permiso de un inquilino para usar la conexión.

Antes de empezar

- Ha iniciado sesión en el Administrador de cuadrícula en cualquiera de las cuadrículas mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) para la red en la que ha iniciado sesión.
- Tienes ["creó una conexión de federación de red"](#) entre dos rejillas.
- Has revisado los flujos de trabajo para ["clon de cuenta"](#) y ["replicación entre redes"](#) .
- Según sea necesario, ya ha configurado el inicio de sesión único (SSO) o la federación de identidad para ambas redes en la conexión. Ver ["¿Qué es la clonación de cuenta?"](#) .

Crear un inquilino permitido

Si desea permitir que una cuenta de inquilino nueva o existente utilice una conexión de federación de red para la clonación de cuentas y la replicación entre redes, siga las instrucciones generales para ["crear un nuevo inquilino S3"](#) o ["editar una cuenta de inquilino"](#) y tenga en cuenta lo siguiente:

- Puede crear el inquilino desde cualquiera de las cuadrículas en 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 se crea o edita el inquilino para habilitar el permiso **Usar conexión de federación de red** y luego se guarda en la primera red, un inquilino idéntico se replica automáticamente en la otra red. La cuadrícula en la que se replica el inquilino es la cuadrícula de destino del inquilino.
- Los inquilinos de ambas redes tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos. Opcionalmente, puede utilizar el campo **Descripción** para ayudar a identificar cuál es el inquilino de origen y cuál es el inquilino de destino. Por ejemplo, esta descripción para un inquilino creado en la Red 1 también aparecerá para el inquilino replicado en la Red 2: "Este inquilino fue creado en la Red 1".
- Por razones de seguridad, la contraseña de un usuario root local no se copia a la red de destino.



Antes de que un usuario raíz local pueda iniciar sesión en el inquilino replicado en la red de destino, un administrador de red para esa red debe ["cambiar la contraseña del usuario root local"](#) .

- Una vez que el inquilino nuevo o editado esté disponible en ambas cuadrículas, los usuarios inquilinos pueden realizar estas operaciones:
 - Desde la red de origen del inquilino, cree grupos y usuarios locales, que se clonarán automáticamente en la red de destino del inquilino. Ver ["Clonar grupos de inquilinos y usuarios"](#) .
 - Cree nuevas claves de acceso S3, que pueden clonarse opcionalmente en la red de destino del inquilino. Ver ["Clonar claves de acceso S3 usando la API"](#) .
 - Cree depósitos idénticos en ambas cuadrículas de la conexión y habilite la replicación entre cuadrículas en una dirección o en ambas direcciones. Ver ["Administrar la replicación entre redes"](#) .

Ver un inquilino permitido

Puede ver los detalles de un inquilino que tiene permiso para utilizar una conexión de federación de red.

Pasos

1. Seleccione **INQUILINOS**.
2. Desde la página Inquilinos, seleccione el nombre del inquilino para ver la página de detalles del inquilino.

Si esta es la cuadrícula de origen del inquilino (es decir, si el inquilino se creó en esta cuadrícula), aparece un banner para recordarle que el inquilino se clonó en otra cuadrícula. Si edita o elimina este inquilino, sus cambios no se sincronizarán con la otra cuadrícula.

Tenants > tenant A for grid federation

tenant A for grid federation

Tenant ID: 0899 6970 1700 0930 0009

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Description: this tenant was created on Grid 1

Sign in

Edit

Actions ▾

This tenant has been cloned to another grid. If you edit or delete this tenant, your changes will not be synced to the other grid.

Space breakdown

Allowed features

Grid federation

Remove permission

Clear error

Search...

Displaying one result

Connection name	Connection status	Remote grid hostname	Last error
☐ Grid 1 to Grid 2	☒ Connected	10.96.106.230	Check for errors

3. Opcionalmente, seleccione la pestaña **Federación de red** para [supervisar la conexión de la federación de red](#).

Editar un inquilino permitido

Si necesita editar un inquilino que tiene el permiso **Usar conexión de federación de red**, siga las instrucciones generales para [editar una cuenta de inquilino](#) y tenga en cuenta lo siguiente:

- Si un inquilino tiene el permiso **Usar conexión de federación de red**, puede editar los detalles del inquilino desde cualquiera de las redes en la conexión. Sin embargo, cualquier cambio que realice no se copiará a la otra cuadrícula. Si desea mantener los detalles del inquilino sincronizados entre las cuadrículas, debe realizar las mismas ediciones en ambas cuadrículas.

- No puedes borrar el permiso **Usar conexión de federación de red** cuando estás editando un inquilino.
- No puedes seleccionar una conexión de federación de red diferente cuando estás editando un inquilino.

Eliminar un inquilino permitido

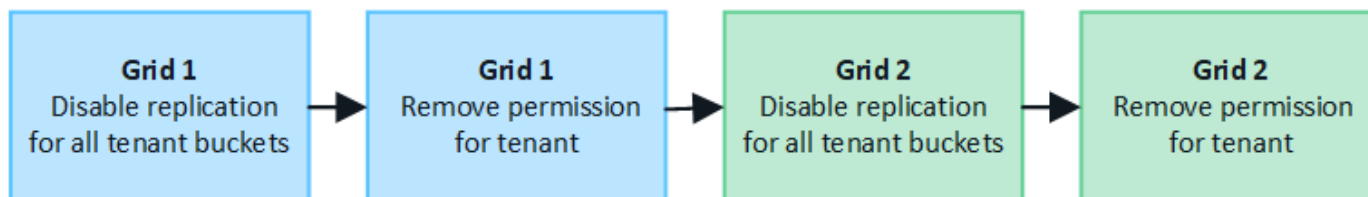
Si necesita eliminar un inquilino que tiene el permiso **Usar conexión de federación de red**, siga las instrucciones generales para ["eliminar una cuenta de inquilino"](#) y tenga en cuenta lo siguiente:

- Antes de poder eliminar al inquilino original en la red de origen, debe eliminar todos los depósitos de la cuenta en la red de origen.
- Antes de poder eliminar el inquilino clonado en la cuadrícula de destino, debe eliminar todos los depósitos de la cuenta en la cuadrícula de destino.
- Si elimina el inquilino original o el clonado, la cuenta ya no podrá usarse para la replicación entre redes.
- Si elimina el inquilino original de la red de origen, los grupos de inquilinos, usuarios o claves que se hayan clonado en la red de destino no se verán afectados. Puede eliminar el inquilino clonado o permitirle administrar sus propios grupos, usuarios, claves de acceso y depósitos.
- Si elimina el inquilino clonado en la cuadrícula de destino, se producirán errores de clonación si se agregan nuevos grupos o usuarios al inquilino original.

Para evitar estos errores, elimine el permiso del inquilino para usar la conexión de federación de red antes de eliminarlo de esta red.

Eliminar el permiso de conexión de federación de red

Para evitar que un inquilino utilice una conexión de federación de red, debe eliminar el permiso **Usar conexión de federación de red**.



Antes de quitarle el permiso a un inquilino para usar una conexión de federación de red, tenga en cuenta lo siguiente:

- No puedes eliminar el permiso **Usar conexión de federación de red** si alguno de los depósitos del inquilino tiene habilitada la replicación entre redes. Primero, la cuenta del inquilino debe deshabilitar la replicación entre redes para todos sus depósitos.
- Quitar el permiso **Usar conexión de federación de red** no elimina ningún elemento que ya se haya replicado entre redes. Por ejemplo, los usuarios, grupos y objetos de inquilinos que existen en ambas cuadrículas no se eliminan de ninguna de ellas cuando se elimina el permiso del inquilino. Si desea eliminar estos elementos, deberá eliminarlos manualmente de ambas cuadrículas.
- Si desea volver a habilitar este permiso con la misma conexión de federación de red, elimine primero este inquilino en la red de destino; de lo contrario, volver a habilitar este permiso generará un error.



Al volver a habilitar el permiso **Usar conexión de federación de red**, la red local se convierte en la red de origen y activa la clonación a la red remota especificada por la conexión de federación de red seleccionada. Si la cuenta del inquilino ya existe en la red remota, la clonación generará un error de conflicto.

Antes de empezar

- Estás usando un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) para ambas cuadrículas.

Deshabilitar la replicación para los depósitos de inquilinos

Como primer paso, deshabilite la replicación entre redes para todos los grupos de inquilinos.

Pasos

1. Para comenzar desde cualquiera de las cuadrículas, inicie sesión en el Administrador de cuadrícula desde el nodo de administración principal.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione el nombre de la conexión para mostrar sus detalles.
4. En la pestaña **Inquilinos permitidos**, determine si el inquilino está usando la conexión.
5. Si el inquilino está en la lista, indíquele que ["Deshabilitar la replicación entre redes"](#) para todos sus cubos en ambas redes en la conexión.



No puedes eliminar el permiso **Usar conexión de federación de red** si alguno de los depósitos de inquilinos tiene habilitada la replicación entre redes. El inquilino debe deshabilitar la replicación entre redes para sus depósitos en ambas redes.

Quitar el permiso al inquilino

Una vez deshabilitada la replicación entre redes para los depósitos de inquilinos, puede eliminar el permiso del inquilino para usar la conexión de federación de red.

Pasos

1. Sign in en Grid Manager desde el nodo de administración principal.
2. Eliminar el permiso de la página de federación de Grid o de la página de inquilinos.

Página de federación de red

- a. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
- b. Seleccione el nombre de la conexión para mostrar su página de detalles.
- c. En la pestaña **Inquilinos permitidos**, seleccione el botón de opción para el inquilino.
- d. Seleccione **Quitar permiso**.

Página de inquilinos

- a. Seleccione **INQUILINOS**.
- b. Seleccione el nombre del inquilino para mostrar la página de detalles.
- c. En la pestaña **Federación de red**, seleccione el botón de opción para la conexión.
- d. Seleccione **Quitar permiso**.

3. Revise las advertencias en el cuadro de diálogo de confirmación y seleccione **Eliminar**.
 - Si se puede eliminar el permiso, regresará a la página de detalles y se mostrará un mensaje de éxito.

Este inquilino ya no puede utilizar la conexión de federación de red.

- Si uno o más depósitos de inquilinos aún tienen habilitada la replicación entre redes, se muestra un error.

 **Remove permission to use grid federation connection** 

Are you sure you want to prevent **Tenant A** from performing account sync and cross-grid replication using grid federation connection **Grid 1-Grid 2**?

- Removing this permission does not delete any items that have already been copied to the other grid.
- After removing this permission for the tenant on this grid, go to the other grid and remove the permission for the corresponding tenant account.

 Connection '5427cbf8-0dd0-4b83-a2c8-e5e23cc49cc5' is used by bucket 'my-cgr-bucket' for cross-grid replication, so it can't be removed. From Tenant Manager, remove the cross-grid configuration from the tenant bucket and retry.

 Using **Force remove** removes the tenant's permission to use the grid federation connection even if tenant buckets still have cross-grid replication enabled. When the permission is removed, data in these buckets can no longer be copied between the grids.

Cancel

Force remove

Remove

Puede realizar cualquiera de las siguientes acciones:

- (Recomendado.) Sign in en el Administrador de inquilinos y deshabilite la replicación para cada uno de los grupos de inquilinos. Ver "[Administrar la replicación entre redes](#)". Luego, repita los pasos para eliminar el permiso **Usar conexión a la red**.
 - Quitar el permiso por la fuerza. Vea la siguiente sección.
4. Vaya a la otra cuadrícula y repita estos pasos para eliminar el permiso para el mismo inquilino en la otra cuadrícula.

Eliminar el permiso por la fuerza

Si es necesario, puede forzar la eliminación del permiso de un inquilino para usar una conexión de federación de red incluso si los depósitos de inquilinos tienen habilitada la replicación entre redes.

Antes de retirar por la fuerza el permiso de un inquilino, tenga en cuenta las consideraciones generales para [eliminando el permiso](#) así como estas consideraciones adicionales:

- Si elimina el permiso **Usar conexión de federación de red** por la fuerza, todos los objetos que estén pendientes de replicación en la otra red (ingeridos pero aún no replicados) continuarán replicándose. Para evitar que estos objetos en proceso lleguen al depósito de destino, también debe eliminar el permiso del inquilino en la otra cuadrícula.
- Cualquier objeto ingerido en el depósito de origen después de eliminar el permiso **Usar conexión de federación de red** nunca se replicará en el depósito de destino.

Pasos

1. Sign in en Grid Manager desde el nodo de administración principal.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione el nombre de la conexión para mostrar su página de detalles.
4. En la pestaña **Inquilinos permitidos**, seleccione el botón de opción para el inquilino.
5. Seleccione **Quitar permiso**.
6. Revise las advertencias en el cuadro de diálogo de confirmación y seleccione **Forzar eliminación**.

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

7. Según sea necesario, vaya a la otra cuadrícula y repita estos pasos para eliminar a la fuerza el permiso para la misma cuenta de inquilino en la otra cuadrícula. Por ejemplo, debe repetir estos pasos en la otra cuadrícula para evitar que los objetos en proceso lleguen al depósito de destino.

Solucionar errores de federación de red

Es posible que necesite solucionar alertas y errores relacionados con las conexiones de federación de red, la clonación de cuentas y la replicación entre redes.

Alertas y errores de conexión de la federación de red

Es posible que reciba alertas o experimente errores con sus conexiones de federación de red.

Después de realizar cualquier cambio para resolver un problema de conexión, pruebe la conexión para asegurarse de que el estado de la conexión vuelva a **Conectado**. Para obtener instrucciones, consulte ["Administrar conexiones de federación de red"](#).

Alerta de fallo de conexión de la federación de red

Asunto

Se activó la alerta **Error de conexión de federación de red**.

Detalles

Esta alerta indica que la conexión de federación de red entre las redes no está funcionando.

Acciones recomendadas

1. Revise la configuración en la página Federación de cuadrícula para ambas cuadrículas. Confirme que todos los valores sean correctos. Ver ["Administrar conexiones de federación de red"](#).
2. Revise los certificados utilizados para la conexión. Asegúrese de que no haya alertas de certificados de federación de red vencidos y que los detalles de cada certificado sean válidos. Consulte las instrucciones para rotar los certificados de conexión en ["Administrar conexiones de federación de red"](#).
3. Confirme que todos los nodos de administración y de puerta de enlace en ambas redes estén en línea y disponibles. Resuelva cualquier alerta que pueda estar afectando a estos nodos y vuelva a intentarlo.

4. Si proporcionó un nombre de dominio completo (FQDN) para la red local o remota, confirme que el servidor DNS esté en línea y disponible. Ver "[¿Qué es la federación de red?](#)" para requisitos de redes, direcciones IP y DNS.

Alerta de vencimiento del certificado de federación de red

Asunto

Se activó la alerta **Expiración del certificado de federación de red**.

Detalles

Esta alerta indica que uno o más certificados de federación de red están a punto de vencer.

Acciones recomendadas

Consulte las instrucciones para rotar los certificados de conexión en "[Administrar conexiones de federación de red](#)".

Error al editar una conexión de federación de red

Asunto

Al editar una conexión de federación de red, verá el siguiente mensaje de advertencia cuando seleccione **Guardar y probar**: "Error al crear un archivo de configuración candidato en uno o más nodos".

Detalles

Cuando edita una conexión de federación de red, StorageGRID intenta guardar un archivo de "configuración candidata" en todos los nodos de administración de la primera red. Aparece un mensaje de advertencia si este archivo no se puede guardar en todos los nodos de administración, por ejemplo, porque un nodo de administración está desconectado.

Acciones recomendadas

1. Desde la cuadrícula que está utilizando para editar la conexión, seleccione **NODOS**.
2. Confirme que todos los nodos de administración de esa red estén en línea.
3. Si algún nodo está fuera de línea, vuelva a conectarlo e intente editar la conexión nuevamente.

Errores de clonación de cuenta

No puedo iniciar sesión en una cuenta de inquilino clonada

Asunto

No puedes iniciar sesión en una cuenta de inquilino clonada. El mensaje de error en la página de inicio de sesión del Administrador de inquilinos es "Sus credenciales para esta cuenta no son válidas". Por favor, inténtelo de nuevo."

Detalles

Por razones de seguridad, cuando se clona una cuenta de inquilino desde la red de origen del inquilino a la red de destino del inquilino, la contraseña establecida para el usuario raíz local del inquilino no se clona. De manera similar, cuando un inquilino crea usuarios locales en su red de origen, las contraseñas de los usuarios locales no se clonan en la red de destino.

Acciones recomendadas

Antes de que el usuario raíz pueda iniciar sesión en la red de destino del inquilino, un administrador de la red debe primero "[cambiar la contraseña del usuario root local](#)" en la cuadrícula de destino.

Antes de que un usuario local clonado pueda iniciar sesión en la red de destino del inquilino, el usuario raíz del inquilino clonado debe agregar una contraseña para el usuario en la red de destino. Para obtener instrucciones, consulte "[Administrar usuarios locales](#)" en las instrucciones para utilizar el Administrador de inquilinos.

Inquilino creado sin un clon

Asunto

Verá el mensaje "Inquilino creado sin un clon" después de crear un nuevo inquilino con el permiso **Usar conexión de federación de red**.

Detalles

Este problema puede ocurrir si las actualizaciones del estado de la conexión se retrasan, lo que podría provocar que una conexión no saludable aparezca como **Conectada**.

Acciones recomendadas

1. Revise el motivo que aparece en el mensaje de error y resuelva cualquier problema de red o de otro tipo que pueda impedir que la conexión funcione. Ver [Alertas y errores de conexión de la federación de red](#).
2. Siga las instrucciones para probar una conexión de federación de red en "[Administrar conexiones de federación de red](#)" para confirmar que el problema se ha solucionado.
3. Desde la cuadrícula de origen del inquilino, seleccione **INQUILINOS**.
4. Localice la cuenta de inquilino que no se pudo clonar.
5. Seleccione el nombre del inquilino para mostrar la página de detalles.
6. Seleccione **Reintentar clonar cuenta**.

Tenants > test

test

Tenant ID: 0040 2213 8117 4859 6503

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Sign in

Edit

Actions ▾

✖

Tenant account could not be cloned to the other grid.

Reason: Internal server error. The server encountered an error and could not complete your request. Try again. If the problem persists, contact support. Internal Server Error

Retry account clone

Si se ha resuelto el error, la cuenta del inquilino ahora se clonará a la otra red.

Alertas y errores de replicación entre redes

Último error mostrado para la conexión o el inquilino

Asunto

Cuando "Visualización de una conexión de federación de red" (o cuando "gestión de los inquilinos permitidos" para una conexión), observa un error en la columna **Último error** en la página de detalles de la conexión. Por ejemplo:

Grid 1 - Grid 2

Local hostname (this grid):

10.96.130.64

Port:

23000

Remote hostname (other grid):

10.96.130.76

Connection status:

✓

Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Remove permission

Clear error

Search...

Displaying one result

Tenant name	Last error
Tenant A	2022-12-22 16:19:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-bucket' to destination bucket 'my-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 13916508109026943924) Check for errors

Detalles

Para cada conexión de federación de red, la columna **Último error** muestra el error más reciente que ocurrió, si lo hubo, cuando los datos de un inquilino se estaban replicando a la otra red. Esta columna solo muestra el último error de replicación entre redes que ocurrió; no se mostrarán los errores anteriores que pudieran haber ocurrido. Un error en esta columna podría ocurrir por una de estas razones:

- No se encontró la versión del objeto de origen.
- No se encontró el depósito de origen.
- Se eliminó el depósito de destino.
- El depósito de destino fue recreado por una cuenta diferente.
- El bucket de destino tiene la versión suspendida.
- El depósito de destino fue recreado por la misma cuenta pero ahora no tiene versión.

Acciones recomendadas

Si aparece un mensaje de error en la columna **Último error**, siga estos pasos:

1. Revise el texto del mensaje.
2. Realice cualquier acción recomendada. Por ejemplo, si se suspendió el control de versiones en el depósito de destino para la replicación entre redes, vuelva a habilitar el control de versiones para ese depósito.

3. Seleccione la conexión o la cuenta de inquilino de la tabla.
4. Seleccione **Borrar error**.
5. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espere 5-6 minutos y luego ingiera un nuevo objeto en el balde. Confirme que el mensaje de error no vuelva a aparecer.



Para garantizar que se borre el mensaje de error, espere al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingerir un nuevo objeto.



Después de eliminar el error, es posible que aparezca un nuevo **Último error** si los objetos se ingieren en un depósito diferente que también tiene un error.

7. Para determinar si algún objeto no se pudo replicar debido al error del depósito, consulte "[Identificar y reintentar operaciones de replicación fallidas](#)".

Alerta de fallo permanente de replicación entre redes

Asunto

Se activó la alerta **Error permanente de replicación entre redes**.

Detalles

Esta alerta indica que los objetos de inquilino no se pueden replicar entre los depósitos en dos cuadrículas por un motivo que requiere la intervención del usuario para resolverlo. Esta alerta generalmente es causada por un cambio en el depósito de origen o de destino.

Acciones recomendadas

1. Sign in en la red donde se activó la alerta.
2. Vaya a **CONFIGURACIÓN > Sistema > Federación de red** y localice el nombre de la conexión que aparece en la alerta.
3. En la pestaña Inquilinos permitidos, mire la columna **Último error** para determinar qué cuentas de inquilino tienen errores.
4. Para obtener más información sobre la falla, consulte las instrucciones en "[Supervisar las conexiones de la federación de red](#)" para revisar las métricas de replicación entre redes.
5. Para cada cuenta de inquilino afectada:
 - a. Vea las instrucciones en "[Supervisar la actividad de los inquilinos](#)" para confirmar que el inquilino no ha excedido su cuota en la red de destino para la replicación entre redes.
 - b. Según sea necesario, aumente la cuota del inquilino en la red de destino para permitir que se guarden nuevos objetos.
6. Para cada inquilino afectado, inicie sesión en Tenant Manager en ambas cuadrículas, para que pueda comparar la lista de grupos.
7. Para cada bucket que tenga habilitada la replicación entre redes, confirme lo siguiente:
 - Hay un depósito correspondiente para el mismo inquilino en la otra cuadrícula (debe usar el nombre exacto).
 - Ambos depósitos tienen habilitada la versión de objetos (la versión no se puede suspender en ninguna de las cuadrículas).
 - Ambos depósitos tienen el bloqueo de objetos S3 deshabilitado.

◦ Ninguno de los depósitos está en estado **Eliminando objetos: solo lectura**.

8. Para confirmar que el problema se resolvió, consulte las instrucciones en "[Supervisar las conexiones de la federación de red](#)" para revisar las métricas de replicación entre redes o realizar estos pasos:
 - a. Regresar a la página de federación de Grid.
 - b. Seleccione el inquilino afectado y seleccione **Borrar error** en la columna **Último error**.
 - c. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
 - d. Espere 5-6 minutos y luego ingiera un nuevo objeto en el balde. Confirme que el mensaje de error no vuelva a aparecer.



Para garantizar que se borre el mensaje de error, espere al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingerir un nuevo objeto.



La alerta podría tardar hasta un día en desaparecer después de resolverse.

- a. Ir a "[Identificar y reintentar operaciones de replicación fallidas](#)" para identificar cualquier objeto o eliminar marcadores que no se pudieron replicar en la otra cuadrícula y volver a intentar la replicación según sea necesario.

Alerta de recurso de replicación entre redes no disponible

Asunto

Se activó la alerta **Recurso de replicación entre redes no disponible**.

Detalles

Esta alerta indica que hay solicitudes de replicación entre redes pendientes porque un recurso no está disponible. Por ejemplo, podría haber un error de red.

Acciones recomendadas

1. Monitoree la alerta para ver si el problema se resuelve por sí solo.
2. Si el problema persiste, determine si alguna de las redes tiene una alerta de **Fallo de conexión de federación de red** para la misma conexión o una alerta de **No se puede comunicar con el nodo** para un nodo. Esta alerta podría resolverse cuando resuelvas esas alertas.
3. Para obtener más información sobre la falla, consulte las instrucciones en "[Supervisar las conexiones de la federación de red](#)" para revisar las métricas de replicación entre redes.
4. Si no puede resolver la alerta, comuníquese con el soporte técnico.

La replicación entre redes continuará de manera normal luego de que se resuelva el problema.

Identificar y reintentar operaciones de replicación fallidas

Después de resolver la alerta **Error permanente de replicación entre cuadrículas**, debe determinar si algún objeto o marcador de eliminación no se pudo replicar en la otra cuadrícula. Luego puede volver a ingerir estos objetos o utilizar la API de administración de cuadrícula para volver a intentar la replicación.

La alerta **Error permanente de replicación entre cuadrículas** indica que los objetos de inquilino no se pueden replicar entre los depósitos en dos cuadrículas por un motivo que requiere la intervención del usuario para resolverlo. Esta alerta generalmente es causada por un cambio en el depósito de origen o de destino.

Para obtener más información, consulte ["Solucionar errores de federación de red"](#) .

Determinar si algún objeto no se pudo replicar

Para determinar si algún objeto o marcador de eliminación no se ha replicado en la otra cuadrícula, puede buscar en el registro de auditoría ["CGRR \(Solicitud de replicación entre redes\)"](#) mensajes. Este mensaje se agrega al registro cuando StorageGRID no puede replicar un objeto, un objeto multiparte o un marcador de eliminación en el depósito de destino.

Puedes utilizar el ["herramienta de auditoría y explicación"](#) para traducir los resultados a un formato más fácil de leer.

Antes de empezar

- Tienes permiso de acceso root.
- Tú tienes el `Passwords.txt` archivo.
- Conoces la dirección IP del nodo de administración principal.

Pasos

1. Inicie sesión en el nodo de administración principal:
 - a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de \$ a # .

2. Busque mensajes CGRR en `audit.log` y utilice la herramienta `audit-explain` para dar formato a los resultados.

Por ejemplo, este comando busca 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 se verán como este ejemplo, que tiene entradas para seis mensajes CGRR. En el ejemplo, todas las solicitudes de replicación entre redes devolvieron un error general porque no se pudo replicar el objeto. Los primeros tres errores son para operaciones de "replicar objeto" y los últimos tres errores son para operaciones de "replicar marcador de eliminación".


```

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 redes CGRR	El nombre de la solicitud
arrendatario	ID de la cuenta del inquilino
conexión	El ID de la conexión de la federación de red
operación	El tipo de operación de replicación que se estaba intentando: • replicar objeto • replicar marcador de eliminación • replicar objeto multiparte
balde	El nombre del cubo
objeto	El nombre del objeto
versión	El ID de la versión del objeto

Campo	Descripción
error	El tipo de error. Si la replicación entre redes falla, el error es "Error general".

Reintentar replicaciones fallidas

Después de generar una lista de objetos y eliminar marcadores que no se replicaron en el depósito de destino y resolver los problemas subyacentes, puede volver a intentar la replicación de una de estas dos maneras:

- Reingerir cada objeto en el depósito de origen.
- Utilice la API privada de administración de cuadrícula, como se describe.

Pasos

1. Desde la parte superior del Administrador de cuadrícula, seleccione el ícono de ayuda y seleccione **Documentación de API**.
2. Seleccione **Ir a la documentación de API privada**.



Los puntos finales de la API de StorageGRID que están marcados como "Privados" están sujetos a cambios sin previo aviso. Los puntos finales privados de StorageGRID también ignoran la versión API de la solicitud.

3. En la sección **cross-grid-replication-advanced**, seleccione el siguiente punto final:

```
POST /private/cross-grid-replication-retry-failed
```

4. Seleccione **Probarlo**.
5. En el cuadro de texto **body**, reemplace la entrada de ejemplo para **versionID** con un ID de versión del audit.log que corresponde a una solicitud de replicación entre redes fallida.

Asegúrese de conservar las comillas dobles alrededor de la cadena.

6. Seleccione **Ejecutar**.
7. Confirme que el código de respuesta del servidor es **204**, lo que indica que el objeto o el marcador de eliminación se ha marcado como pendiente para la replicación entre cuadrículas a la otra cuadrícula.



Pendiente significa que la solicitud de replicación entre redes se ha agregado a la cola interna para su procesamiento.

Monitorear reintentos de replicación

Debe supervisar las operaciones de reintento de replicación para asegurarse de que se completen.



Podría tomar varias horas o más para que un objeto o un marcador de eliminación se replique en la otra cuadrícula.

Puede supervisar las operaciones de reintento de dos maneras:

- Utilice un S3 "[Objeto principal](#)" o "[Obtener objeto](#)" pedido. La respuesta incluye el StorageGRID específico

x-ntap-sg-cgr-replication-status encabezado de respuesta, que tendrá uno de los siguientes valores:

Red	Estado de replicación
Fuente	• COMPLETADO: La replicación fue exitosa. • PENDIENTE: El objeto aún no ha sido replicado. • FALLO: La replicación falló con un error permanente. Un usuario debe resolver el error.
Destino	RÉPLICA : El objeto fue replicado desde la cuadrícula de origen.

- Utilice la API privada de administración de cuadrícula, como se describe.

Pasos

1. En la sección **cross-grid-replication-advanced** de la documentación de la API privada, seleccione el siguiente punto final:

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Seleccione **Probarlo**.
3. En la sección Parámetro, ingrese el ID de la versión que utilizó en el `cross-grid-replication-retry-failed` pedido.
4. Seleccione **Ejecutar**.
5. Confirme que el código de respuesta del servidor es **200**.
6. Revise el estado de la replicación, que será uno de los siguientes:
 - **PENDIENTE**: El objeto aún no ha sido replicado.
 - **COMPLETADO**: La replicación fue exitosa.
 - **FALLÓ**: La replicación falló con un error permanente. Un usuario debe resolver el error.

Gestionar la seguridad

Gestionar la seguridad

Puede configurar varias configuraciones de seguridad desde Grid Manager para ayudar a proteger su sistema StorageGRID .

Administrar el cifrado

StorageGRID ofrece varias opciones para cifrar datos. Debería [revisar los métodos de cifrado disponibles](#) para determinar cuáles cumplen con sus requisitos de protección de datos.

Administrar certificados

Puede [configurar y administrar los certificados del servidor](#) Se utiliza para conexiones HTTP o los certificados de cliente utilizados para autenticar la identidad de un cliente o usuario en el servidor.

Configurar servidores de administración de claves

Usando un ["servidor de gestión de claves"](#) Le permite proteger los datos de StorageGRID incluso si se elimina un dispositivo del centro de datos. Una vez cifrados los volúmenes del dispositivo, no podrá acceder a ningún dato del dispositivo a menos que el nodo pueda comunicarse con el KMS.



Para utilizar la administración de claves de cifrado, debe habilitar la configuración **Cifrado de nodo** para cada dispositivo durante la instalación, antes de agregar el dispositivo a la red.

Administrar la configuración del proxy

Si está utilizando servicios de la plataforma S3 o grupos de almacenamiento en la nube, puede configurar un ["servidor proxy de almacenamiento"](#) entre los nodos de almacenamiento y los puntos finales externos de S3. Si envía paquetes de AutoSupport mediante HTTPS o HTTP, puede configurar un ["servidor proxy de administración"](#) entre los nodos de administración y el soporte técnico.

Controlar cortafuegos

Para mejorar la seguridad de su sistema, puede controlar el acceso a los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en el ["cortafuegos externo"](#). También puede controlar el acceso a la red de cada nodo configurando su ["cortafuegos interno"](#). Puede evitar el acceso a todos los puertos excepto aquellos necesarios para su implementación.

Revisar los métodos de cifrado de StorageGRID

StorageGRID ofrece varias opciones para cifrar datos. Debe revisar los métodos disponibles para determinar cuáles cumplen con sus requisitos de protección de datos.

La tabla proporciona un resumen de alto nivel de los métodos de cifrado disponibles en StorageGRID.

Opción de cifrado	Cómo funciona	Se aplica a
Servidor de administración de claves (KMS) en Grid Manager	Tú "configurar un servidor de administración de claves" para el sitio StorageGRID y "Habilitar el cifrado de nodos para el dispositivo" . Luego, un nodo del dispositivo se conecta al KMS para solicitar una clave de cifrado de clave (KEK). Esta clave cifra y descifra la clave de cifrado de datos (DEK) en cada volumen.	Nodos de dispositivo que tienen Cifrado de nodo habilitado durante la instalación. Todos los datos del dispositivo están protegidos contra pérdida física o eliminación del centro de datos. Nota: La administración de claves de cifrado con un KMS solo es compatible con nodos de almacenamiento y dispositivos de servicios.

Opción de cifrado	Cómo funciona	Se aplica a
Página de cifrado de unidad en el instalador del dispositivo StorageGRID	Si el dispositivo contiene unidades que admiten cifrado de hardware, puede establecer una frase de contraseña para la unidad durante la instalación. Cuando se establece una frase de contraseña de unidad, es imposible que alguien recupere datos válidos de unidades que se han eliminado del sistema, a menos que conozca la frase de contraseña. Antes de comenzar la instalación, vaya a Configurar hardware > Cifrado de unidad para establecer una frase de contraseña de unidad que se aplique a todas las unidades con cifrado automático administradas por StorageGRID en un nodo.	Dispositivos que contienen unidades con cifrado automático. Todos los datos de las unidades seguras están protegidos contra pérdida física o eliminación del centro de datos. El cifrado de unidad no se aplica a las unidades administradas SANtricity. Si tiene un dispositivo de almacenamiento con unidades de autocifrado y controladores SANtricity , puede habilitar la seguridad de la unidad en SANtricity.
Impulse la seguridad en SANtricity System Manager	Si la función Seguridad de la unidad está habilitada para su dispositivo StorageGRID , puede 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.	Dispositivos de almacenamiento que tienen unidades de cifrado de disco completo (FDE) o unidades de cifrado automático. Todos los datos de las unidades seguras están protegidos contra pérdida física o eliminación del centro de datos. No se puede utilizar con algunos dispositivos de almacenamiento ni con ningún dispositivo de servicio.
Cifrado de objetos almacenados	Habilitas el " Cifrado de objetos almacenados " opción en el Administrador de cuadrícula. Cuando esta opción está habilitada, todos los objetos nuevos que no estén cifrados en el nivel de depósito o en el nivel de objeto se cifran durante la ingesta.	Datos de objetos S3 recién ingeridos. Los objetos almacenados existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados.

Opción de cifrado	Cómo funciona	Se aplica a
Cifrado de buckets S3	Emite una solicitud PutBucketEncryption para habilitar el cifrado para el depósito. Cualquier objeto nuevo que no esté cifrado a nivel de objeto se cifra durante la ingesta.	Solo datos de objetos S3 recién ingeridos. Se debe especificar el cifrado para el depósito. Los objetos de bucket existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados. "Operaciones en buckets"
Cifrado del lado del servidor de objetos S3 (SSE)	Emite una solicitud S3 para almacenar un objeto e incluirlo x-amz-server-side-encryption encabezado de solicitud.	Solo datos de objetos S3 recién ingeridos. Se debe especificar el cifrado para el objeto. Los metadatos de los objetos y otros datos confidenciales no están cifrados. StorageGRID administra las claves. "Utilice cifrado del lado del servidor"
Cifrado del lado del servidor de objetos S3 con claves proporcionadas por el cliente (SSE-C)	Emite una solicitud S3 para almacenar un objeto e incluye 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 de los objetos y otros datos confidenciales no están cifrados. Las claves se administran fuera de StorageGRID. "Utilice cifrado del lado del servidor"

Opción de cifrado	Cómo funciona	Se aplica a
Cifrado de volumen externo o almacén de datos	Utilice un método de cifrado externo a StorageGRID para cifrar un volumen o almacén de datos completo, si su plataforma de implementación lo admite.	Todos los datos de objetos, metadatos y datos de configuración del sistema, asumiendo que cada volumen o almacén de datos está cifrado. Un método de cifrado externo proporciona un control más estricto sobre los algoritmos y claves de cifrado. Se puede combinar con los otros métodos enumerados.
Cifrado de objetos fuera de StorageGRID	Utilice un método de cifrado externo a StorageGRID para cifrar datos y metadatos de objetos antes de que se ingieran en StorageGRID.	Solo datos de objeto y metadatos (los datos de configuración del sistema no están cifrados). Un método de cifrado externo proporciona un control más estricto sobre los algoritmos y claves de cifrado. Se puede combinar con los otros métodos enumerados. "Amazon Simple Storage Service - Guía del usuario: Protección de datos mediante cifrado del lado del cliente"

Utilice múltiples métodos de cifrado

Dependiendo de sus requisitos, puede utilizar más de un método de cifrado a la vez. Por ejemplo:

- Puede utilizar un KMS para proteger los nodos del dispositivo y también usar la función de seguridad de la unidad en SANtricity System Manager para "cifrar doblemente" los datos en las unidades con cifrado automático en los mismos dispositivos.
- Puede utilizar un KMS para proteger datos en los nodos del dispositivo y también utilizar la opción de cifrado de objetos almacenados para cifrar todos los objetos cuando se ingieren.

Si solo una pequeña parte de sus objetos requieren cifrado, considere controlar el cifrado a nivel de depósito o de objeto individual. Habilitar múltiples niveles de cifrado tiene un costo de rendimiento adicional.

Administrar certificados

Administrar certificados de seguridad

Los certificados de seguridad son pequeños archivos de datos que se utilizan para crear conexiones seguras y confiables entre los componentes de StorageGRID y entre los componentes de StorageGRID y sistemas externos.

StorageGRID utiliza dos tipos de certificados de seguridad:

- Se requieren **certificados de servidor** cuando se utilizan conexiones HTTPS. Los certificados de servidor se utilizan para establecer conexiones seguras entre clientes y servidores, autenticando la identidad de un servidor ante sus clientes y proporcionando una ruta de comunicación segura para los datos. Tanto el servidor como el cliente tienen una copia del certificado.
- Los **certificados de cliente** autentican la identidad de un cliente o usuario en el servidor, proporcionando una autenticación más segura que las contraseñas 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 verifica este certificado comparando la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión con el servidor utilizando la misma clave pública.

StorageGRID funciona como servidor para algunas conexiones (como el punto final del equilibrador de carga) o como cliente para otras conexiones (como el servicio de replicación CloudMirror).

Certificado CA de Grid predeterminado

StorageGRID incluye una autoridad de certificación (CA) incorporada que genera un certificado CA de Grid interno durante la instalación del sistema. El certificado CA de Grid se utiliza, de forma predeterminada, para proteger el tráfico interno de StorageGRID. Una autoridad de certificación (CA) externa puede emitir certificados personalizados que cumplan totalmente con las políticas de seguridad de la información de su organización. Si bien puede utilizar el certificado CA de Grid para un entorno que no sea de producción, la mejor práctica para un entorno de producción es utilizar certificados personalizados firmados por una autoridad de certificación externa. También se admiten 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 del servidor.
- Todos los certificados personalizados deben cumplir con los ["Pautas de fortalecimiento del sistema para certificados de servidor"](#).
- StorageGRID admite la agrupación de certificados de una CA en un solo archivo (conocido como paquete de certificados de CA).



StorageGRID también incluye certificados CA del sistema operativo que son los mismos en todas las redes. En entornos de producción, asegúrese de especificar un certificado personalizado firmado por una autoridad de certificación externa en lugar del certificado CA del sistema operativo.

Las variantes de los tipos de certificado de servidor y cliente se implementan de varias maneras. Debe tener todos los certificados necesarios para su configuración específica de StorageGRID listos antes de configurar el sistema.

Certificados de seguridad de acceso

Puede acceder a información sobre todos los certificados StorageGRID en una sola ubicación, junto con enlaces al flujo de trabajo de configuración para cada certificado.

Pasos

1. Desde Grid Manager, seleccione **CONFIGURACIÓN > Seguridad > Certificados**.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global

Grid CA

Client

Load balancer endpoints

Tenants

Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type 	Expiration date  
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Seleccione una pestaña en la página Certificados para obtener información sobre cada categoría de certificado y acceder a la configuración del certificado. Puedes acceder a una pestaña si tienes la "[permiso apropiado](#)".

- **Global:** protege el acceso a StorageGRID desde navegadores web y clientes API externos.
- **Grid CA:** protege el tráfico interno de StorageGRID .
- **Cliente:** protege las conexiones entre clientes externos y la base de datos StorageGRID Prometheus.
- **Puntos finales del balanceador de carga:** protege las conexiones entre los clientes S3 y el balanceador de carga StorageGRID .
- **Inquilinos:** protege las conexiones a servidores de federación de identidad o desde puntos finales de servicio de la plataforma a recursos de almacenamiento S3.
- **Otro:** Protege las conexiones StorageGRID que requieren certificados específicos.

A continuación se describe cada pestaña con enlaces a detalles adicionales del certificado.

Global

Los certificados globales protegen el acceso a StorageGRID desde navegadores web y clientes API S3 externos. La autoridad de certificación StorageGRID genera inicialmente dos certificados globales durante la instalación. La mejor práctica para un entorno de producción es utilizar certificados personalizados firmados por una autoridad de certificación externa.

- [Certificado de interfaz de gestión](#): Asegura las conexiones del navegador web del cliente a las interfaces de administración de StorageGRID .
- [Certificado API S3](#): Asegura las conexiones de API de cliente a los nodos de almacenamiento, nodos de administración y nodos de puerta de enlace, que las aplicaciones de cliente S3 utilizan para cargar y descargar datos de objetos.

La información sobre los certificados globales que están instalados incluye:

- **Nombre**: Nombre del certificado con enlace para administrar el certificado.
- **Descripción**
- **Tipo**: Personalizado o predeterminado. + Siempre debe utilizar un certificado personalizado para mejorar la seguridad de la red.
- **Fecha de vencimiento**: si se utiliza el certificado predeterminado, no se muestra ninguna fecha de vencimiento.

Puede:

- Reemplace los certificados predeterminados con certificados personalizados firmados por una autoridad de certificación externa para mejorar la seguridad de la red:
 - ["Reemplazar el certificado de interfaz de administración generado por StorageGRID predeterminado"](#) Se utiliza para conexiones de Grid Manager y Tenant Manager.
 - ["Reemplazar el certificado de API S3"](#) Se utiliza para conexiones de nodo de almacenamiento y punto final del equilibrador de carga (opcional).
- ["Restaurar el certificado de interfaz de administración predeterminado"](#) .
- ["Restaurar el certificado API S3 predeterminado"](#) .
- ["Utilice un script para generar un nuevo certificado de interfaz de administración autofirmado"](#) .
- Copiar o descargar el ["certificado de interfaz de gestión"](#) o ["Certificado API S3"](#) .

Red CA

El [Certificado de CA de Grid](#) , generado por la autoridad de certificación de StorageGRID durante la instalación de StorageGRID , protege todo el tráfico interno de StorageGRID .

La información del certificado incluye la fecha de vencimiento del certificado y el contenido del certificado.

Puede [copiar o descargar el certificado de Grid CA](#) , pero no puedes cambiarlo.

Cliente

[Certificados de cliente](#), generado por una autoridad de certificación externa, protege las conexiones entre las herramientas de monitoreo externas y la base de datos StorageGRID Prometheus.

La tabla de certificados tiene una fila para cada certificado de cliente configurado e indica si el certificado se puede usar para acceder a la base de datos de Prometheus, junto con la fecha de

vencimiento del certificado.

Puede:

- ["Cargar o generar un nuevo certificado de cliente."](#)
- Seleccione un nombre de certificado para mostrar los detalles del certificado donde podrá:
 - ["Cambiar el nombre del certificado del cliente."](#)
 - ["Establecer el permiso de acceso de Prometheus."](#)
 - ["Cargar y reemplazar el certificado del cliente."](#)
 - ["Copie o descargue el certificado del cliente."](#)
 - ["Eliminar el certificado del cliente."](#)
- Seleccione **Acciones** para acceder rápidamente ["editar"](#) , ["adjuntar"](#) , o ["eliminar"](#) un certificado de cliente. Puede seleccionar hasta 10 certificados de cliente y eliminarlos a la vez usando **Acciones > Eliminar**.

Puntos finales del balanceador de carga

[Certificados de punto final del balanceador de carga](#) Asegure las conexiones entre los clientes S3 y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace y los nodos de administración.

La tabla de puntos finales del equilibrador de carga tiene una fila para cada punto final del equilibrador de carga configurado e indica si se utiliza el certificado de API S3 global o un certificado de punto final del equilibrador de carga personalizado para el punto final. También se muestra la fecha de vencimiento de cada certificado.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Puede:

- ["Ver un punto final del balanceador de carga"](#), incluidos los detalles de su certificado.
- ["Especifique un certificado de punto final del equilibrador de carga para FabricPool."](#)
- ["Utilice el certificado API global de S3"](#) en lugar de generar un nuevo certificado de punto final del equilibrador de carga.

Inquilinos

Los inquilinos pueden utilizar [certificados de servidor de federación de identidad](#) o [certificados de punto final del servicio de plataforma](#) para proteger 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 servicios de plataforma.

Puede:

- ["Seleccione un nombre de inquilino para iniciar sesión en el Administrador de inquilinos"](#)
- ["Seleccione un nombre de inquilino para ver los detalles de la federación de identidad del inquilino"](#)
- ["Seleccione el nombre de un inquilino para ver los detalles de los servicios de la plataforma de inquilinos"](#)

- "Especifique un certificado de punto final del servicio de plataforma durante la creación del punto final"

Otro

StorageGRID utiliza otros certificados de seguridad para fines específicos. Estos certificados se enumeran por su nombre funcional. Otros certificados de seguridad incluyen:

- [Certificados de grupo de almacenamiento en la nube](#)
- [Certificados de notificación de alertas por correo electrónico](#)
- [Certificados de servidor syslog externo](#)
- [Certificados de conexión de la federación de red](#)
- [Certificados de federación de identidad](#)
- [Certificados de servidor de administración de claves \(KMS\)](#)
- [Certificados de inicio de sesión único](#)

La información indica el tipo de certificado que utiliza una función y las fechas de vencimiento de sus certificados de servidor y cliente, según corresponda. Al seleccionar un nombre de función, se abre una pestaña del navegador donde puede ver y editar los detalles del certificado.



Solo puede ver y acceder a la información de otros certificados si tiene la ["permiso apropiado"](#).

Puede:

- ["Especifique un certificado de grupo de almacenamiento en la nube para S3, C2S S3 o Azure"](#)
- ["Especificar un certificado para notificaciones de alerta por correo electrónico"](#)
- ["Utilice un certificado para un servidor syslog externo"](#)
- ["Rotar certificados de conexión de federación de red"](#)
- ["Ver y editar un certificado de federación de identidad"](#)
- ["Cargar certificados de cliente y servidor del servidor de administración de claves \(KMS\)"](#)
- ["Especificar manualmente un certificado SSO para una relación de confianza de usuario autenticado"](#)

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 del cliente y la interfaz de administración de StorageGRID , lo que permite a los usuarios acceder a Grid Manager y Tenant Manager sin advertencias de seguridad. Este certificado también autentica las conexiones de la API de administración de red y la API de administración de inquilinos. Puede utilizar el certificado predeterminado creado durante la instalación o cargar un certificado personalizado.	CONFIGURACIÓN > Seguridad > Certificados , seleccione la pestaña Global y luego seleccione Certificado de interfaz de administración	"Configurar certificados de interfaz de administración"

Certificado API S3

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica conexiones seguras de cliente S3 a un nodo de almacenamiento y a puntos finales del balanceador de carga (opcional).	CONFIGURACIÓN > Seguridad > Certificados , seleccione la pestaña Global y luego seleccione Certificado API S3	"Configurar certificados de API S3"

Certificado de CA de Grid

Ver el [Descripción del certificado de CA de Grid predeterminado](#) .

Certificado de cliente administrador

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Cliente	Se instala en cada cliente, lo que permite que StorageGRID autentique el acceso de clientes externos. • Permite que los clientes externos autorizados accedan a la base de datos StorageGRID Prometheus. • Permite la monitorización segura de StorageGRID mediante herramientas externas.	CONFIGURACIÓN > Seguridad > Certificados y luego seleccione la pestaña Cliente	"Configurar certificados de cliente"

Certificado de punto final del balanceador de carga

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los clientes S3 y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace y los nodos de administración. Puede cargar o generar un certificado de equilibrador de carga cuando configura un punto final de equilibrador de carga. Las aplicaciones cliente utilizan el certificado del equilibrador de carga cuando se conectan a StorageGRID para guardar y recuperar datos de objetos. También puedes utilizar una versión personalizada del global Certificado API S3 Certificado para autenticar conexiones al servicio Load Balancer. Si el certificado global se utiliza para autenticar las conexiones del balanceador de carga, no es necesario cargar ni generar un certificado separado para cada punto final del balanceador de carga. Nota: El certificado utilizado para la autenticación del equilibrador de carga es el certificado más usado durante el funcionamiento normal de StorageGRID .	CONFIGURACIÓN > Red > Puntos finales del balanceador de carga	• "Configurar los puntos finales del balanceador de carga" • "Crear un punto final de balanceador de carga para FabricPool"

Certificado de punto final del grupo de almacenamiento en la nube

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión desde un grupo de almacenamiento en la nube StorageGRID 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 alerta 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 utiliza para notificaciones de alerta. • Si las comunicaciones con el servidor SMTP requieren seguridad de la capa de transporte (TLS), debe especificar el certificado CA del servidor de correo electrónico. • Especifique un certificado de cliente solo si el servidor de correo electrónico SMTP requiere certificados de cliente para la autenticación.	ALERTAS > Configuración de correo electrónico	"Configurar notificaciones por correo electrónico para alertas"

Certificado de 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 conexiones TCP, RELP/TCP y UDP a un servidor syslog externo.	CONFIGURACIÓN > Monitoreo > Servidor de auditoría y syslog	"Utilice un servidor syslog externo"

Certificado de conexión de federación de red

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autenticar y cifrar la información enviada entre el sistema StorageGRID actual y otra red en una conexión de federación de redes.	CONFIGURACIÓN > Sistema > Federación de red	• "Crear conexiones de federación de red" • "Rotar certificados de conexión"

Certificado de federación de identidad

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre StorageGRID y un proveedor de identidad externo, como Active Directory, OpenLDAP u Oracle Directory Server. Se utiliza para la federación de identidad, que permite que los grupos de administradores y los usuarios sean gestionados por un sistema externo.	CONFIGURACIÓN > Control de acceso > Federación de identidades	"Utilizar la federación de identidades"

Certificado de servidor de administración de claves (KMS)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre StorageGRID y un servidor de administración de claves externo (KMS), que proporciona claves de cifrado a los nodos del dispositivo StorageGRID .	CONFIGURACIÓN > Seguridad > Servidor de gestión de claves	"Agregar servidor de administración de claves (KMS)"

Certificado de punto final de servicios de plataforma

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión del servicio de la plataforma StorageGRID a un recurso de almacenamiento S3.	Administrador de inquilinos > ALMACENAMIENTO (S3) > Puntos finales de servicios de plataforma	"Crear punto final de servicios de plataforma" "Editar el punto final de los servicios de la plataforma"

Certificado de inicio de sesión único (SSO)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los servicios de federación de identidad, como los Servicios de federación de Active Directory (AD FS) y StorageGRID , que se utilizan para solicitudes de inicio de sesión único (SSO).	CONFIGURACIÓN > Control de acceso > Inicio de sesión único	"Configurar el inicio de sesión único"

Ejemplos de certificados

Ejemplo 1: Servicio de balanceo de carga

En este ejemplo, StorageGRID actúa como servidor.

1. Configura un punto final del equilibrador de carga y carga o genera un certificado de servidor en StorageGRID.
2. Configura una conexión de cliente S3 al punto final del equilibrador de carga y carga el mismo certificado en el cliente.
3. Cuando el cliente desea guardar o recuperar datos, se conecta al punto final del balanceador 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 verifica este certificado comparando la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión utilizando la misma clave pública.
6. El cliente envía datos de objetos a StorageGRID.

Ejemplo 2: Servidor de administración de claves externo (KMS)

En este ejemplo, StorageGRID actúa como cliente.

1. Al utilizar el software de servidor de administración de claves externo, configura StorageGRID como un cliente KMS y obtiene un certificado de servidor firmado por una CA, un certificado de cliente público y la clave privada para el certificado de cliente.
2. Con Grid Manager, configura un servidor KMS y carga los certificados del servidor y del cliente y la clave privada del cliente.
3. Cuando un nodo StorageGRID necesita una clave de cifrado, realiza una solicitud al servidor KMS que incluye datos del certificado y una firma basada en la clave privada.
4. El servidor KMS valida la firma del certificado y decide que puede confiar en StorageGRID.
5. El servidor KMS responde utilizando la conexión validada.

Tipos de certificados de servidor admitidos

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



El tipo de cifrado para 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. Ver ["Administrar certificados de seguridad"](#) . Si configura una política de seguridad personalizada que no es compatible con el certificado del servidor, puede ["volver temporalmente a la política de seguridad predeterminada"](#) .

Para obtener más información sobre cómo StorageGRID protege las conexiones de los clientes, consulte ["Seguridad para clientes S3"](#) .

Configurar certificados de interfaz de administración

Puede reemplazar el certificado de interfaz de administración predeterminado con un único certificado personalizado que permita a los usuarios acceder al Administrador de Grid y al Administrador de inquilinos sin encontrar advertencias de seguridad. También puede volver al certificado de interfaz de administración predeterminado o generar uno nuevo.

Acerca de esta tarea

De forma predeterminada, a cada nodo de administración se le emite un certificado firmado por la CA de la red. Estos certificados firmados por CA se pueden reemplazar por un único certificado de interfaz de administración personalizada común y su clave privada correspondiente.

Debido a que se utiliza un único certificado de interfaz de administración personalizado para todos los nodos

de administración, debe especificar el certificado como comodín o como certificado multidominio si los clientes necesitan verificar el nombre de host al conectarse al Administrador de red y al Administrador de inquilinos. Defina el certificado personalizado de modo que coincida con todos los nodos de administración en la cuadrícula.

Debe completar la configuración en el servidor y, dependiendo de la autoridad de certificación raíz (CA) que esté utilizando, los usuarios también podrían necesitar instalar el certificado de CA de Grid en el navegador web que usarán para acceder a Grid Manager y Tenant Manager.



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, se activa la alerta **Expiración del certificado de servidor para la interfaz de administración** cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **CONFIGURACIÓN > Seguridad > Certificados** y mirando la fecha de vencimiento del certificado de la interfaz de administración en la pestaña Global.



Si accede al Administrador de red o al Administrador de inquilinos mediante un nombre de dominio en lugar de una dirección IP, el navegador muestra un error de certificado sin una opción para omitirlo si ocurre alguna de las siguientes situaciones:

- Su certificado de interfaz de administración personalizada caduca.
- Tú [Revertir de un certificado de interfaz de administración personalizado al certificado de servidor predeterminado](#) .

Agregar un certificado de interfaz de administración personalizado

Para agregar un certificado de interfaz de administración personalizado, puede proporcionar su propio certificado o generar uno utilizando Grid Manager.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **Usar certificado personalizado**.
4. Subir o generar el certificado.

Subir certificado

Cargue los archivos de certificado de servidor necesarios.

a. Seleccione **Subir certificado**.

b. Cargue los archivos de certificado de servidor necesarios:

- **Certificado de servidor:** el archivo de certificado de servidor personalizado (codificado en PEM).
- **Clave privada del certificado:** El archivo de clave privada del certificado del servidor personalizado(`.key`).



Las claves privadas EC deben tener 224 bits o más. Las claves privadas RSA deben tener 2048 bits o más.

- **Paquete 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 certificado CA codificados en PEM, concatenados en el orden de la cadena de certificados.

c. Expande **Detalles del certificado** para ver los metadatos de cada certificado que hayas cargado. Si cargó un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Seleccione **Guardar**. + El certificado de interfaz de administración personalizada se utiliza para todas las nuevas conexiones posteriores a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

Generar certificado

Generar los archivos de certificado del servidor.



La mejor práctica para un entorno de producción es utilizar un certificado de interfaz de administración personalizado firmado por una autoridad de certificación externa.

a. Seleccione **Generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más nombres de dominio completos para incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
Propiedad intelectual	Una o más direcciones IP para incluir en el certificado.

Campo	Descripción
Asunto (opcional)	Sujeto X.509 o nombre distinguido (DN) del propietario del certificado. Si no se ingresa ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o dirección IP como nombre común del sujeto (CN).
Días válidos	Número de días después de su creación que expira el certificado.
Agregar extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y uso de clave extendido se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. Nota: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **Generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Seleccione **Guardar**. + El certificado de interfaz de administración personalizada se utiliza para todas las nuevas conexiones posteriores a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

5. Actualice la página para asegurarse de que el navegador web esté actualizado.



Después de cargar o generar un nuevo certificado, espere hasta un día para que desaparezcan las alertas de vencimiento del certificado relacionadas.

6. Después de agregar un certificado de interfaz de administración personalizado, la página Certificado de interfaz de administración muestra información detallada de los certificados que están en uso. + Puede descargar o copiar el certificado PEM según sea necesario.

Restaurar el certificado de interfaz de administración predeterminado

Puede volver a utilizar el certificado de interfaz de administración predeterminado para las conexiones de Grid Manager y Tenant Manager.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **Usar certificado predeterminado**.

Cuando restaura el certificado de interfaz de administración predeterminado, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. El certificado de interfaz de administración predeterminado se utiliza para todas las conexiones de nuevos clientes posteriores.

4. Actualice la página para asegurarse de que el navegador web esté actualizado.

Utilice un script para generar un nuevo certificado de interfaz de administración autofirmado

Si se requiere una validación estricta del nombre de host, puede utilizar un script para generar el certificado de interfaz de administración.

Antes de empezar

- Tienes "[permisos de acceso específicos](#)".
- Tú tienes el `Passwords.txt` archivo.

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

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

3. Configure StorageGRID con un nuevo certificado autofirmado.

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

- Para `--domains`, utilice caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración. Por ejemplo, `*.ui.storagegrid.example.com` utiliza el comodín `*` para representar `admin1.ui.storagegrid.example.com` y `admin2.ui.storagegrid.example.com`.
- Colocar `--type` a `management` para configurar el certificado de la interfaz de administración, que utilizan Grid Manager y Tenant Manager.
- De forma predeterminada, los certificados generados son válidos por un año (365 días) y deben volver a crearse antes de que caduquen. Puedes utilizar el `--days` argumento para anular el período de validez predeterminado.



El período de validez de un certificado comienza cuando `make-certificate` se ejecuta. Debe asegurarse de que el cliente de administración 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
```

La salida resultante contiene el certificado público que necesita su cliente de API de administración.

4. Seleccione y copie el certificado.

Incluya las etiquetas BEGIN y END en su selección.

5. Cierre la sesión del shell de comandos. `$ exit`

6. Confirme que se configuró el certificado:

- Acceda al Administrador de cuadrícula.
- Seleccione **CONFIGURACIÓN > Seguridad > Certificados**
- En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.

7. Configure su cliente de administración para utilizar el certificado público que copió. Incluya las etiquetas BEGIN y END.

Descargue o copie el certificado de interfaz de administración

Puede guardar o copiar el contenido del certificado de la interfaz de administración para usarlo en otro lugar.

Pasos

- Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
- En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.
- Seleccione la pestaña **Servidor** o **Paquete CA** y luego descargue o copie el certificado.

Descargar archivo de certificado o paquete de CA

Descargar el certificado o paquete de CA .pem archivo. Si está utilizando un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

- a. Seleccione **Descargar certificado** o **Descargar paquete de CA**.

Si está descargando un paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se descargan como un solo archivo.

- b. Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem .

Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado o paquete de CA PEM

Copie el texto del certificado para pegarlo en otro lugar. Si está utilizando un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

- a. Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM**.

Si está copiando un paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se copian juntos.

- b. Pegue el certificado copiado en un editor de texto.
- c. Guarde el archivo de texto con la extensión .pem .

Por ejemplo: `storagegrid_certificate.pem`

Configurar certificados de API S3

Puede reemplazar o restaurar el certificado de servidor que se utiliza para las conexiones de cliente S3 a los nodos de almacenamiento o a los puntos finales del equilibrador de carga. El certificado de servidor personalizado de reemplazo es específico para su organización.



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["StorageGRID 11.8: Configurar certificados de API de S3 y Swift"](#) .

Acerca de esta tarea

De forma predeterminada, a cada nodo de almacenamiento se le emite un certificado de servidor X.509 firmado por la CA de la red. Estos certificados firmados por CA se pueden reemplazar por un único certificado de servidor personalizado común y su clave privada correspondiente.

Se utiliza un único certificado de servidor personalizado para todos los nodos de almacenamiento, por lo que debe especificar el certificado como comodín o un certificado multidominio si los clientes necesitan verificar el nombre de host al conectarse al punto final de almacenamiento. Defina el certificado personalizado de modo que coincida con todos los nodos de almacenamiento de la red.

Después de completar la configuración en el servidor, es posible que también necesite instalar el certificado

CA de Grid en el cliente API S3 que usará para acceder al sistema, dependiendo de la autoridad de certificación raíz (CA) que esté utilizando.



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, la alerta **Expiración del certificado de servidor global para la API S3** se activa cuando el certificado del servidor raíz está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **CONFIGURACIÓN > Seguridad > Certificados** y mirando la fecha de vencimiento del certificado de API S3 en la pestaña Global.

Puede cargar o generar un certificado API S3 personalizado.

Agregar un certificado API S3 personalizado

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **Certificado API S3**.
3. Seleccione **Usar certificado personalizado**.
4. Subir o generar el certificado.

Subir certificado

Cargue los archivos de certificado de servidor necesarios.

a. Seleccione **Subir certificado**.

b. Cargue los archivos de certificado de servidor necesarios:

- **Certificado de servidor:** el archivo de certificado de servidor personalizado (codificado en PEM).
- **Clave privada del certificado:** El archivo de clave privada del certificado del servidor personalizado(`.key`).



Las claves privadas EC deben tener 224 bits o más. Las claves privadas RSA deben tener 2048 bits o más.

- **Paquete 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 certificado CA codificados en PEM, concatenados en el orden de la cadena de certificados.
- c. Seleccione los detalles del certificado para mostrar los metadatos y PEM de cada certificado API S3 personalizado que se cargó. Si cargó un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Seleccione **Guardar**.

El certificado de servidor personalizado se utiliza para nuevas conexiones de cliente S3 posteriores.

Generar certificado

Generar los archivos de certificado del servidor.

a. Seleccione **Generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más nombres de dominio completos para incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
Propiedad intelectual	Una o más direcciones IP para incluir en el certificado.

Campo	Descripción
Asunto (opcional)	Sujeto X.509 o nombre distinguido (DN) del propietario del certificado. Si no se ingresa ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o dirección IP como nombre común del sujeto (CN).
Días válidos	Número de días después de su creación que expira el certificado.
Agregar extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y uso de clave extendido se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. Nota: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **Generar**.

d. Seleccione **Detalles del certificado** para mostrar los metadatos y PEM del certificado API S3 personalizado que se generó.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Seleccione **Guardar**.

El certificado de servidor personalizado se utiliza para nuevas conexiones de cliente S3 posteriores.

5. Seleccione una pestaña para mostrar los metadatos del certificado de servidor StorageGRID predeterminado, un certificado firmado por CA que se cargó o un certificado personalizado que se generó.



Después de cargar o generar un nuevo certificado, espere hasta un día para que desaparezcan las alertas de vencimiento del certificado relacionadas.

6. Actualice la página para asegurarse de que el navegador web esté actualizado.

7. Después de agregar un certificado API S3 personalizado, la página del certificado API S3 muestra información detallada del certificado API S3 personalizado que está en uso. + Puede descargar o copiar el certificado PEM según sea necesario.

Restaurar el certificado API S3 predeterminado

Puede volver a utilizar el certificado API S3 predeterminado para las conexiones de cliente S3 a los nodos de almacenamiento. Sin embargo, no puedes usar el certificado API S3 predeterminado para un punto final del balanceador de carga.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **Certificado API S3**.
3. Seleccione **Usar certificado predeterminado**.

Cuando restaura la versión predeterminada del certificado API S3 global, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. El certificado API S3 predeterminado se utilizará para las nuevas conexiones de clientes S3 posteriores a los nodos de almacenamiento.

4. Seleccione **Aceptar** para confirmar la advertencia y restaurar el certificado API S3 predeterminado.

Si tiene permiso de acceso de root y se utilizó el certificado API S3 personalizado para las conexiones de puntos finales del balanceador de carga, se muestra una lista de puntos finales del balanceador de carga que ya no serán accesibles mediante el certificado API S3 predeterminado. Ir a ["Configurar los puntos finales del balanceador de carga"](#) para editar o eliminar los puntos finales afectados.

5. Actualice la página para asegurarse de que el navegador web esté actualizado.

Descargue o copie el certificado de API S3

Puede guardar o copiar el contenido del certificado API S3 para usarlo en otro lugar.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **Certificado API S3**.
3. Seleccione la pestaña **Servidor** o **Paquete CA** y luego descargue o copie el certificado.

Descargar archivo de certificado o paquete de CA

Descargar el certificado o paquete de CA .pem archivo. Si está utilizando un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

- a. Seleccione **Descargar certificado** o **Descargar paquete de CA**.

Si está descargando un paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se descargan como un solo archivo.

- b. Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem .

Por ejemplo: storagegrid_certificate.pem

Copiar certificado o paquete de CA PEM

Copie el texto del certificado para pegarlo en otro lugar. Si está utilizando un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

- a. Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM**.

Si está copiando un paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se copian juntos.

- b. Pegue el certificado copiado en un editor de texto.
- c. Guarde el archivo de texto con la extensión .pem .

Por ejemplo: storagegrid_certificate.pem

Información relacionada

- ["Utilice la API REST de S3"](#)
- ["Configurar nombres de dominio de puntos finales S3"](#)

Copiar el certificado de CA de Grid

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante 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 CA del sistema StorageGRID .

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Grid CA**.

2. En la sección **Certificado PEM**, descargue o copie el certificado.

Descargar archivo de certificado

Descargar el certificado .pem archivo.

- Seleccione **Descargar certificado**.
- Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem .

Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado PEM

Copie el texto del certificado para pegarlo en otro lugar.

- Seleccione **Copiar certificado PEM**.
- Pegue el certificado copiado en un editor de texto.
- Guarde el archivo de texto con la extensión .pem .

Por ejemplo: `storagegrid_certificate.pem`

Configurar certificados StorageGRID para FabricPool

Para los clientes S3 que realizan una validación estricta del nombre de host y no admiten la desactivación de la validación estricta del nombre de host, como los clientes ONTAP que usan FabricPool, puede generar o cargar un certificado de servidor cuando configura el punto final del equilibrador de carga.

Antes de empezar

- Tienes ["permisos de acceso específicos"](#) .
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .

Acerca de esta tarea

Cuando crea un punto final de balanceador de carga, puede generar un certificado de servidor autofirmado o cargar un certificado firmado por una autoridad de certificación (CA) conocida. En entornos de producción, debe utilizar 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 del tipo "man-in-the-middle".

Los siguientes pasos proporcionan pautas generales para los clientes S3 que utilizan FabricPool. Para obtener información y procedimientos más detallados, consulte ["Configurar StorageGRID para FabricPool"](#) .

Pasos

- Opcionalmente, configure un grupo de alta disponibilidad (HA) para que lo utilice FabricPool .
- Cree un punto final de balanceador de carga S3 para que lo utilice FabricPool .

Cuando crea un punto final de balanceador de carga HTTPS, se le solicita que cargue su certificado de servidor, la clave privada del certificado y el paquete de CA opcional.

3. Adjunte StorageGRID como un nivel de nube en ONTAP.

Especifique el puerto del punto final del equilibrador de carga y el nombre de dominio completo utilizado en el certificado de CA que cargó. Luego, proporcione el certificado CA.



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

Configurar certificados de cliente

Los certificados de cliente permiten que los clientes externos autorizados accedan a la base de datos Prometheus de StorageGRID , lo que proporciona una forma segura para que las herramientas externas monitoreen StorageGRID.

Si necesita acceder a StorageGRID mediante una herramienta de monitoreo externa, debe cargar o generar un certificado de cliente utilizando Grid Manager y copiar la información del certificado a la herramienta externa.

Ver "[Administrar certificados de seguridad](#)" y "[Configurar certificados de servidor personalizados](#)".



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, se activa la alerta **Expiración de certificados de cliente configurados en la página Certificados** cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **CONFIGURACIÓN > Seguridad > Certificados** y mirando la fecha de vencimiento del certificado del cliente en la pestaña Cliente.



Si está utilizando un servidor de administración de claves (KMS) para proteger los datos en nodos de dispositivos especialmente configurados, consulte la información específica sobre "[Cargar un certificado de cliente KMS](#)".

Antes de empezar

- Tienes permiso de acceso root.
- Ha 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 nodo de administración.
 - Si ha configurado el certificado de interfaz de administración de StorageGRID , tiene la CA, el certificado de cliente y la clave privada que se utilizan para configurar el certificado de interfaz de administración.
 - Para cargar su propio certificado, la clave privada del certificado está disponible en su computadora local.
 - La clave privada debe haber sido guardada o registrada en el momento de su creación. Si no tiene la clave privada original, debe crear una nueva.
- Para editar un certificado de cliente:
 - Tienes la dirección IP o el nombre de dominio del nodo de administración.
 - Para cargar su propio certificado o un certificado nuevo, la clave privada, el certificado del cliente y la CA (si se utiliza) están disponibles en su computadora local.

Agregar certificados de cliente

Para agregar el certificado de cliente, utilice uno de estos procedimientos:

- [Certificado de interfaz de administración ya configurado](#)
- [Certificado de cliente emitido por CA](#)
- [Certificado generado desde Grid Manager](#)

Certificado de interfaz de administración ya configurado

Utilice este procedimiento para agregar un certificado de cliente si ya hay configurado un certificado de interfaz de administración mediante una CA proporcionada por el cliente, un certificado de cliente y una clave privada.

Pasos

1. En el Administrador de red, seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.
5. Seleccione **Continuar**.
6. Para el paso **Adjuntar certificados**, cargue el certificado de la interfaz de administración.
 - a. Seleccione **Subir certificado**.
 - b. Seleccione **Explorar** y seleccione el archivo de certificado de la interfaz de administración(.pem).
 - Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.
 - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
 - c. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

El nuevo certificado aparece en la pestaña Cliente.

7. [Configurar una herramienta de monitorización externa](#), como Grafana.

Certificado de cliente emitido por CA

Utilice este procedimiento para agregar un certificado de cliente administrador si no se configuró un certificado de interfaz de administración y planea agregar un certificado de cliente para Prometheus que utiliza un certificado de cliente emitido por una CA y una clave privada.

Pasos

1. Realice los pasos para ["configurar un certificado de interfaz de administración"](#) .
2. En el Administrador de red, seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
3. Seleccione **Agregar**.
4. Introduzca un nombre de certificado.

5. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.
6. Seleccione **Continuar**.
7. Para el paso **Adjuntar certificados**, cargue el certificado del cliente, la clave privada y los archivos del paquete de CA:
 - a. Seleccione **Subir certificado**.
 - b. Seleccione **Explorar** y seleccione el certificado del cliente, la clave privada y los archivos del paquete de CA(.pem).
 - Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.
 - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
 - c. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

Los nuevos certificados aparecen en la pestaña Cliente.

8. [Configurar una herramienta de monitorización externa](#), como Grafana.

Certificado generado desde Grid Manager

Utilice este procedimiento para agregar un certificado de cliente administrador si no se configuró un certificado de interfaz de administración y planea agregar un certificado de cliente para Prometheus que use la función de generar certificado en Grid Manager.

Pasos

1. En el Administrador de red, seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.
5. Seleccione **Continuar**.
6. Para el paso **Adjuntar certificados**, seleccione **Generar certificado**.
7. Especifique la información del certificado:
 - **Asunto** (opcional): sujeto X.509 o nombre distinguido (DN) del propietario del certificado.
 - **Días de validez**: La cantidad de días que el certificado generado es válido, a partir del momento en que se genera.
 - **Agregar extensiones de uso de clave**: si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y de uso de clave extendida se agregan al certificado generado.

Estas extensiones definen el propósito de la clave contenida en el certificado.



Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

8. Seleccione **Generar**.

9. Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.



No podrá ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copie o descargue la clave en un lugar seguro.

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar clave privada** para copiar la clave privada del certificado y pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como un archivo.

Especifique el nombre del archivo de clave privada y la ubicación de descarga.

10. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

El nuevo certificado aparece en la pestaña Cliente.

11. En el Administrador de red, seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Global**.
12. Seleccione **Certificado de interfaz de administración**.
13. Seleccione **Usar certificado personalizado**.
14. Cargue los archivos `certificate.pem` y `private_key.pem` desde el [detalles del certificado del cliente](#) paso. No es necesario cargar el paquete CA.
- a. Seleccione **Cargar certificado** y luego seleccione **Continuar**.
 - b. Subir cada archivo de certificado(`.pem`).
 - c. Seleccione **Guardar** para guardar el certificado en el Administrador de Grid.

El nuevo certificado aparece en la página de certificados de la interfaz de administración.

15. [Configurar una herramienta de monitorización externa](#), como Grafana.

Configurar una herramienta de monitoreo externo

Pasos

1. Configure los siguientes ajustes en su herramienta de monitoreo externa, como Grafana.
 - a. **Nombre:** Ingrese un nombre para la conexión.

StorageGRID no requiere esta información, pero debe proporcionar un nombre para probar la conexión.
 - b. **URL:** Ingrese el nombre de dominio o la dirección IP del nodo de administración. Especifique HTTPS y el puerto 9091.

Por ejemplo: `https://admin-node.example.com:9091`

c. Habilitar **Autenticación de cliente TLS y Con certificado CA**.

d. En Detalles de autenticación TLS/SSL, copie y pegue: +

- El certificado CA de la interfaz de administración para **CA Cert**
- El certificado de cliente para **Certificado de cliente**
- La clave privada de **Clave de cliente**

e. **ServerName**: Ingrese 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 administración.

2. Guarde y pruebe el certificado y la clave privada que copió de StorageGRID o de un archivo local.

Ahora puede acceder a las métricas de Prometheus desde StorageGRID con su herramienta de monitoreo externa.

Para obtener información sobre las métricas, consulte la ["Instrucciones para monitorear StorageGRID"](#).

Editar certificados de cliente

Puede editar un certificado de cliente administrador para cambiar su nombre, habilitar o deshabilitar el acceso a Prometheus o cargar un nuevo certificado cuando el actual haya expirado.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.

Las fechas de vencimiento de los certificados y los permisos de acceso de Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya caducó, aparece un mensaje en la tabla y se activa una alerta.

2. Seleccione el certificado que desea editar.

3. Seleccione **Editar** y luego seleccione **Editar nombre y permiso**

4. Introduzca un nombre de certificado.

5. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.

6. Seleccione **Continuar** para guardar el certificado en el Administrador de Grid.

El certificado actualizado se muestra en la pestaña Cliente.

Adjuntar nuevo certificado de cliente

Puede cargar un nuevo certificado cuando el actual haya expirado.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.

Las fechas de vencimiento de los certificados y los permisos de acceso de Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya caducó, aparece un mensaje en la tabla y se activa una alerta.

2. Seleccione el certificado que desea editar.
3. Seleccione **Editar** y luego seleccione una opción de edición.

Subir certificado

Copie el texto del certificado para pegarlo en otro lugar.

- a. Seleccione **Cargar certificado** y luego seleccione **Continuar**.
- b. Subir el nombre del certificado del cliente(.pem).

Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem .

Por ejemplo: storagegrid_certificate.pem

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
- c. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

El certificado actualizado se muestra en la pestaña Cliente.

Generar certificado

Generar el texto del certificado para pegarlo en otro lugar.

- a. Seleccione **Generar certificado**.
- b. Especifique la información del certificado:

- **Asunto** (opcional): sujeto X.509 o nombre distinguido (DN) del propietario del certificado.
- **Días de validez**: La cantidad de días que el certificado generado es válido, a partir del momento en que se genera.
- **Agregar extensiones de uso de clave**: si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y de uso de clave extendida se agregan al certificado generado.

Estas extensiones definen el propósito de la clave contenida en el certificado.



Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

- c. Seleccione **Generar**.
- d. Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.



No podrá ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copie o descargue la clave en un lugar seguro.

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro

lugar.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar clave privada** para copiar la clave privada del certificado y pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como un archivo.

Especifique el nombre del archivo de clave privada y la ubicación de descarga.

e. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

El nuevo certificado aparece en la pestaña Cliente.

Descargar o copiar certificados de cliente

Puede descargar o copiar un certificado de cliente para usarlo en otro lugar.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione el certificado que desea copiar o descargar.
3. Descargue o copie el certificado.

Descargar archivo de certificado

Descargar el certificado `.pem` archivo.

- a. Seleccione **Descargar certificado**.
- b. Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado

Copie el texto del certificado para pegarlo en otro lugar.

- a. Seleccione **Copiar certificado PEM**.
- b. Pegue el certificado copiado en un editor de texto.
- c. Guarde el archivo de texto con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

Eliminar certificados de cliente

Si ya no necesita un certificado de cliente administrador, puede eliminarlo.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione el certificado que desea eliminar.
3. Seleccione **Eliminar** y luego confirme.



Para eliminar hasta 10 certificados, seleccione cada certificado que desee eliminar en la pestaña Cliente y luego seleccione **Acciones > Eliminar**.

Después de eliminar un certificado, los clientes que lo usaron deben especificar un nuevo certificado de cliente para acceder a la base de datos StorageGRID Prometheus.

Configurar ajustes de seguridad

Administrar la política TLS y SSH

La política TLS y SSH determina qué protocolos y cifrados se utilizan para establecer conexiones TLS seguras con aplicaciones cliente y conexiones SSH seguras con servicios internos de StorageGRID .

La política de seguridad controla cómo TLS y SSH cifran los datos en movimiento. En general, utilice la política de compatibilidad moderna (predeterminada), a menos que su sistema necesite cumplir con los Criterios comunes o necesite utilizar otros cifrados.



Algunos servicios de StorageGRID no se han actualizado para usar los cifrados en estas políticas.

Antes de empezar

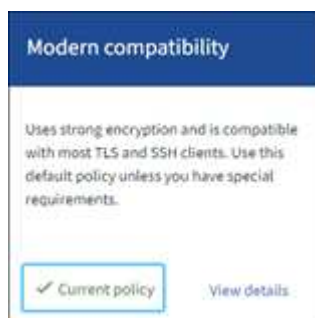
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .

Seleccione una política de seguridad

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Configuración de seguridad**.

La pestaña **Políticas TLS y SSH** muestra las políticas disponibles. La política actualmente activa se indica mediante una marca de verificación verde en el mosaico de políticas.



2. Revise los mosaicos para conocer las políticas disponibles.

Política	Descripción
Compatibilidad moderna (predeterminada)	Utilice la política predeterminada si necesita un cifrado fuerte y a menos que tenga requisitos especiales. Esta política es compatible con la mayoría de los clientes TLS y SSH.
Compatibilidad heredada	Utilice esta política si necesita opciones de compatibilidad adicionales para clientes más antiguos. Las opciones adicionales en esta política podrían hacerla menos segura que la política de compatibilidad moderna.
Criterios comunes	Utilice esta política si necesita la certificación Common Criteria.
FIPS estricto	Utilice esta política si necesita la certificación Common Criteria y usar el Módulo de seguridad criptográfica de NetApp 3.0.8 para conexiones de clientes externos a puntos finales de balanceador de carga, Tenant Manager y Grid Manager. El uso de esta política podría reducir el rendimiento. Nota: Después de seleccionar esta política, todos los nodos deben estar "reiniciado de forma continua" para activar el módulo de seguridad criptográfica de NetApp . Utilice Mantenimiento > Reinicio progresivo para iniciar y supervisar los reinicios.
Costumbre	Cree una política personalizada si necesita aplicar sus propios cifrados.

3. Para ver detalles sobre los cifrados, protocolos y algoritmos de cada política, seleccione **Ver detalles**.
4. Para cambiar la política actual, seleccione **Usar política**.

Aparece una marca de verificación verde junto a **Política actual** en el mosaico de políticas.

Crear una política de seguridad personalizada

Puede crear una política personalizada si necesita aplicar sus propios cifrados.

Pasos

1. Desde el mosaico de la política que sea más similar a la política personalizada que desea crear, seleccione **Ver detalles**.
2. Seleccione **Copiar al portapapeles** y luego seleccione **Cancelar**.



3. Desde el mosaico **Política personalizada**, seleccione **Configurar y usar**.
4. Pegue el JSON que copió y realice los cambios necesarios.
5. Seleccione **Política de uso**.

Aparece una marca de verificación verde junto a **Política actual** en el mosaico Política personalizada.

6. Opcionalmente, seleccione **Editar configuración** para realizar más cambios en la nueva política personalizada.

Revertir temporalmente a la política de seguridad predeterminada

Si configuró una política de seguridad personalizada, es posible que no pueda iniciar sesión en Grid Manager si la política TLS configurada es incompatible con la ["certificado de servidor configurado"](#).

Puede volver temporalmente a la política de seguridad predeterminada.

Pasos

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

Cuando inicia sesión como root, el mensaje cambia de \$ a # .

2. Ejecute el siguiente comando:

```
restore-default-cipher-configurations
```

3. Desde un navegador web, acceda al Administrador de cuadrícula en el mismo nodo de administración.
4. Siga los pasos en [Seleccione una política de seguridad](#) para configurar la política nuevamente.

Configurar la seguridad de la red y de los objetos

Puede configurar la seguridad de la red y de los objetos para cifrar los objetos almacenados, evitar ciertas solicitudes S3 o permitir que las conexiones de los clientes a los nodos de almacenamiento utilicen HTTP en lugar de HTTPS.

Cifrado de objetos almacenados

El cifrado de objetos almacenados permite el cifrado de todos los datos de los objetos a medida que se ingieren a través de S3. De forma predeterminada, los objetos almacenados no están cifrados, pero puede elegir cifrarlos utilizando el algoritmo de cifrado AES-128 o AES-256. Cuando habilita la configuración, todos los objetos recién ingeridos se cifran, pero no se realiza ningún cambio en los objetos almacenados existentes. Si deshabilita el cifrado, los objetos actualmente cifrados permanecerán cifrados, pero los objetos recién ingeridos no lo estarán.

La configuración de cifrado de objetos almacenados se aplica únicamente a los objetos S3 que no se han cifrado mediante cifrado a nivel de depósito o de objeto.

Para obtener más detalles sobre los métodos de cifrado de StorageGRID , consulte ["Revisar los métodos de cifrado de StorageGRID"](#) .

Evitar modificaciones del cliente

Evitar modificaciones del cliente es una configuración de todo el sistema. Cuando se selecciona la opción **Impedir modificación del cliente**, se rechazan las siguientes solicitudes.

API REST de S3

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

Habilitar HTTP para conexiones de nodo de almacenamiento

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para cualquier conexión directa a los nodos de almacenamiento. Opcionalmente, puede habilitar HTTP para estas conexiones, por ejemplo, al probar una cuadrícula que no es de producción.

Utilice HTTP para las conexiones de nodo de almacenamiento solo si los clientes S3 necesitan realizar conexiones HTTP directamente a los nodos de almacenamiento. No es necesario utilizar esta opción para clientes que solo usan conexiones HTTPS o para clientes que se conectan al servicio Load Balancer (porque puede ["configurar cada punto final del balanceador de carga"](#) para utilizar HTTP o HTTPS).

Ver ["Resumen: Direcciones IP y puertos para conexiones de cliente"](#) para conocer qué puertos utilizan los clientes S3 cuando se conectan a nodos de almacenamiento mediante HTTP o HTTPS.

Seleccionar opciones

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes permiso de acceso root.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Configuración de seguridad**.
2. Seleccione la pestaña **Red y objetos**.
3. Para el cifrado de objetos almacenados, utilice la configuración **Ninguno** (predeterminada) si no desea que se cifren los objetos almacenados, o seleccione **AES-128** o **AES-256** para cifrar los objetos almacenados.
4. Opcionalmente, seleccione **Evitar modificación del cliente** si desea evitar que los clientes S3 realicen solicitudes específicas.



Si cambia esta configuración, tomará aproximadamente un minuto para que se aplique la nueva configuración. El valor configurado se almacena en caché para mejorar el rendimiento y la escala.

5. Opcionalmente, seleccione **Habilitar HTTP para conexiones de nodo de almacenamiento** si los clientes se conectan directamente a los nodos de almacenamiento y desea utilizar conexiones HTTP.



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

6. Seleccione **Guardar**.

Cambiar la configuración de seguridad de la interfaz

La configuración de seguridad de la interfaz le permite controlar si se cierra la sesión de los usuarios si están inactivos durante más de la cantidad de tiempo especificada y si se incluye un seguimiento de pila en las respuestas de error de API.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["Permiso de acceso root"](#).

Acerca de esta tarea

La página **Configuración de seguridad** incluye las configuraciones de **Tiempo de espera de inactividad del navegador** y **Seguimiento de la pila de API de administración**.

Tiempo de espera por inactividad del navegador

Indica cuánto tiempo puede estar inactivo el navegador de un usuario antes de que se cierre la sesión. El valor predeterminado es 15 minutos.

El tiempo de espera por inactividad del navegador también está controlado por lo siguiente:

- Un temporizador StorageGRID independiente, no configurable, que se incluye para la seguridad del sistema. El token de autenticación de cada usuario expira 16 horas después de que el usuario inicia sesión. Cuando expira la autenticación de un usuario, ese usuario cierra la sesión automáticamente, incluso si el tiempo de espera de inactividad del navegador está deshabilitado o no se ha alcanzado el valor del tiempo de espera del navegador. Para renovar el token, el usuario deberá volver a iniciar sesión.
- Configuración de tiempo de espera para el proveedor de identidad, asumiendo que el inicio de sesión único (SSO) está habilitado para StorageGRID.

Si SSO está habilitado y el navegador de un usuario expira, el usuario debe volver a ingresar sus

credenciales de SSO para acceder a StorageGRID nuevamente. Ver ["Configurar el inicio de sesión único"](#) .

Seguimiento de la pila de la API de gestión

Controla si se devuelve un seguimiento de pila en las respuestas de error de API de Grid Manager y Tenant Manager.

Esta opción está deshabilitada de forma predeterminada, pero es posible que desee habilitar esta funcionalidad para un entorno de prueba. En general, debe dejar el seguimiento de pila deshabilitado en entornos de producción para evitar revelar detalles internos del software cuando ocurren errores de API.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Configuración de seguridad**.
2. Seleccione la pestaña **Interfaz**.
3. Para cambiar la configuración del tiempo de espera por inactividad del navegador:
 - a. Expandir el acordeón.
 - b. Para cambiar el período de tiempo de espera, especifique un valor entre 60 segundos y 7 días. El tiempo de espera predeterminado es de 15 minutos.
 - c. Para desactivar esta función, desmarque la casilla de verificación.
 - d. Seleccione **Guardar**.

La nueva configuración no afecta a los usuarios que actualmente hayan iniciado sesión. Los usuarios deben iniciar sesión nuevamente o actualizar sus navegadores para que la nueva configuración de tiempo de espera surta efecto.

4. Para cambiar la configuración del seguimiento de la pila de la API de administración:
 - a. Expandir el acordeón.
 - b. Seleccione la casilla de verificación para devolver un seguimiento de la pila en las respuestas de error de API de Grid Manager y Tenant Manager.



Deje el seguimiento de pila deshabilitado en entornos de producción para evitar revelar detalles internos del software cuando se producen errores de API.

- c. Seleccione **Guardar**.

Configurar servidores de administración de claves

¿Qué es un servidor de administración de claves (KMS)?

Un servidor de administración de claves (KMS) es un sistema externo de terceros que proporciona claves de cifrado a los nodos del dispositivo StorageGRID en el sitio StorageGRID asociado mediante el Protocolo de interoperabilidad de administración de claves (KMIP).

StorageGRID solo admite ciertos servidores de administración de claves. Para obtener una lista de productos y versiones compatibles, utilice el ["Herramienta de matriz de interoperabilidad de NetApp \(IMT\)"](#) .

Puede utilizar uno o más servidores de administración de claves para administrar las claves de cifrado de nodo para cualquier nodo del dispositivo StorageGRID que tenga la configuración **Cifrado de nodo** habilitada

durante la instalación. El uso de servidores de administración de claves con estos nodos de dispositivos le permite proteger sus datos incluso si se quita un dispositivo del centro de datos. Una vez cifrados los volúmenes del dispositivo, no podrá acceder a ningún dato del dispositivo a menos que el nodo pueda comunicarse con el KMS.



StorageGRID no crea ni administra las claves externas que se utilizan para cifrar y descifrar los nodos del dispositivo. Si planea utilizar un servidor de administración de claves externo para proteger los datos de StorageGRID , debe comprender cómo configurar ese servidor y cómo administrar las claves de cifrado. La realización de tareas de gestión de claves queda fuera del alcance de estas instrucciones. Si necesita ayuda, consulte la documentación de su servidor de administración de claves o comuníquese con el soporte técnico.

Configuración de KMS y dispositivos

Antes de poder usar un servidor de administración de claves (KMS) para proteger los datos de StorageGRID en los nodos del dispositivo, debe completar dos tareas de configuración: configurar uno o más servidores KMS y habilitar el cifrado de nodos para los nodos del dispositivo. Una vez completadas estas dos tareas de configuración, el proceso de gestión de claves se produce automáticamente.

El diagrama de flujo muestra los pasos de alto nivel para usar un KMS para proteger los datos de StorageGRID en los nodos del dispositivo.

El diagrama de flujo muestra la configuración de KMS y la configuración del dispositivo ocurriendo en paralelo; sin embargo, puede configurar los servidores de administración de claves antes o después de habilitar el cifrado de nodos para los nuevos nodos del dispositivo, según sus requisitos.

Configurar el servidor de administración de claves (KMS)

La configuración de un servidor de administración de claves incluye los siguientes pasos de alto nivel.

Paso	Referirse a
Acceda al software KMS y agregue un cliente para StorageGRID a cada KMS o clúster KMS.	"Configurar StorageGRID como cliente en el KMS"
Obtenga la información requerida para el cliente StorageGRID en el KMS.	"Configurar StorageGRID como cliente en el KMS"
Agregue el KMS al Grid Manager, asígnelo a un solo sitio o a un grupo predeterminado de sitios, cargue los certificados necesarios y guarde la configuración del KMS.	"Agregar un servidor de administración de claves (KMS)"

Configurar el aparato

La configuración de un nodo de dispositivo para el uso de KMS incluye los siguientes pasos de alto nivel.

1. Durante la etapa de configuración de hardware de la instalación del dispositivo, utilice el instalador de dispositivos StorageGRID para habilitar la configuración **Cifrado de nodo** para el dispositivo.



No se puede habilitar la configuración **Cifrado de nodo** después de agregar un dispositivo a la red, y no se puede usar la administración de claves externa para dispositivos que no tengan habilitado el cifrado de nodo.

2. Ejecute el instalador del dispositivo StorageGRID . Durante la instalación, se asigna una clave de cifrado de datos aleatoria (DEK) a cada volumen del dispositivo, de la siguiente manera:
 - Las DEK se utilizan para cifrar los datos en cada volumen. Estas claves se generan mediante el cifrado de disco LUKS (configuración de clave unificada de Linux) en el sistema operativo del dispositivo y no se pueden modificar.
 - Cada DEK individual está encriptado por una clave de encriptación maestra (KEK). La KEK inicial es una clave temporal que cifra las DEK hasta que el dispositivo pueda conectarse al KMS.
3. Agregue el nodo del dispositivo a StorageGRID.

Ver "[Habilitar el cifrado de nodos](#)" Para más detalles.

Proceso de cifrado de gestión de claves (se produce automáticamente)

El cifrado de gestión de claves incluye los siguientes pasos de alto nivel que se realizan automáticamente.

1. Cuando instala un dispositivo que tiene el cifrado de nodo habilitado en la red, StorageGRID determina 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 de KMS.
 - Si aún no se ha configurado un KMS para el sitio, los datos del dispositivo continúan encriptados por la KEK temporal hasta que configure un KMS para el sitio y el dispositivo reciba la configuración del KMS.
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 reemplaza 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, los volúmenes del dispositivo no deben considerarse protegidos contra la eliminación del centro de datos hasta que la clave temporal sea reemplazada por la clave de cifrado KMS.

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 puede sobrevivir a una pérdida de energía o a un reinicio.

Consideraciones y requisitos para utilizar un servidor de administración de claves

Antes de configurar un servidor de administración de claves externo (KMS), debe comprender las consideraciones y los requisitos.

¿Qué versión de KMIP es compatible?

StorageGRID es compatible con KMIP versión 1.4.

["Especificación del protocolo de interoperabilidad de gestión de claves versión 1.4"](#)

¿Cuáles son las consideraciones de la red?

La configuración del firewall de red debe permitir que cada nodo del dispositivo se comuniquen a través del puerto utilizado para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El puerto KMIP predeterminado es 5696.

Debe asegurarse de que cada nodo del dispositivo que utiliza cifrado de nodo tenga acceso a la red del KMS o del clúster KMS que configuró 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 un clúster KMS, según lo que admita el KMS y que ["Política de TLS y SSH"](#) estás usando

StorageGRID negocia el protocolo y el cifrado (TLS 1.2) o el conjunto de cifrados (TLS 1.3) con el KMS cuando realiza la conexión. Para ver qué versiones de protocolo y cifrados/conjuntos de cifrados están disponibles, revise la `tlsOutbound` sección de la política TLS y SSH activa de la red (**CONFIGURACIÓN > Seguridad Configuración de seguridad**).

¿Qué dispositivos son compatibles?

Puede utilizar un servidor de administración de claves (KMS) para administrar las claves de cifrado para cualquier dispositivo StorageGRID en su red que tenga habilitada la configuración **Cifrado de nodo**. Esta configuración solo se puede habilitar durante la etapa de configuración de hardware de la instalación del dispositivo mediante el instalador de dispositivos StorageGRID.



No se puede habilitar el cifrado de nodos después de agregar un dispositivo a la red, y no se puede usar la administración de claves externa para dispositivos que no tengan habilitado el cifrado de nodos.

Puede utilizar el KMS configurado para dispositivos StorageGRID y nodos de dispositivos.

No se puede utilizar el KMS configurado para nodos basados en software (que no sean dispositivos), incluidos los siguientes:

- Nodos implementados como máquinas virtuales (VM)
- Nodos implementados dentro de motores de contenedores en hosts Linux

Los nodos implementados en estas otras plataformas pueden usar cifrado fuera de StorageGRID en el nivel de disco o de almacén de datos.

¿Cuándo debo configurar los servidores de administración de claves?

Para una nueva instalación, normalmente debe configurar uno o más servidores de administración de claves en Grid Manager antes de crear inquilinos. Esta orden garantiza que los nodos estén protegidos antes de que se almacenen datos de objetos en ellos.

Puede configurar los servidores de administración de claves en Grid Manager antes o después de instalar los nodos del dispositivo.

¿Cuántos servidores de gestión de claves necesito?

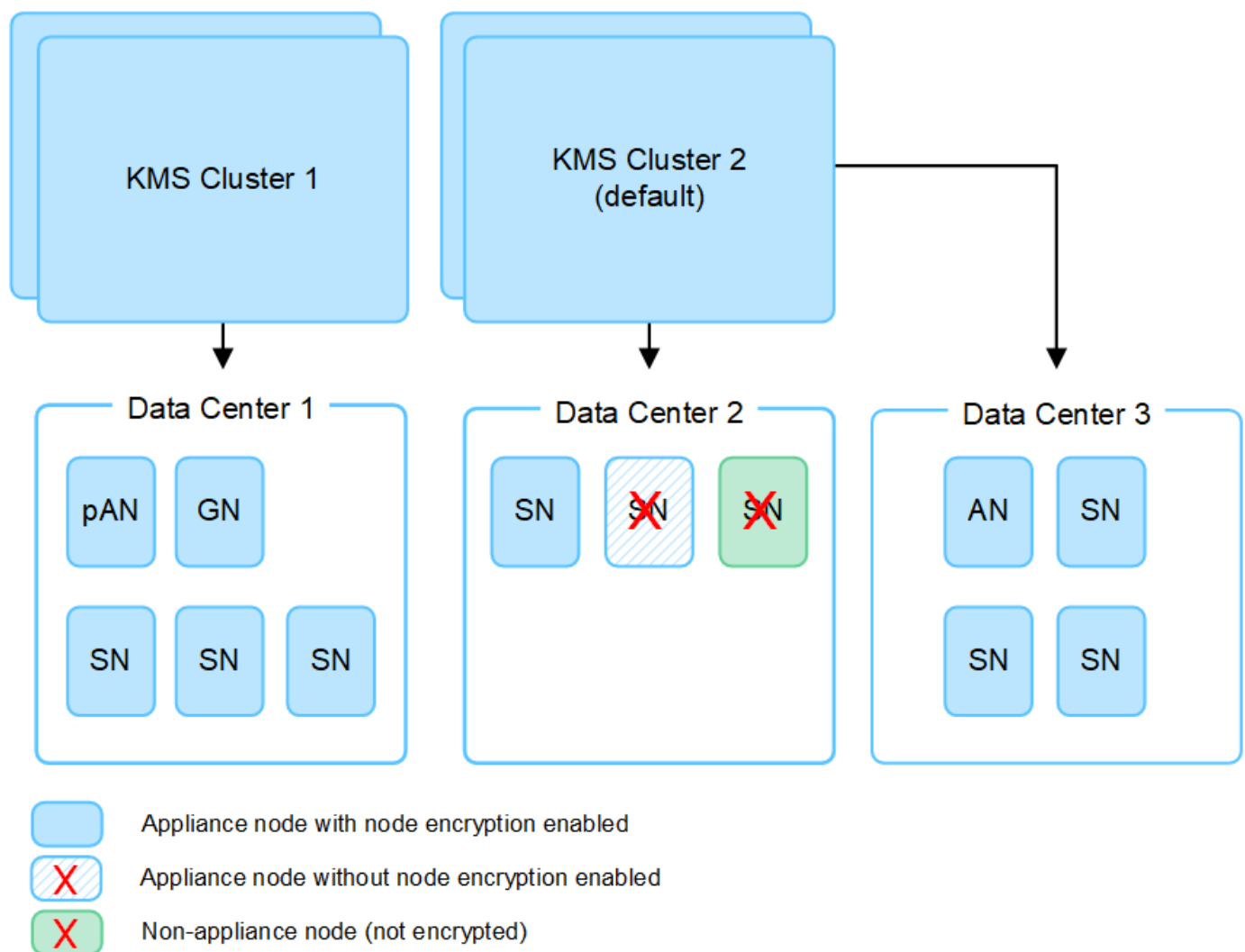
Puede configurar uno o más servidores de administración de claves externos para proporcionar claves de

cifrado a los nodos del dispositivo en su sistema StorageGRID . Cada KMS proporciona una única clave de cifrado a los nodos del dispositivo StorageGRID en un solo sitio o en un grupo de sitios.

StorageGRID admite el uso de clústeres KMS. Cada clúster KMS contiene varios servidores de administración de claves replicados que comparten configuraciones y claves de cifrado. Se recomienda el uso de clústeres KMS para la administración de claves porque mejora las capacidades de conmutación por error de una configuración de alta disponibilidad.

Por ejemplo, supongamos que su sistema StorageGRID tiene tres sitios de centros de datos. Puede configurar un clúster KMS para proporcionar una clave a todos los nodos del dispositivo en el centro de datos 1 y un segundo clúster KMS para proporcionar una clave a todos los nodos del dispositivo en todos los demás sitios. Cuando agrega el segundo clúster KMS, puede configurar un KMS predeterminado para el Centro de datos 2 y el Centro de datos 3.

Tenga en cuenta que no puede usar un KMS para nodos que no sean dispositivos o para ningún nodo de dispositivo que no tuviera habilitada la configuración **Cifrado de nodo** durante la instalación.



¿Qué sucede cuando se gira una llave?

Como práctica recomendada de seguridad, debe realizar periódicamente ["rotar la clave de cifrado"](#) utilizado por cada KMS configurado.

Cuando la nueva versión de la clave esté disponible:

- Se distribuye automáticamente a los nodos del dispositivo cifrado en el sitio o sitios asociados con el KMS. La distribución debe ocurrir dentro de una hora después de que se gira la clave.
- Si el nodo del dispositivo cifrado está fuera de línea cuando se distribuye la nueva versión de la clave, el nodo recibirá la nueva clave tan pronto como se reinicie.
- Si por algún motivo no se puede usar la nueva versión de la clave para cifrar los volúmenes del dispositivo, se activa la alerta **Error en la rotación de la clave de cifrado KMS** para el nodo del dispositivo. Es posible que necesite ponerse en contacto con el soporte técnico para obtener ayuda para resolver esta alerta.

¿Puedo reutilizar un nodo de dispositivo después de haberlo cifrado?

Si necesita instalar un dispositivo cifrado en otro sistema StorageGRID , primero debe dismantelar el nodo de la red para mover los datos del objeto a otro nodo. Luego, puede utilizar el instalador del dispositivo StorageGRID para "[borrar la configuración de KMS](#)". Al borrar la configuración de KMS se deshabilita la configuración de **Cifrado de nodo** y se elimina la asociación entre el nodo del dispositivo y la configuración de KMS para el sitio StorageGRID .



Sin acceso a la clave de cifrado KMS, ya no se puede acceder a los datos que permanecen en el dispositivo y quedan bloqueados de forma permanente.

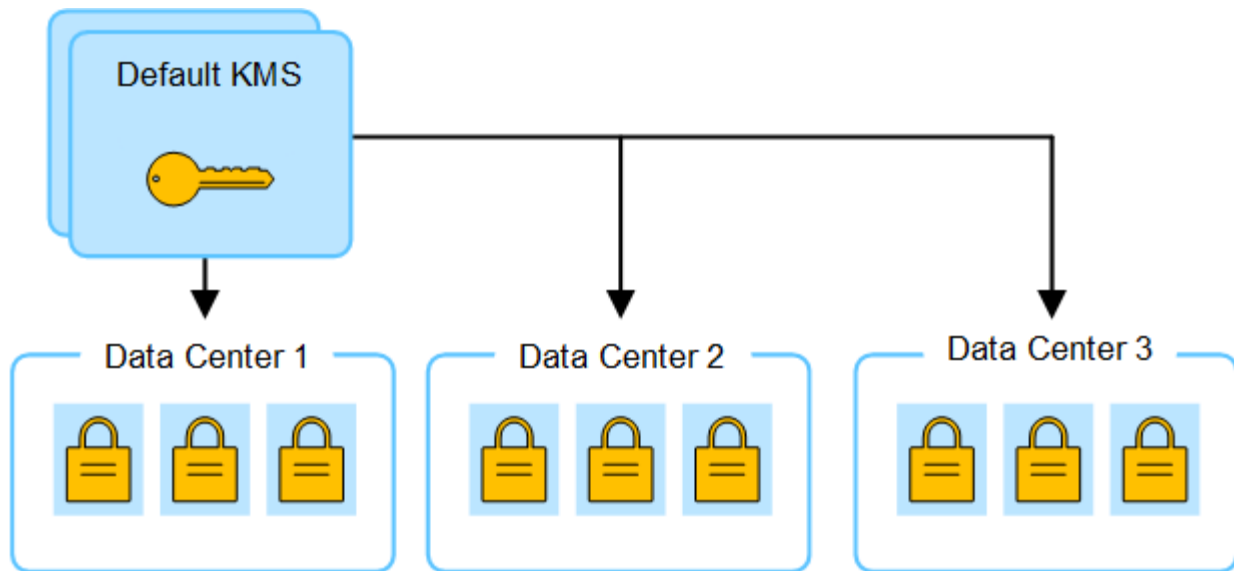
Consideraciones para cambiar el KMS de un sitio

Cada servidor de administración de claves (KMS) o clúster KMS proporciona una clave de cifrado a todos los nodos del dispositivo en un solo sitio o en un grupo de sitios. Si necesita cambiar el KMS que se utiliza para un sitio, es posible que deba copiar la clave de cifrado de un KMS a otro.

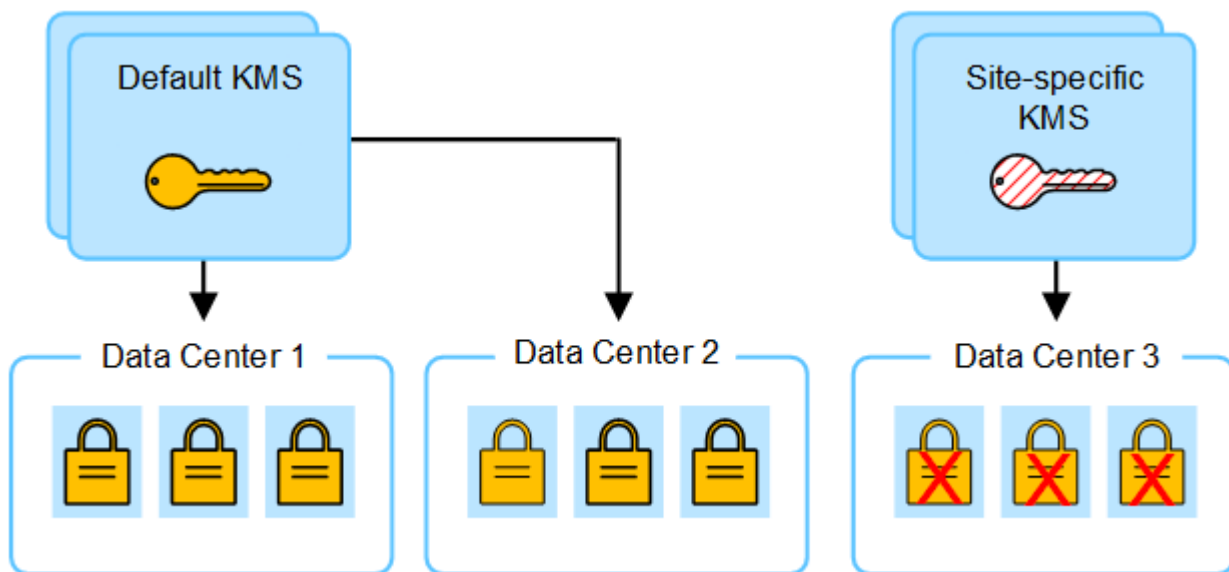
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo previamente cifrados en ese sitio se puedan descifrar usando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesites copiar la versión actual de la clave de cifrado del KMS original al nuevo KMS. Debe asegurarse de que el KMS tenga la clave correcta para descifrar los nodos del dispositivo cifrados en el sitio.

Por ejemplo:

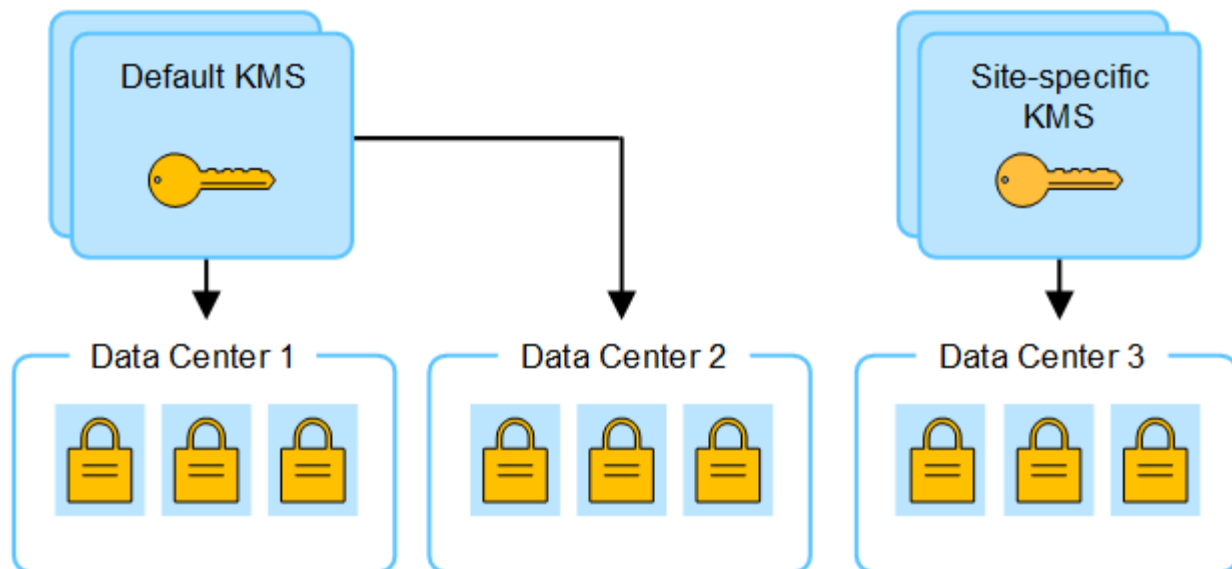
1. Inicialmente, configura un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos del dispositivo que tienen habilitada la configuración **Cifrado de nodo** se conectan al KMS y solicitan la clave de cifrado. Esta clave se utiliza para cifrar los nodos del dispositivo en todos los sitios. Esta misma clave también debe utilizarse para descifrar dichos dispositivos.



- Decide agregar un KMS específico del sitio para un sitio (Centro de datos 3 en la figura). Sin embargo, debido a que los nodos del dispositivo ya están cifrados, se produce un error de validación cuando intenta guardar la configuración del KMS específico del sitio. El error se produce porque el KMS específico del sitio no tiene la clave correcta para descifrar los nodos en ese sitio.



- Para solucionar el problema, copie la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. (Técnicamente, se copia la clave original a una nueva clave con el mismo alias. (La clave original se convierte en una versión anterior de la nueva clave). El KMS específico del sitio ahora tiene la clave correcta para descifrar los nodos del dispositivo en el Centro de datos 3, por lo que se puede guardar en StorageGRID.



Casos de uso para cambiar el KMS que se utiliza para un sitio

La tabla resume los pasos necesarios para los casos más comunes de cambio del KMS de un sitio.

Caso de uso para cambiar el KMS de un sitio	Pasos necesarios
Tiene una o más entradas KMS específicas del sitio y desea utilizar una de ellas como KMS predeterminado.	Editar el KMS específico del sitio. En el campo Administra claves para, seleccione Sitios no administrados por otro KMS (KMS predeterminado). El KMS específico del sitio ahora se utilizará como KMS predeterminado. Se aplicará a cualquier sitio que no tenga un KMS dedicado. "Editar un servidor de administración de claves (KMS)"
Tienes un KMS predeterminado y agregas un nuevo sitio en una expansión. No desea utilizar el KMS predeterminado para el nuevo sitio.	1. Si los nodos del dispositivo en el nuevo sitio ya fueron cifrados por el KMS predeterminado, use el software KMS para copiar la versión actual de la clave de cifrado del KMS predeterminado a un nuevo KMS. 2. Utilizando el Administrador de cuadrícula, agregue el nuevo KMS y seleccione el sitio. "Agregar un servidor de administración de claves (KMS)"
Desea que el KMS de un sitio utilice un servidor diferente.	1. Si los nodos del dispositivo en el sitio ya han sido cifrados por el KMS existente, utilice el software KMS para copiar la versión actual de la clave de cifrado del KMS existente al nuevo KMS. 2. Utilizando el Administrador de cuadrícula, edite la configuración KMS existente e ingrese el nuevo nombre de host o dirección IP. "Agregar un servidor de administración de claves (KMS)"

Configurar StorageGRID como cliente en el KMS

Debe configurar StorageGRID como cliente para cada servidor de administración de claves externo o clúster KMS antes de poder agregar el KMS a StorageGRID.



Estas instrucciones se aplican a Thales CipherTrust Manager y Hashicorp Vault. Para obtener una lista de productos y versiones compatibles, utilice el ["Herramienta de matriz de interoperabilidad de NetApp \(IMT\)"](#).

Pasos

1. Desde el software KMS, cree un cliente StorageGRID para cada KMS o clúster KMS que planee utilizar.

Cada KMS administra una única clave de cifrado para los nodos de dispositivos StorageGRID en un solo sitio o en un grupo de sitios.

2. Cree una clave utilizando uno de los dos métodos siguientes:
 - Utilice la página de administración de claves de su producto KMS. Cree una clave de cifrado AES para cada KMS o clúster KMS.

La clave de cifrado debe tener 2048 bits o más y debe ser exportable.

- Haga que StorageGRID cree la clave. Se le avisará cuando realice la prueba y guarde después ["cargando certificados de cliente"](#).

3. Registre la siguiente información para cada KMS o clúster KMS.

Necesita esta información cuando agrega el KMS a StorageGRID:

- Nombre de host o dirección IP para cada servidor.
- Puerto KMIP utilizado por el KMS.
- Alias de clave para la clave de cifrado en el KMS.

4. Para cada KMS o clúster KMS, obtenga un certificado de servidor firmado por una autoridad de certificación (CA) o un paquete de certificados que contenga cada uno de los archivos de certificado de CA codificados en 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 utilizar el formato X.509 codificado en Base-64 de correo de privacidad mejorada (PEM).
- El campo Nombre alternativo del sujeto (SAN) en cada certificado de servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP a la que se conectará StorageGRID.



Al configurar el KMS en StorageGRID, debe ingresar los mismos FQDN o direcciones IP en el campo **Nombre de host**.

- El certificado del servidor debe coincidir con el certificado utilizado por la interfaz KMIP del KMS, que normalmente utiliza el puerto 5696.

5. Obtenga el certificado de cliente público emitido a StorageGRID por el KMS externo y la clave privada para el certificado de cliente.

El certificado de cliente permite que StorageGRID se autentique ante el KMS.

Agregar un servidor de administración de claves (KMS)

Utilice el asistente del servidor de administración de claves StorageGRID para agregar cada KMS o clúster KMS.

Antes de empezar

- Usted ha revisado el ["Consideraciones y requisitos para utilizar un servidor de administración de claves"](#) .
- Tienes ["configuró StorageGRID como cliente en el KMS"](#) y tiene la información requerida para cada KMS o clúster KMS.
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .

Acerca de esta tarea

Si es posible, configure cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplique a todos los sitios no administrados por otro KMS. Si crea primero el KMS predeterminado, todos los dispositivos con nodos cifrados en la red se cifrarán con el KMS predeterminado. Si más adelante desea crear un KMS específico del sitio, primero debe copiar la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. Ver ["Consideraciones para cambiar el KMS de un sitio"](#) Para más detalles.

Paso 1: Detalles del KMS

En el Paso 1 (Detalles de KMS) del asistente Agregar un servidor de administración de claves, debe proporcionar detalles sobre el KMS o el clúster de KMS.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.

Aparece la página del servidor de administración de claves con la pestaña Detalles de configuración seleccionada.

2. Seleccione **Crear**.

Aparece el paso 1 (detalles de KMS) del asistente Agregar un servidor de administración de claves.

3. Ingrese la siguiente información para el KMS y el cliente StorageGRID que configuró en ese KMS.

Campo	Descripción
Nombre KMS	Un nombre descriptivo para ayudarlo a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	El alias de clave exacto para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Nota: Si no ha creado una clave con su producto KMS, se le solicitará que StorageGRID cree la clave.

Campo	Descripción
Administra claves para	El sitio StorageGRID que se asociará con este KMS. Si es posible, debe configurar cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplique a todos los sitios no administrados por otro KMS. • Seleccione un sitio si este KMS administrará claves de cifrado para los nodos del dispositivo en un sitio específico. • Seleccione Sitios no administrados 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 agregue en expansiones posteriores. Nota: Se producirá un error de validación cuando guarde la configuración de KMS si selecciona un sitio que anteriormente fue cifrado por el KMS predeterminado pero no proporcionó la versión actual de la clave de cifrado original al nuevo KMS.
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar KMIP.
Nombre de host	El nombre de dominio completo o la dirección IP para el KMS. Nota: El campo Nombre alternativo del sujeto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que ingrese aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor en el clúster.
5. Seleccione **Continuar**.

Paso 2: Cargar el certificado del servidor

En el paso 2 (Cargar certificado de servidor) del asistente Agregar un servidor de administración de claves, cargue el certificado de servidor (o paquete de certificados) para el KMS. El certificado del servidor permite que el KMS externo se autentique en StorageGRID.

Pasos

1. Desde el **Paso 2 (Cargar certificado de servidor)**, busque la ubicación del certificado de servidor o paquete de certificados guardado.
2. Subir el archivo del certificado.

Aparecen los metadatos del certificado del servidor.



Si cargó un paquete de certificados, los metadatos de cada certificado aparecen en su propia pestaña.

3. Seleccione **Continuar**.

Paso 3: Cargar certificados de cliente

En el paso 3 (Cargar certificados de cliente) del asistente Agregar un servidor de administración de claves, cargue 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. Desde el **Paso 3 (Cargar certificados de cliente)**, busque la ubicación del certificado de cliente.
2. Subir el archivo del certificado del cliente.

Aparecen los metadatos del certificado del cliente.

3. Busque la ubicación de la clave privada para el certificado del cliente.
4. Sube el archivo de clave privada.
5. Seleccione **Probar y guardar**.

Si no existe una clave, se le solicitará que StorageGRID cree una.

Se prueban las conexiones entre el servidor de administración 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 administración de claves se agrega a la tabla en la página Servidor de administración de claves.



Inmediatamente después de agregar un KMS, el estado del certificado en la página del Servidor de administración de claves aparece como Desconocido. StorageGRID podría tardar hasta 30 minutos en obtener el estado real de cada certificado. Debe actualizar su navegador web para ver el estado actual.

6. Si aparece un mensaje de error al seleccionar **Probar y guardar**, revise los detalles del mensaje y luego seleccione **Aceptar**.

Por ejemplo, es posible que reciba un error 422: Entidad no procesable si falla una prueba de conexión.

7. Si necesita guardar la configuración actual sin probar la conexión externa, seleccione **Forzar guardado**.



Al seleccionar **Forzar guardado** se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos del dispositivo que tengan el cifrado de nodo habilitado en el sitio afectado. Podría perder el acceso a sus datos hasta que se resuelvan los problemas.

8. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.

Se guarda la configuración del KMS pero no se prueba la conexión al KMS.

Administrar un KMS

Administrar un servidor de administración de claves (KMS) implica ver o editar detalles, administrar certificados, ver nodos cifrados y eliminar un KMS cuando ya no es

necesario.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["permiso de acceso requerido"](#).

Ver detalles de KMS

Puede ver información sobre cada servidor de administración de claves (KMS) en su sistema StorageGRID, incluidos los detalles de la clave y el estado actual de los certificados del servidor y del cliente.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.

Aparece la página del servidor de administración de claves y muestra la siguiente información:

- La pestaña Detalles de configuración enumera todos los servidores de administración de claves que están configurados.
 - La pestaña Nodos cifrados enumera todos los nodos que tienen el cifrado de nodo habilitado.
2. Para ver los detalles de un KMS específico y realizar operaciones en ese KMS, seleccione el nombre del KMS. La página de detalles del KMS enumera la siguiente información:

Campo	Descripción
Administra claves para	El sitio StorageGRID asociado con el KMS. Este campo muestra el nombre de un sitio StorageGRID específico o Sitios no administrados por otro KMS (KMS predeterminado) .
Nombre de host	El nombre de dominio completo o la dirección IP del KMS. Si hay un clúster de dos servidores de administración de claves, se enumeran el nombre de dominio completo o la dirección IP de ambos servidores. Si hay más de dos servidores de administración de claves en un clúster, se incluye el nombre de dominio completo o la dirección IP del primer KMS junto con la cantidad de servidores de administración de claves adicionales en el clúster. Por ejemplo: 10.10.10.10 and 10.10.10.11 o 10.10.10.10 and 2 others . Para ver todos los nombres de host en un clúster, seleccione un KMS y seleccione Editar o Acciones > Editar .

3. Seleccione una pestaña en la página de detalles de KMS para ver la siguiente información:

Pestaña	Campo	Descripción
Detalles clave	Nombre de la clave	El alias de clave para el cliente StorageGRID en el KMS.

Pestaña	Campo	Descripción
UID de clave	El identificador único de la última versión de la clave.	Última modificación
La fecha y hora de la última versión de la clave.	Certificado de servidor	Metadatos
Los metadatos del certificado, como el número de serie, la fecha y hora de vencimiento y el PEM del certificado.	Certificado PEM	El contenido del archivo PEM (correo con privacidad mejorada) del certificado.
Certificado de cliente	Metadatos	Los metadatos del certificado, como el número de serie, la fecha y hora de vencimiento y el PEM del certificado.

4. Con la frecuencia que requieran las prácticas de seguridad de su organización, seleccione **Rotar clave** o utilice el software KMS para crear una nueva versión de la clave.

Cuando la rotación de clave es exitosa, se actualizan los campos UID de clave y Última modificación.



Si rota la clave de cifrado utilizando el software KMS, rótele desde la última versión utilizada de la clave a una nueva versión de la misma clave. No gire a una clave completamente diferente.

Nunca intente rotar una clave cambiando el nombre de la clave (alias) para el KMS. StorageGRID requiere que todas las versiones de clave utilizadas anteriormente (así como cualquier versión futura) sean accesibles desde el KMS con el mismo alias de clave. Si cambia el alias de clave de un KMS configurado, es posible que StorageGRID no pueda descifrar sus datos.

Administrar certificados

Aborde rápidamente cualquier problema con el certificado del servidor o del cliente. Si es posible, reemplace los certificados antes de que caduquen.



Debe abordar cualquier problema de certificado lo antes posible para mantener el acceso a los datos.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.
2. En la tabla, observe el valor de vencimiento del certificado para cada KMS.
3. Si la expiración del certificado para cualquier KMS es desconocida, espere hasta 30 minutos y luego actualice su navegador web.
4. Si la columna Vencimiento del certificado indica que un certificado ha vencido o está próximo a vencer,

seleccione el KMS para ir a la página de detalles del KMS.

- a. Seleccione **Certificado de servidor** y verifique el valor del campo "Vence el".
 - b. Para reemplazar el certificado, seleccione **Editar certificado** para cargar un nuevo certificado.
 - c. Repita estos subpasos y seleccione **Certificado de cliente** en lugar de Certificado de servidor.
5. Cuando se activan las alertas **Expiración del certificado de CA de KMS**, **Expiración del certificado de cliente de KMS** y **Expiración del certificado de servidor de KMS**, tenga en cuenta la descripción de cada alerta y realice las acciones recomendadas.

StorageGRID podría tardar hasta 30 minutos en obtener actualizaciones sobre la expiración del certificado. Actualice su navegador web para ver los valores actuales.



Si obtiene un estado de **El estado del certificado del servidor es desconocido**, asegúrese de que su KMS permita obtener un certificado de servidor sin requerir un certificado de cliente.

Ver nodos cifrados

Puede ver información sobre los nodos del dispositivo en su sistema StorageGRID que tienen habilitada la configuración **Cifrado de nodo**.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.

Aparece la página del Servidor de administración de claves. La pestaña Detalles de configuración muestra todos los servidores de administración de claves que se han configurado.

2. Desde la parte superior de la página, seleccione la pestaña **Nodos cifrados**.

La pestaña Nodos cifrados enumera los nodos del dispositivo en su sistema StorageGRID que tienen habilitada la configuración **Cifrado de nodo**.

3. Revise la información en la tabla para cada nodo del dispositivo.

Columna	Descripción
Nombre del nodo	El nombre del nodo del dispositivo.
Tipo de nodo	El tipo de nodo: Almacenamiento, Administración o Puerta de enlace.
Sitio	El nombre del sitio StorageGRID donde está instalado el nodo.
Nombre KMS	El nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS, seleccione la pestaña Detalles de configuración para agregar un KMS. "Agregar un servidor de administración de claves (KMS)"

Columna	Descripción
UID de clave	El identificador único de la clave de cifrado utilizada para cifrar y descifrar datos en el nodo del dispositivo. Para ver un UID de clave completo, seleccione el texto. Un guion (--) indica que el UID de la clave es desconocido, posiblemente debido a un problema de conexión entre el nodo del dispositivo 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. El estado de la conexión puede tardar varios minutos en actualizarse después de los cambios de configuración de KMS. Nota: Actualice su navegador web para ver los nuevos valores.

4. Si la columna Estado indica un problema de KMS, solucione el problema de inmediato.

Durante las operaciones normales de KMS, el estado será **Conectado a KMS**. Si un nodo se desconecta de la red, se muestra el estado de conexión del nodo (Administrativamente inactivo o Desconocido).

Otros mensajes de estado corresponden a alertas de StorageGRID con los mismos nombres:

- La configuración de KMS no se pudo cargar
- Error de conectividad KMS
- No se encontró el nombre de la clave de cifrado KMS
- Error en la rotación de la clave de cifrado KMS
- La clave KMS no pudo descifrar un volumen del dispositivo
- KMS no está configurado

Realice las acciones recomendadas para estas alertas.



Debe abordar cualquier problema de inmediato para garantizar que sus datos estén completamente protegidos.

Editar un KMS

Es posible que necesite editar la configuración de un servidor de administración de claves, por ejemplo, si un certificado está a punto de caducar.

Antes de empezar

- Si planea actualizar el sitio seleccionado para un KMS, ha revisado el ["Consideraciones para cambiar el KMS de un sitio"](#).
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.

Aparece la página del servidor de administración de claves y muestra todos los servidores de administración de claves que se han configurado.

2. Seleccione el KMS que desea editar y seleccione **Acciones > Editar**.

También puede editar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Editar** en la página de detalles del KMS.

3. Opcionalmente, actualice los detalles en el **Paso 1 (detalles de KMS)** del asistente Editar un servidor de administración de claves.

Campo	Descripción
Nombre KMS	Un nombre descriptivo para ayudarle a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	El alias de clave exacto para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Solo es necesario editar el nombre de la clave en casos excepcionales. Por ejemplo, debe editar el nombre de la clave si se cambia el nombre del alias en el KMS o si se han copiado todas las versiones de la clave anterior al historial de versiones del nuevo alias.
Administra claves para	Si está editando un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione opcionalmente Sitios no administrados por otro KMS (KMS predeterminado). Esta selección convierte un KMS específico del sitio en el KMS predeterminado, que se aplicará a todos los sitios que no tengan un KMS dedicado y a cualquier sitio agregado en una expansión. Nota: Si está editando un KMS específico del sitio, no podrá seleccionar otro sitio. Si está editando el KMS predeterminado, no podrá seleccionar un sitio específico.
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar KMIP.
Nombre de host	El nombre de dominio completo o la dirección IP para el KMS. Nota: El campo Nombre alternativo del sujeto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que ingrese aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor en el clúster.
5. Seleccione **Continuar**.

Aparece el paso 2 (Cargar certificado de servidor) del asistente Editar un servidor de administración de claves.

6. Si necesita reemplazar el certificado del servidor, seleccione **Explorar** y cargue el nuevo archivo.

7. Seleccione **Continuar**.

Aparece el paso 3 (Cargar certificados de cliente) del asistente Editar un servidor de administración de claves.

8. Si necesita reemplazar el certificado del cliente y la clave privada del certificado del cliente, seleccione **Explorar** y cargue los nuevos archivos.

9. Seleccione **Probar y guardar**.

Se prueban las conexiones entre el servidor de administración de claves y todos los nodos del dispositivo cifrados en los sitios afectados. Si todas las conexiones de nodo son válidas y se encuentra la clave correcta en el KMS, el servidor de administración de claves se agrega a la tabla en la página Servidor de administración de claves.

10. Si aparece un mensaje de error, revise los detalles del mensaje y seleccione **Aceptar**.

Por ejemplo, es posible que reciba un error 422: Entidad no procesable si el sitio que seleccionó para este KMS ya está administrado por otro KMS o si falló una prueba de conexión.

11. Si necesita guardar la configuración actual antes de resolver los errores de conexión, seleccione **Forzar guardado**.



Al seleccionar **Forzar guardado** se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos del dispositivo que tengan el cifrado de nodo habilitado en el sitio afectado. Podría perder el acceso a sus datos hasta que se resuelvan los problemas.

Se guarda la configuración de KMS.

12. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.

Se guarda la configuración del KMS, pero no se prueba la conexión al KMS.

Eliminar un servidor de administración de claves (KMS)

Es posible que en algunos casos desees eliminar un servidor de administración de claves. Por ejemplo, es posible que desees eliminar un KMS específico del sitio si has dado de baja el sitio.

Antes de empezar

- Usted ha revisado el ["Consideraciones y requisitos para utilizar un servidor de administración de claves"](#).
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).

Acerca de esta tarea

Puedes eliminar un KMS en estos casos:

- Puede eliminar un KMS específico del sitio si el sitio se ha dado de baja o si no incluye nodos de dispositivos con cifrado de nodos habilitado.

- Puede eliminar el KMS predeterminado si ya existe un KMS específico del sitio para cada sitio que tenga nodos de dispositivo con cifrado de nodo habilitado.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.

Aparece la página del servidor de administración de claves y muestra todos los servidores de administración de claves que se han configurado.

2. Seleccione el KMS que desea eliminar y seleccione **Acciones > Eliminar**.

También puede eliminar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Eliminar** en la página de detalles del KMS.

3. Confirme que lo siguiente es verdadero:

- Está eliminando un KMS específico del sitio para un sitio que no tiene ningún nodo de dispositivo con cifrado de nodo habilitado.
- Está eliminando el KMS predeterminado, pero ya existe un KMS específico del sitio para cada sitio con cifrado de nodo.

4. Seleccione **Sí**.

Se elimina la configuración de KMS.

Administrar la configuración del proxy

Configurar el proxy de almacenamiento

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



Las configuraciones del proxy de almacenamiento configuradas no se aplican a los puntos finales de los servicios de la plataforma Kafka.

Antes de empezar

- Tienes ["permisos de acceso específicos"](#).
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).

Acerca de esta tarea

Puede configurar los ajustes para un único proxy de almacenamiento.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Configuración de proxy**.
2. En la pestaña **Almacenamiento**, seleccione la casilla de verificación **Habilitar proxy de almacenamiento**.
3. Seleccione el protocolo para el proxy de almacenamiento.

4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Opcionalmente, ingrese el puerto utilizado para conectarse al servidor proxy.

Deje este campo en blanco para utilizar el puerto predeterminado para el protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Seleccione **Guardar**.

Una vez guardado el proxy de almacenamiento, se pueden configurar y probar nuevos puntos finales para los servicios de la plataforma o los grupos de almacenamiento en la nube.



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

7. Verifique la configuración de su servidor proxy para asegurarse de que los mensajes relacionados con el servicio de la plataforma de StorageGRID no se bloqueen.
8. Si necesita deshabilitar un proxy de almacenamiento, desmarque la casilla de verificación y seleccione **Guardar**.

Configurar los ajustes del proxy de administración

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

Para obtener más información sobre AutoSupport, consulte ["Configurar AutoSupport"](#).

Antes de empezar

- Tienes ["permisos de acceso específicos"](#).
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).

Acerca de esta tarea

Puede configurar los ajustes para un solo proxy de administrador.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Configuración de proxy**.

Aparece la página Configuración de proxy. De forma predeterminada, Almacenamiento está seleccionado en el menú de pestañas.

2. Seleccione la pestaña **Admin**.
3. Seleccione la casilla de verificación **Habilitar proxy de administración**.
4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Introduzca el puerto utilizado para conectarse al servidor proxy.
6. Opcionalmente, ingrese un nombre de usuario y una contraseña para el servidor proxy.

Deje estos campos en blanco si su servidor proxy no requiere un nombre de usuario o una contraseña.

7. Seleccione una de las siguientes opciones:

- Si desea proteger la conexión al proxy de administración, seleccione **Verificar certificado de proxy**.

Cargue un paquete de CA para verificar la autenticidad de los certificados SSL presentados por el servidor proxy de administración.



AutoSupport on Demand, E-Series AutoSupport a través de StorageGRID y la determinación de ruta de actualización en la página Actualización de StorageGRID no funcionarán si se verifica un certificado de proxy.

Después de cargar el paquete de CA, aparecen sus metadatos.

- Si no desea validar certificados al comunicarse con el servidor proxy de administración, seleccione **No verificar certificado proxy**.

8. Seleccione **Guardar**.

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



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

9. Si necesita deshabilitar el proxy de administración, desmarque la casilla **Habilitar proxy de administración** y luego seleccione **Guardar**.

Controlar cortafuegos

Controlar el acceso al firewall externo

Puede abrir o cerrar puertos específicos en el firewall externo.

Puede controlar el acceso a las interfaces de usuario y las API en los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en el firewall externo. Por ejemplo, es posible que desee evitar que los inquilinos puedan conectarse al Grid Manager en el firewall, además de utilizar otros métodos para controlar el acceso al sistema.

Si desea configurar el firewall interno de StorageGRID, consulte ["Configurar el firewall interno"](#).

Puerto	Descripción	Si el puerto está abierto...
443	Puerto HTTPS predeterminado para nodos de administración	Los navegadores web y los clientes de API de administración pueden acceder al Administrador de Grid, la API de administración de Grid, el Administrador de inquilinos y la API de administración de inquilinos. Nota: El puerto 443 también se utiliza para cierto tráfico interno.

Puerto	Descripción	Si el puerto está abierto...
8443	Puerto de Grid Manager restringido en los nodos de administración	• Los navegadores web y los clientes de API de administración pueden acceder al Administrador de Grid y a la API de administración de Grid mediante HTTPS. • Los navegadores web y los clientes de API de administración no pueden acceder al Administrador de inquilinos ni a la API de administración de inquilinos. • Las solicitudes de contenido interno serán rechazadas.
9443	Puerto de administrador de inquilinos restringido en nodos de administración	• Los navegadores web y los clientes de API de administración pueden acceder al Administrador de inquilinos y a la API de administración de inquilinos mediante HTTPS. • Los navegadores web y los clientes de API de administración no pueden acceder al Administrador de Grid ni a la API de administración de Grid. • Las solicitudes de contenido interno serán rechazadas.



El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autenticuen con inicio de sesión único.

Información relacionada

- ["Sign in en el Administrador de cuadrícula"](#)
- ["Crear una cuenta de inquilino"](#)
- ["Comunicaciones externas"](#)

Administrar los controles internos del firewall

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad de su red al permitirle controlar el acceso de la red al nodo. Utilice el firewall para evitar el acceso a la red en todos los puertos excepto aquellos necesarios para su implementación de red específica. Los cambios de configuración que realice en la página de control del Firewall se implementarán en cada nodo.

Utilice las tres pestañas de la página de control de Firewall para personalizar el acceso que necesita para su red.

- **Lista de direcciones privilegiadas:** utilice esta pestaña para permitir el acceso seleccionado a puertos cerrados. Puede agregar direcciones IP o subredes en notación CIDR que puedan acceder a puertos cerrados mediante la pestaña Administrar acceso externo.
- **Administrar acceso externo:** utilice esta pestaña para cerrar puertos que están abiertos de forma

predeterminada o reabrir puertos previamente cerrados.

- **Red de cliente no confiable:** utilice esta pestaña para especificar si un nodo confía en el tráfico entrante de la red de cliente.

La configuración de esta pestaña anula la configuración de la pestaña Administrar acceso externo.

- Un nodo con una red de cliente no confiable solo aceptará conexiones en los puertos de punto final del balanceador de carga configurados en ese nodo (puntos finales globales, de interfaz de nodo y enlazados al tipo de nodo).
- Los puertos finales del equilibrador de carga *son los únicos puertos abiertos* en redes de cliente que no son de confianza, independientemente de la configuración en la pestaña Administrar redes externas.
- Cuando es confiable, todos los puertos abiertos en la pestaña Administrar acceso externo son accesibles, así como también cualquier punto final del balanceador de carga abierto en la red del cliente.



Las configuraciones que realice en una pestaña pueden afectar los cambios de acceso que realice en otra pestaña. Asegúrese de verificar la configuración en todas las pestañas para asegurarse de que su red se comporte de la manera esperada.

Para configurar los controles internos del firewall, consulte ["Configurar los controles del firewall"](#) .

Para obtener más información sobre firewalls externos y seguridad de red, consulte ["Controlar el acceso al firewall externo"](#) .

Lista de direcciones privilegiadas y pestañas para administrar acceso externo

La pestaña Lista de direcciones privilegiadas le permite registrar una o más direcciones IP a las que se les concede acceso a los puertos de la red que están cerrados. La pestaña Administrar acceso externo le permite cerrar el acceso externo a puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son puertos a los que pueden acceder los nodos que no pertenecen a la red de manera predeterminada). Estas dos pestañas a menudo se pueden usar juntas para personalizar el acceso de red exacto que necesita permitir para su red.



Las direcciones IP privilegiadas no tienen acceso al puerto de la red interna de forma predeterminada.

Ejemplo 1: Utilizar un host de salto para tareas de mantenimiento

Supongamos que desea utilizar un host de salto (un host con seguridad reforzada) para la administración de la red. Podrías utilizar estos pasos generales:

1. Utilice la pestaña Lista de direcciones privilegiadas para agregar la dirección IP del host de salto.
2. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos.



Agregue la dirección IP privilegiada antes de bloquear los puertos 443 y 8443. Cualquier usuario actualmente conectado a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas.

Después de guardar su configuración, todos los puertos externos en el nodo de administración de su red se bloquearán para todos los hosts excepto el host de salto. Luego, puede utilizar el host de salto para realizar

tareas de mantenimiento en su red de forma más segura.

Ejemplo 2: Bloquear puertos sensibles

Supongamos que desea bloquear puertos sensibles y el servicio en ese puerto (por ejemplo, SSH en el puerto 22). Podrías utilizar los siguientes pasos generales:

1. Utilice la pestaña Lista de direcciones privilegiadas para otorgar acceso solo a los hosts que necesitan acceso al servicio.
2. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos.



Agregue la dirección IP privilegiada antes de bloquear el acceso a cualquier puerto asignado para acceder a Grid Manager y al administrador de inquilinos (los puertos preestablecidos son 443 y 8443). Cualquier usuario actualmente conectado a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas.

Después de guardar su configuración, el puerto 22 y el servicio SSH 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 de qué interfaz provenga la solicitud.

Ejemplo 3: Deshabilitar el acceso a servicios no utilizados

A nivel de red, podrías deshabilitar algunos servicios que no desees utilizar. Por ejemplo, para bloquear el tráfico del cliente HTTP S3, deberá utilizar el interruptor en la pestaña Administrar acceso externo para bloquear el puerto 18084.

Pestaña Redes de clientes no confiables

Si utiliza una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles al aceptar tráfico de cliente entrante solo en puntos finales configurados explícitamente.

De forma predeterminada, la red de cliente en cada nodo de la red es *confiable*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de la red en todos los ["puertos externos disponibles"](#).

Puede reducir la amenaza de ataques hostiles en su sistema StorageGRID especificando que la red de cliente en cada nodo sea *no confiable*. Si la red de cliente de un nodo no es confiable, el nodo solo acepta conexiones entrantes en puertos configurados explícitamente como puntos finales del balanceador de carga. Ver ["Configurar los puntos finales del balanceador de carga"](#) y ["Configurar los controles del firewall"](#).

Ejemplo 1: El nodo de puerta de enlace solo acepta solicitudes HTTPS S3

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

1. Desde ["Puntos finales del balanceador de carga"](#) página, configure un punto final de balanceador de carga para S3 sobre HTTPS en el puerto 443.
2. Desde la página de control de Firewall, seleccione No confiable para especificar que la red de cliente en el nodo de puerta de enlace no es confiable.

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

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

Supongamos que desea habilitar el tráfico saliente de servicios de la plataforma S3 desde un nodo de almacenamiento, pero desea evitar cualquier conexión entrante a ese nodo de almacenamiento en la red del cliente. Realizarías este paso general:

- Desde la pestaña Redes de clientes no confiables de la página de control de Firewall, indique que la red de clientes en el nodo de almacenamiento no es confiable.

Después de guardar su configuración, el nodo de almacenamiento ya no acepta tráfico entrante en la red del cliente, pero continúa permitiendo solicitudes salientes a los destinos de servicios de plataforma configurados.

Ejemplo 3: Limitar el acceso a Grid Manager a una subred

Supongamos que desea permitir el acceso a Grid Manager solo en una subred específica. Realizarías los siguientes pasos:

1. Conecte la red de cliente de sus nodos de administración a la subred.
2. Utilice la pestaña Red de cliente no confiable para configurar la red de cliente como no confiable.
3. Cuando crea un punto final de balanceador de carga de interfaz de administración, ingrese el puerto y seleccione la interfaz de administración a la que accederá el puerto.
4. Seleccione **Sí** para Red de cliente no confiable.
5. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos externos (con o sin direcciones IP privilegiadas configuradas para hosts fuera de esa subred).

Después de guardar su configuración, solo los hosts en la subred que especificó podrán acceder al Administrador de Grid. Todos los demás hosts están bloqueados.

Configurar el firewall interno

Puede configurar el firewall de StorageGRID para controlar el acceso de red a puertos específicos en sus nodos de StorageGRID .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Has revisado la información en ["Administrar los controles del firewall"](#) y ["Pautas para establecer redes"](#) .
- Si desea que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante solo en puntos finales configurados explícitamente, debe definir los puntos finales del equilibrador de carga.



Al cambiar la configuración de la red del cliente, las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Acerca de esta tarea

StorageGRID incluye un firewall interno en cada nodo que le permite abrir o cerrar algunos de los puertos en los nodos de su red. Puede utilizar las pestañas de control de Firewall para abrir o cerrar puertos que están abiertos de manera predeterminada en la red de cuadrícula, la red de administración y la red de cliente. También puede crear una lista de direcciones IP privilegiadas que pueden acceder a los puertos de la red que están cerrados. Si está utilizando una red de cliente, puede especificar si un nodo confía en el tráfico entrante de la red de cliente y puede configurar el acceso a puertos específicos en la red de cliente.

Limitar la cantidad de puertos abiertos a direcciones IP fuera de su red a solo aquellos que sean absolutamente necesarios mejora la seguridad de su red. Utilice la configuración de cada una de las tres pestañas de control del Firewall para asegurarse de que solo los puertos necesarios estén abiertos.

Para obtener más información sobre el uso de los controles de firewall, incluidos ejemplos, consulte ["Administrar los controles del firewall"](#) .

Para obtener más información sobre firewalls externos y seguridad de red, consulte ["Controlar el acceso al firewall externo"](#) .

Controles de firewall de acceso

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Control de firewall**.

Las tres pestañas de esta página se describen en ["Administrar los controles del firewall"](#) .

2. Seleccione cualquier pestaña para configurar los controles del firewall.

Puede utilizar estas pestañas en cualquier orden. Las configuraciones que establezca en una pestaña no limitan lo que puede hacer en las otras pestañas; sin embargo, los cambios de configuración que realice en una pestaña podrían cambiar el comportamiento de los puertos configurados en otras pestañas.

Lista de direcciones privilegiadas

Utilice la pestaña Lista de direcciones privilegiadas para otorgar a los hosts acceso a puertos que están cerrados de manera predeterminada o cerrados por la configuración de la pestaña Administrar acceso externo.

Las direcciones IP y subredes privilegiadas no tienen acceso a la red interna de forma predeterminada. Además, los puntos finales del balanceador de carga y los puertos adicionales abiertos en la pestaña Lista de direcciones privilegiadas son accesibles incluso si están bloqueados en la pestaña Administrar acceso externo.



Las configuraciones en la pestaña Lista de direcciones privilegiadas no pueden anular las configuraciones en la pestaña Red de cliente no confiable.

Pasos

1. En la pestaña Lista de direcciones privilegiadas, ingrese la dirección o subred IP a la que desea otorgar acceso a los puertos cerrados.
2. Opcionalmente, seleccione **Agregar otra dirección IP o subred en notación CIDR** para agregar clientes privilegiados adicionales.



Agregue la menor cantidad posible de direcciones a la lista privilegiada.

3. Opcionalmente, seleccione ***Permitir que las direcciones IP privilegiadas accedan a los puertos internos de StorageGRID ***. Ver ["Puertos internos de StorageGRID"](#) .



Esta opción elimina algunas protecciones para los servicios internos. Déjelo deshabilitado si es posible.

4. Seleccione **Guardar**.

Gestionar el acceso externo

Cuando se cierra un puerto en la pestaña Administrar acceso externo, ninguna dirección IP que no sea de la red podrá acceder al puerto a menos que agregue la dirección IP a la lista de direcciones privilegiadas. Solo puedes cerrar puertos que estén abiertos de forma predeterminada y solo puedes abrir puertos que hayas cerrado.



Las configuraciones en la pestaña Administrar acceso externo no pueden anular las configuraciones en la pestaña Red de cliente no confiable. Por ejemplo, si un nodo no es confiable, el puerto SSH/22 se bloquea en la red del cliente incluso si está abierto en la pestaña Administrar acceso externo. Las configuraciones en la pestaña Red de cliente no confiable anulan los puertos cerrados (como 443, 8443, 9443) en la red del cliente.

Pasos

1. Seleccione **Administrar acceso externo**. La pestaña muestra una tabla con todos los puertos externos (puertos a los que pueden acceder los nodos que no pertenecen a la red de manera predeterminada) para los nodos de su red.
2. Configure los puertos que desea abrir y cerrar utilizando las siguientes opciones:
 - Utilice el interruptor junto a cada puerto para abrir o cerrar el puerto seleccionado.
 - Seleccione **Abrir todos los puertos mostrados** para abrir todos los puertos enumerados en la tabla.
 - Seleccione **Cerrar todos los puertos mostrados** para cerrar todos los puertos enumerados en la tabla.



Si cierra los puertos 443 o 8443 de Grid Manager, todos los usuarios que estén conectados actualmente en un puerto bloqueado, incluido usted, perderán el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas.



Utilice la barra de desplazamiento en el lado derecho de la tabla para asegurarse de haber visto todos los puertos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier puerto externo ingresando un número de puerto. Puede ingresar un número de puerto parcial. Por ejemplo, si ingresa un **2**, se mostrarán todos los puertos que tengan la cadena "2" como parte de su nombre.

3. Seleccione **Guardar**

Red de clientes no confiables

Si la red de cliente de un nodo no es confiable, el nodo solo acepta tráfico entrante en los puertos configurados como puntos finales del balanceador de carga y, opcionalmente, puertos adicionales que seleccione en esta pestaña. También puede utilizar esta pestaña para especificar la configuración predeterminada para los nuevos nodos agregados en una expansión.



Las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Los cambios de configuración que realice en la pestaña **Red de cliente no confiable** anulan las configuraciones de la pestaña **Administrar acceso externo**.

Pasos

1. Seleccione **Red de cliente no confiable**.
2. En la sección Establecer nuevo nodo predeterminado, especifique cuál debe ser la configuración predeterminada cuando se agregan nuevos nodos a la cuadrícula en un procedimiento de expansión.
 - **Confiable** (predeterminado): cuando se agrega un nodo en una expansión, su red de cliente es confiable.
 - **No confiable**: cuando se agrega un nodo en una expansión, su red de cliente no es confiable.

Según sea necesario, puede regresar a esta pestaña para cambiar la configuración de un nuevo nodo específico.



Esta configuración no afecta a los nodos existentes en su sistema StorageGRID .

3. Utilice las siguientes opciones para seleccionar los nodos que deben permitir conexiones de clientes solo en puntos finales del balanceador de carga configurados explícitamente o en puertos seleccionados adicionales:
 - Seleccione **No confiar en los nodos mostrados** para agregar todos los nodos que se muestran en la tabla a la lista de Red de clientes no confiables.
 - Seleccione **Confiar en los nodos mostrados** para eliminar todos los nodos que se muestran en la tabla de la lista Red de clientes no confiables.
 - Utilice el interruptor junto a cada nodo para configurar la red del cliente como confiable o no confiable para el nodo seleccionado.

Por ejemplo, puede seleccionar **No confiar en los nodos mostrados** para agregar todos los nodos a la lista de Red de clientes no confiables y luego usar el botón junto a un nodo individual para agregar ese único nodo a la lista de Red de clientes confiables.



Utilice la barra de desplazamiento en el lado derecho de la tabla para asegurarse de haber visto todos los nodos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier nodo ingresando el nombre del nodo. Puede introducir un nombre parcial. Por ejemplo, si ingresa un **GW**, se mostrarán todos los nodos que tengan la cadena "GW" como parte de su nombre.

4. Seleccione **Guardar**.

La nueva configuración del firewall se aplica y se ejecuta de inmediato. Las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Administrar inquilinos

¿Qué son las cuentas de inquilinos?

Una cuenta de inquilino le permite utilizar la API REST de Simple Storage Service (S3) para almacenar y recuperar objetos en un sistema StorageGRID .



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["StorageGRID 11.8: Administrar inquilinos"](#) .

Como administrador de la red, usted crea y administra las cuentas de inquilino que los clientes S3 usan para

almacenar y recuperar objetos.

Cada cuenta de inquilino tiene grupos federados o locales, usuarios, depósitos S3 y objetos.

Las cuentas de inquilino se pueden utilizar para segregar objetos almacenados por diferentes entidades. Por ejemplo, se pueden utilizar varias cuentas de inquilino para cualquiera de estos casos de uso:

- **Caso de uso empresarial:** si está administrando un sistema StorageGRID en una aplicación empresarial, es posible que desee segregar el almacenamiento de objetos de la red por los diferentes departamentos de su organización. En este caso, podría crear cuentas de inquilino para el departamento de Marketing, el departamento de Atención al Cliente, el departamento de Recursos Humanos, etc.



Si utiliza el protocolo de cliente S3, puede usar depósitos S3 y políticas de depósitos para segregar objetos entre los departamentos de una empresa. No es necesario utilizar cuentas de inquilino. Consulte las instrucciones para la implementación "[Cubos S3 y políticas de cubos](#)" Para más información.

- **Caso de uso de proveedor de servicios:** Si administra un sistema StorageGRID como proveedor de servicios, puede segregar el almacenamiento de objetos de la red por las diferentes entidades que alquilarán el almacenamiento en su red. En este caso, crearía cuentas de inquilino para la Empresa A, la Empresa B, la Empresa C, etc.

Para obtener más información, consulte "[Utilice una cuenta de inquilino](#)".

¿Cómo creo una cuenta de inquilino?

Utilice el administrador de Grid para crear una cuenta de inquilino. Al crear una cuenta de inquilino, se especifica la siguiente información:

- Información básica que incluye el nombre del inquilino, el tipo de cliente (S3) y la cuota de almacenamiento opcional.
- Permisos para la cuenta de inquilino, como si la cuenta de inquilino puede usar servicios de la plataforma S3, configurar su propia fuente de identidad, usar S3 Select o usar una conexión de federación de red.
- El acceso raíz inicial para el inquilino, en función de si el sistema StorageGRID utiliza grupos y usuarios locales, federación de identidad o inicio de sesión único (SSO).

Además, puede habilitar la configuración de Bloqueo de objetos S3 para el sistema StorageGRID si las cuentas de inquilinos S3 deben cumplir con requisitos reglamentarios. Cuando el bloqueo de objetos S3 está habilitado, todas las cuentas de inquilinos de S3 pueden crear y administrar depósitos compatibles.

¿Para qué se utiliza Tenant Manager?

Después de crear la cuenta de inquilino, los usuarios inquilinos pueden iniciar sesión en el Administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidad (a menos que la fuente de identidad se comparta con la red)
- Administrar grupos y usuarios
- Utilice la federación de red para la clonación de cuentas y la replicación entre redes
- Administrar claves de acceso S3
- Crear y administrar depósitos S3
- Utilice los servicios de la plataforma S3

- Utilice S3 Select
- Monitorear el uso del almacenamiento



Si bien los usuarios inquilinos de S3 pueden crear y administrar claves de acceso y depósitos de S3 con el Administrador de inquilinos, deben usar una aplicación cliente de S3 para ingerir y administrar objetos. Ver "[Utilice la API REST de S3](#)" Para más detalles.

Crear una cuenta de inquilino

Debe crear al menos una cuenta de inquilino para controlar el acceso al almacenamiento en su sistema StorageGRID .

Los pasos para crear una cuenta de inquilino varían según si "[federación de identidades](#)" y "[inicio de sesión único](#)" están configurados y si la cuenta de Grid Manager que utiliza para crear la cuenta de inquilino pertenece a un grupo de administradores con permiso de acceso raíz.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)" .
- Tú tienes el "[Permiso de acceso de root o de cuentas de inquilino](#)" .
- Si la cuenta del inquilino utilizará la fuente de identidad que se configuró para Grid Manager y desea otorgar permiso de acceso raíz para la cuenta del inquilino a un grupo federado, debe importar ese grupo federado a Grid Manager. No es necesario asignar ningún permiso de administrador de cuadrícula a este grupo de administradores. Ver "[Administrar grupos de administradores](#)" .
- Si desea permitir que un inquilino de S3 clone datos de cuenta y replique objetos de bucket a otra red mediante una conexión de federación de red:
 - Tienes "[configuró la conexión de la federación de red](#)" .
 - El estado de la conexión es **Conectado**.
 - Tienes permiso de acceso root.
 - Has revisado las consideraciones para "[Gestión de los inquilinos permitidos para la federación de red](#)" .
 - Si la cuenta del inquilino utilizará la fuente de identidad que se configuró para Grid Manager, habrá importado el mismo grupo federado a Grid Manager en ambas redes.

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



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

Acceder al asistente

Pasos

1. Seleccione **INQUILINOS**.
2. Seleccione **Crear**.

Introducir detalles

Pasos

1. Introduzca los detalles del inquilino.

Campo	Descripción
Nombre	Un nombre para la cuenta del inquilino. Los nombres de los inquilinos no necesitan ser únicos. Cuando se crea la cuenta de inquilino, recibe un ID de cuenta único de 20 dígitos.
Descripción (opcional)	Una descripción para ayudar a identificar al inquilino. Si está creando un inquilino que utilizará una conexión de federación de red, opcionalmente, utilice este campo para ayudar a identificar cuál es el inquilino de origen y cuál es el inquilino de destino. Por ejemplo, esta descripción para un inquilino creado en la Red 1 también aparecerá para el inquilino replicado en la Red 2: "Este inquilino fue creado en la Red 1".
Tipo de cliente	El tipo de protocolo de cliente que utilizará este inquilino, ya sea S3 o Swift . Nota: La compatibilidad con aplicaciones cliente Swift ha quedado obsoleta y se eliminará en una versión futura.
Cuota de almacenamiento (opcional)	Si desea que este inquilino tenga una cuota de almacenamiento, un valor numérico para la cuota y las unidades.

2. Seleccione **Continuar**.

Seleccionar permisos

Pasos

1. Opcionalmente, seleccione los permisos básicos que desea que tenga este inquilino.



Algunos de estos permisos tienen requisitos adicionales. Para obtener más detalles, seleccione el icono de ayuda para cada permiso.

Permiso	Si se selecciona...
Permitir servicios de plataforma	El inquilino puede utilizar servicios de la plataforma S3 como CloudMirror. Ver "Administrar servicios de plataforma para cuentas de inquilinos de S3" .
Utilice su propia fuente de identidad	El inquilino puede configurar y administrar su propia fuente de identidad para grupos y usuarios federados. Esta opción está deshabilitada si tiene "SSO configurado" para su sistema StorageGRID .

Permiso	Si se selecciona...
Permitir selección de S3	El inquilino puede emitir solicitudes de API S3 SelectObjectContent para filtrar y recuperar datos de objetos. Ver "Administrar S3 Select para cuentas de inquilinos" . Importante: Las solicitudes SelectObjectContent pueden disminuir el rendimiento del balanceador de carga para todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

2. Opcionalmente, seleccione los permisos avanzados que desea que tenga este inquilino.

Permiso	Si se selecciona...
Conexión de federación de red	El inquilino puede utilizar una conexión de federación de red, que: • Hace que este inquilino y todos los grupos de inquilinos y usuarios agregados a la cuenta se clonen desde esta cuadrícula (la <i>cuadrícula de origen</i>) a la otra cuadrícula en la conexión seleccionada (la <i>cuadrícula de destino</i>). • Permite que este inquilino configure la replicación entre redes entre los contenedores correspondientes en cada red. Ver "Gestionar los inquilinos permitidos para la federación de red" .
Bloqueo de objetos S3	Permitir que el inquilino utilice funciones específicas de S3 Object Lock: • Establecer período máximo de retención define durante cuánto tiempo se deben conservar los objetos nuevos agregados a este depósito, a partir del momento en que se ingieren. • Permitir modo de cumplimiento evita que los usuarios sobrescriban o eliminen versiones de objetos protegidos durante el período de retención.

3. Seleccione **Continuar**.

Definir el acceso raíz y crear un inquilino

Pasos

1. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza federación de identidad, inicio de sesión único (SSO) o ambos.

Opción	Haz esto
Si la federación de identidad no está habilitada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.

Opción	Haz esto
Si la federación de identidad está habilitada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si tanto la federación de identidad como el inicio de sesión único (SSO) están habilitados	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

2. Seleccione **Crear inquilino**.

Aparece un mensaje de éxito y el nuevo inquilino aparece en la página Inquilinos. Para saber cómo ver los detalles de los inquilinos y monitorear su actividad, consulte ["Supervisar la actividad de los inquilinos"](#).



La aplicación de la configuración de los inquilinos en toda la red podría demorar 15 minutos o más según la conectividad de la red, el estado del nodo y las operaciones de Cassandra.

3. Si seleccionó el permiso **Usar conexión de federación de red** para el inquilino:

- Confirme que se haya replicado un inquilino idéntico en la otra red en la conexión. Los inquilinos de ambas redes tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos.



Si ve el mensaje de error "Inquilino creado sin un clon", consulte las instrucciones en ["Solucionar errores de federación de red"](#).

- Si proporcionó una contraseña de usuario raíz local al definir el acceso raíz, ["cambiar la contraseña del usuario root local"](#) para el inquilino replicado.



Un usuario root local no puede iniciar sesión en Tenant Manager en la red de destino hasta que se cambie la contraseña.

Sign in en el inquilino (opcional)

Según sea necesario, puede iniciar sesión en el nuevo inquilino ahora para completar la configuración, o puede iniciar sesión en el inquilino más tarde. Los pasos para iniciar sesión dependen de si ha iniciado sesión en Grid Manager utilizando el puerto predeterminado (443) o un puerto restringido. Ver ["Controlar el acceso al firewall externo"](#).

Sign in ahora

Si estás usando...	Haz esto...
Puerto 443 y establece una contraseña para el usuario root local	1. Seleccione * Sign in como root*. Al iniciar sesión, aparecen enlaces para configurar depósitos, federación de identidad, grupos y usuarios. 2. Seleccione los enlaces para configurar la cuenta del inquilino. Cada enlace abre la página correspondiente en el Administrador de inquilinos. Para completar la página, consulte la "Instrucciones para usar cuentas de inquilinos".
Puerto 443 y no configuró una contraseña para el usuario root local	Seleccione * Sign in* e ingrese las credenciales de un usuario en el grupo federado de acceso raíz.
Un puerto restringido	1. Seleccionar Finalizar 2. Seleccione Restringido en la tabla de inquilinos para obtener más información sobre cómo acceder a esta cuenta de inquilino. La URL del Administrador de inquilinos tiene este formato: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> ◦ <code>`FQDN_or_Admin_Node_IP`</code> es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ <code>`port`</code> es el puerto exclusivo para inquilinos ◦ <code>`20-digit-account-id`</code> es el ID de cuenta único del inquilino

Sign in más tarde

Si estás usando...	Haz uno de estos...
Puerto 443	• Desde el Administrador de red, seleccione INQUILINOS y seleccione * Sign in* a la derecha del nombre del inquilino. • Introduzca la URL del inquilino en un navegador web: <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> ◦ <code>`FQDN_or_Admin_Node_IP`</code> es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ <code>`20-digit-account-id`</code> es el ID de cuenta único del inquilino

Si estás usando...	Haz uno de estos...
Un puerto restringido	• Desde el Administrador de red, seleccione INQUILINOS y seleccione Restringido. • Introduzca la URL del inquilino en un navegador web: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> ◦ <code>FQDN_or_Admin_Node_IP</code> es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ <code>port</code> Es el puerto restringido solo para inquilinos? ◦ <code>20-digit-account-id</code> es el ID de cuenta único del inquilino

Configurar el inquilino

Siga las instrucciones en ["Utilice una cuenta de inquilino"](#) para administrar grupos de inquilinos y usuarios, claves de acceso S3, buckets, servicios de plataforma, clonación de cuentas y replicación entre redes.

Editar cuenta de inquilino

Puede editar una cuenta de inquilino para cambiar el nombre para mostrar, la cuota de almacenamiento o los permisos del inquilino.



Si un inquilino tiene el permiso **Usar conexión de federación de red**, puede editar los detalles del inquilino desde cualquiera de las redes en la conexión. Sin embargo, cualquier cambio que realice en una cuadrícula de la conexión no se copiará a la otra cuadrícula. Si desea mantener los detalles del inquilino exactamente sincronizados entre las cuadrículas, realice las mismas ediciones en ambas cuadrículas. Ver ["Administrar los inquilinos permitidos para la conexión de la federación de red"](#).

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso de root o de cuentas de inquilino"](#).



La aplicación de la configuración de los inquilinos en toda la red podría demorar 15 minutos o más según la conectividad de la red, el estado del nodo y las operaciones de Cassandra.

Pasos

1. Seleccione **INQUILINOS**.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Localice la cuenta de inquilino que desea editar.

Utilice el cuadro de búsqueda para buscar un inquilino por nombre o ID de inquilino.

3. Seleccione el inquilino. Puede realizar cualquiera de las siguientes acciones:

- Seleccione la casilla de verificación del inquilino y seleccione **Acciones > Editar**.
- Seleccione el nombre del inquilino para mostrar la página de detalles y seleccione **Edit**.

4. Opcionalmente, cambie los valores de estos campos:

- **Nombre**
- **Descripción**
- **Cuota de almacenamiento**

5. Seleccione **Continuar**.

6. Seleccione o borre los permisos para la cuenta de inquilino.

- Si deshabilita 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 ha configurado como punto final. Ver "[Administrar servicios de plataforma para cuentas de inquilinos de S3](#)".
- Cambie la configuración de **Usar fuente de identidad propia** para determinar si la cuenta del inquilino utilizará su propia fuente de identidad o la fuente de identidad que se configuró para Grid Manager.

Si **Utilizar fuente de identidad propia** es:

- Deshabilitado y seleccionado, el inquilino ya ha habilitado su propia fuente de identidad. Un inquilino debe deshabilitar su fuente de identidad antes de poder usar la fuente de identidad que se configuró para Grid Manager.
- Deshabilitado y no seleccionado, SSO está habilitado para el sistema StorageGRID. El inquilino debe utilizar la fuente de identidad que se configuró para Grid Manager.

- Seleccione o desmarque el permiso **Permitir selección S3** según sea necesario. Ver "[Administrar S3 Select para cuentas de inquilinos](#)".
- Para eliminar el permiso **Usar conexión de federación de red**:
 - i. Seleccione la pestaña **Federación de red**.
 - ii. Seleccione **Quitar permiso**.
- Para agregar el permiso **Usar conexión de federación de red**:
 - i. Seleccione la pestaña **Federación de red**.
 - ii. Seleccione la casilla de verificación **Usar conexión de federación de red**.
 - iii. Opcionalmente, seleccione **Clonar usuarios y grupos locales existentes** para clonarlos en la red remota. Si lo desea, puede detener la clonación en curso o volver a intentar la clonación si algunos usuarios o grupos locales no pudieron ser clonados después de que se completó la última operación de clonación.
- Para establecer un período máximo de retención o permitir el modo de cumplimiento:



El bloqueo de objetos S3 debe estar habilitado en la cuadrícula antes de poder usar estas configuraciones.

- i. Seleccione la pestaña **Bloqueo de objeto S3**.
- ii. Para **Establecer período máximo de retención**, ingrese un valor y seleccione el período de tiempo en el menú desplegable.
- iii. Para **Permitir modo de cumplimiento**, seleccione la casilla de verificación.

Cambiar la contraseña del usuario root local del inquilino

Es posible que necesite cambiar la contraseña del usuario raíz local de un inquilino si el usuario raíz no puede acceder a la cuenta.

Antes de empezar

- Ha 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 su sistema StorageGRID, el usuario raíz local no puede iniciar sesión en la cuenta del inquilino. Para realizar tareas de usuario root, los usuarios deben pertenecer a un grupo federado que tenga permiso de acceso root para el inquilino.

Pasos

1. Seleccione **INQUILINOS**.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Seleccione la cuenta del inquilino. Puede realizar cualquiera de las siguientes acciones:
 - Seleccione la casilla de verificación del inquilino y seleccione **Acciones** > **Cambiar contraseña root**.
 - Seleccione el nombre del inquilino para mostrar la página de detalles y seleccione **Acciones** > **Cambiar contraseña root**.
3. Introduzca la nueva contraseña para la cuenta del inquilino.
4. Seleccione **Guardar**.

Eliminar cuenta de inquilino

Puede eliminar una cuenta de inquilino si desea eliminar permanentemente el acceso del inquilino al sistema.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Tienes [permisos de acceso específicos](#).
- Ha eliminado todos los depósitos y objetos S3 asociados con la cuenta del inquilino.
- Si al inquilino se le permite usar una conexión de federación de red, ha revisado las consideraciones para [eliminar un inquilino con el permiso Usar conexión de federación de red](#).

Pasos

1. Seleccione **INQUILINOS**.
2. Localice la cuenta o cuentas de inquilino que desea eliminar.

Utilice el cuadro de búsqueda para buscar un inquilino por nombre o ID de inquilino.
3. Para eliminar varios inquilinos, seleccione las casillas de verificación y seleccione **Acciones** > **Eliminar**.
4. Para eliminar un solo inquilino, realice una de las siguientes acciones:
 - Seleccione la casilla de verificación y seleccione **Acciones** > **Eliminar**.

- Seleccione el nombre del inquilino para mostrar la página de detalles y luego seleccione **Acciones > Eliminar**.

5. Seleccione **Sí**.

Administrar los servicios de la plataforma

¿Qué son los servicios de plataforma?

Los servicios de la plataforma incluyen la replicación de CloudMirror, notificaciones de eventos y el servicio de integración de búsqueda.

Si habilita los servicios de plataforma para las cuentas de inquilinos de S3, debe configurar su red para que los inquilinos puedan acceder a los recursos externos necesarios para usar estos servicios.

Replicación de CloudMirror

El servicio de replicación StorageGRID CloudMirror se utiliza para reflejar objetos específicos de un depósito StorageGRID a un destino externo especificado.

Por ejemplo, puede utilizar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y luego aprovechar los servicios de AWS para realizar análisis de sus datos.



La replicación de CloudMirror tiene algunas similitudes y diferencias importantes con la función de replicación entre redes. Para obtener más información, consulte "[Comparar la replicación entre redes y la replicación de CloudMirror](#)".



La replicación de CloudMirror no es compatible si el depósito de origen tiene habilitado el bloqueo de objetos S3.

Notificaciones

Las notificaciones de eventos por bucket se utilizan para enviar notificaciones sobre acciones específicas realizadas en objetos a un clúster externo de Kafka o Amazon Simple Notification Service especificado.

Por ejemplo, puede configurar alertas para que se envíen a los administradores sobre cada objeto agregado a un depósito, donde los objetos representan archivos de registro asociados con un evento crítico del sistema.



Si bien la notificación de eventos se puede configurar en un bucket con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluidos la fecha de retención y el estado de retención legal) 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 metadatos de objetos S3 a un índice Elasticsearch específico donde los metadatos se pueden buscar o analizar mediante el servicio externo.

Por ejemplo, puede configurar sus depósitos para enviar metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, puede usar Elasticsearch para realizar búsquedas en diferentes grupos y realizar análisis sofisticados de patrones presentes en los metadatos de sus objetos.



Si bien la integración de Elasticsearch se puede configurar en un bucket con S3 Object Lock habilitado, los metadatos de S3 Object Lock (incluidos Conservar hasta la fecha y el estado de Retención legal) de los objetos no se incluirán en los mensajes de notificación.

Los servicios de plataforma brindan a los inquilinos la posibilidad de utilizar recursos de almacenamiento externo, servicios de notificación y servicios de búsqueda o análisis con sus datos. Dado que la ubicación de destino de los servicios de la plataforma generalmente es externa a su implementación de StorageGRID, debe decidir si desea permitir que los inquilinos utilicen estos servicios. Si lo hace, debe habilitar el uso de los servicios de la plataforma cuando cree o edite cuentas de inquilinos. También debe configurar su red de manera que los mensajes de servicios de plataforma que generan los inquilinos puedan llegar a sus destinos.

Recomendaciones para el uso de los servicios de la plataforma

Antes de utilizar los servicios de la plataforma, tenga en cuenta las siguientes recomendaciones:

- Si un bucket S3 en el sistema StorageGRID tiene habilitadas tanto la versión como la replicación de CloudMirror, también debe habilitar la versión del bucket S3 para el punto final de destino. Esto permite que la replicación de CloudMirror genere versiones de objetos similares en el punto final.
- No debe utilizar más de 100 inquilinos activos con solicitudes S3 que requieran replicación, notificaciones e integración de búsqueda de CloudMirror. Tener más de 100 inquilinos activos puede generar un rendimiento más lento del cliente S3.
- Las solicitudes a un punto final que no se puedan completar se pondrán en cola hasta un máximo de 500 000 solicitudes. Este límite se comparte equitativamente entre los inquilinos activos. A los nuevos inquilinos se les permite exceder temporalmente este límite de 500.000 para que los inquilinos recién creados no sean penalizados injustamente.

Información relacionada

- ["Administrar los servicios de la plataforma"](#)
- ["Configurar los ajustes del proxy de almacenamiento"](#)
- ["Monitorear StorageGRID"](#)

Red y puertos para servicios de plataforma

Si permite que un inquilino de S3 utilice servicios de plataforma, debe configurar la red para la red a fin de garantizar que los mensajes de servicios de plataforma puedan entregarse a sus destinos.

Puede habilitar los servicios de plataforma para una cuenta de inquilino S3 cuando crea o actualiza la cuenta de inquilino. Si los servicios de plataforma están habilitados, el inquilino puede crear puntos finales que sirvan como destino para la replicación de CloudMirror, notificaciones de eventos o mensajes de integración de búsqueda desde sus depósitos S3. Estos mensajes de servicios de plataforma se envían desde los nodos de almacenamiento que ejecutan el servicio ADC a los puntos finales de destino.

Por ejemplo, los inquilinos pueden configurar los siguientes tipos de puntos finales de destino:

- Un clúster de Elasticsearch alojado localmente
- Una aplicación local que admite la recepción de mensajes de Amazon Simple Notification Service
- Un clúster de Kafka alojado localmente
- Un depósito S3 alojado localmente en la misma instancia 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 servicios de la plataforma, debe configurar la red o las redes que contienen los nodos de almacenamiento de ADC. Debe asegurarse de que los siguientes puertos se puedan usar para enviar mensajes de servicios de plataforma a los puntos finales de destino.

De forma predeterminada, los mensajes de servicios de la plataforma se envían en los siguientes puertos:

- **80**: Para URI de puntos finales que comienzan con http (la mayoría de los puntos finales)
- **443**: Para URI de puntos finales que comienzan con https (la mayoría de los puntos finales)
- **9092**: Para URI de puntos finales que comienzan con http o https (solo puntos finales de Kafka)

Los inquilinos pueden especificar un puerto diferente cuando crean o editan un punto final.



Si se utiliza una implementación de StorageGRID como destino para la replicación de CloudMirror, es posible que se reciban mensajes de replicación en un puerto distinto de 80 o 443. Asegúrese de que el puerto que utiliza la implementación de StorageGRID de destino para S3 esté especificado en el punto final.

Si utiliza un servidor proxy no transparente, también debe [configurar los ajustes del proxy de almacenamiento](#) para permitir que se envíen mensajes a puntos finales externos, como un punto final en Internet.

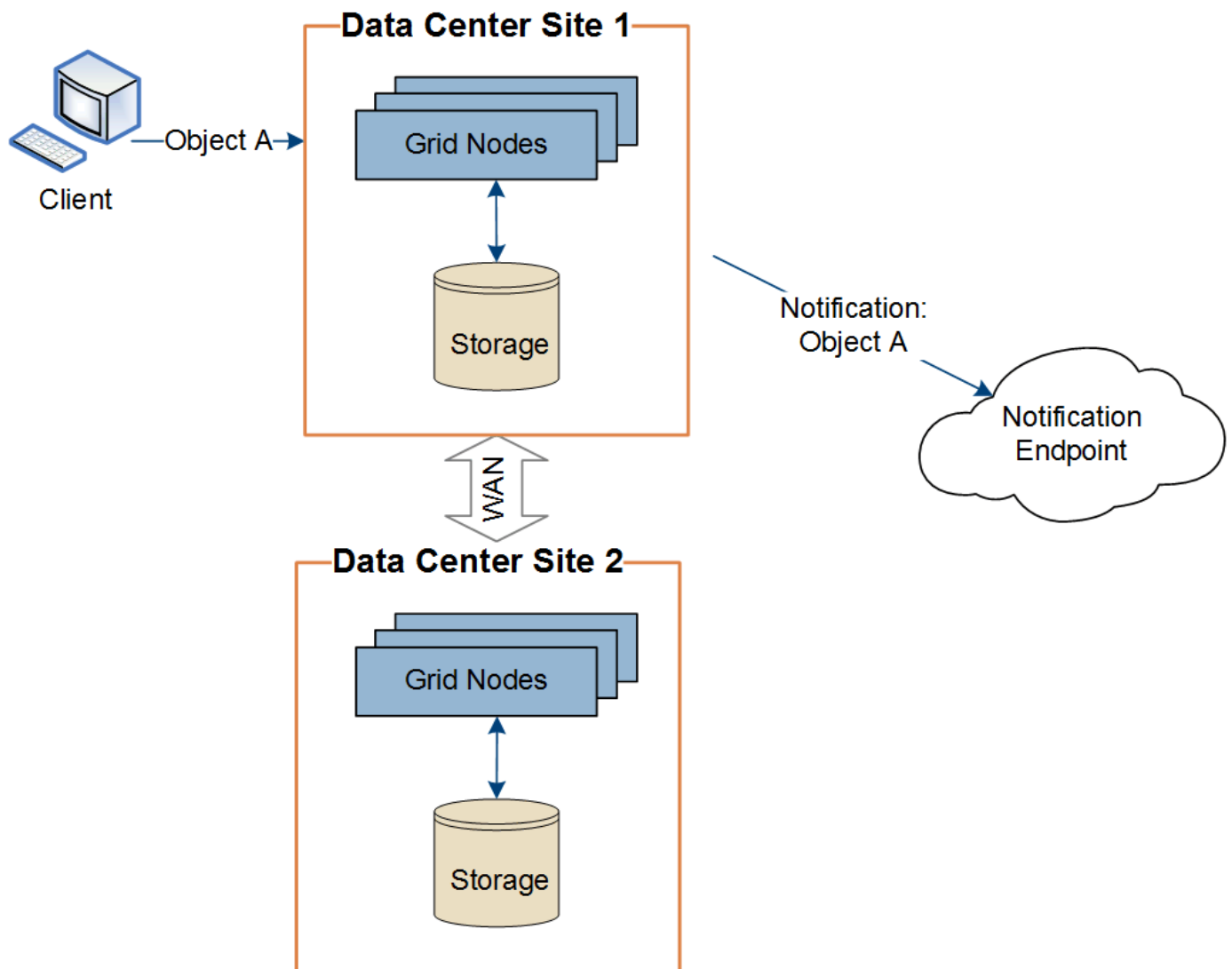
Información relacionada

["Utilice una cuenta de inquilino"](#)

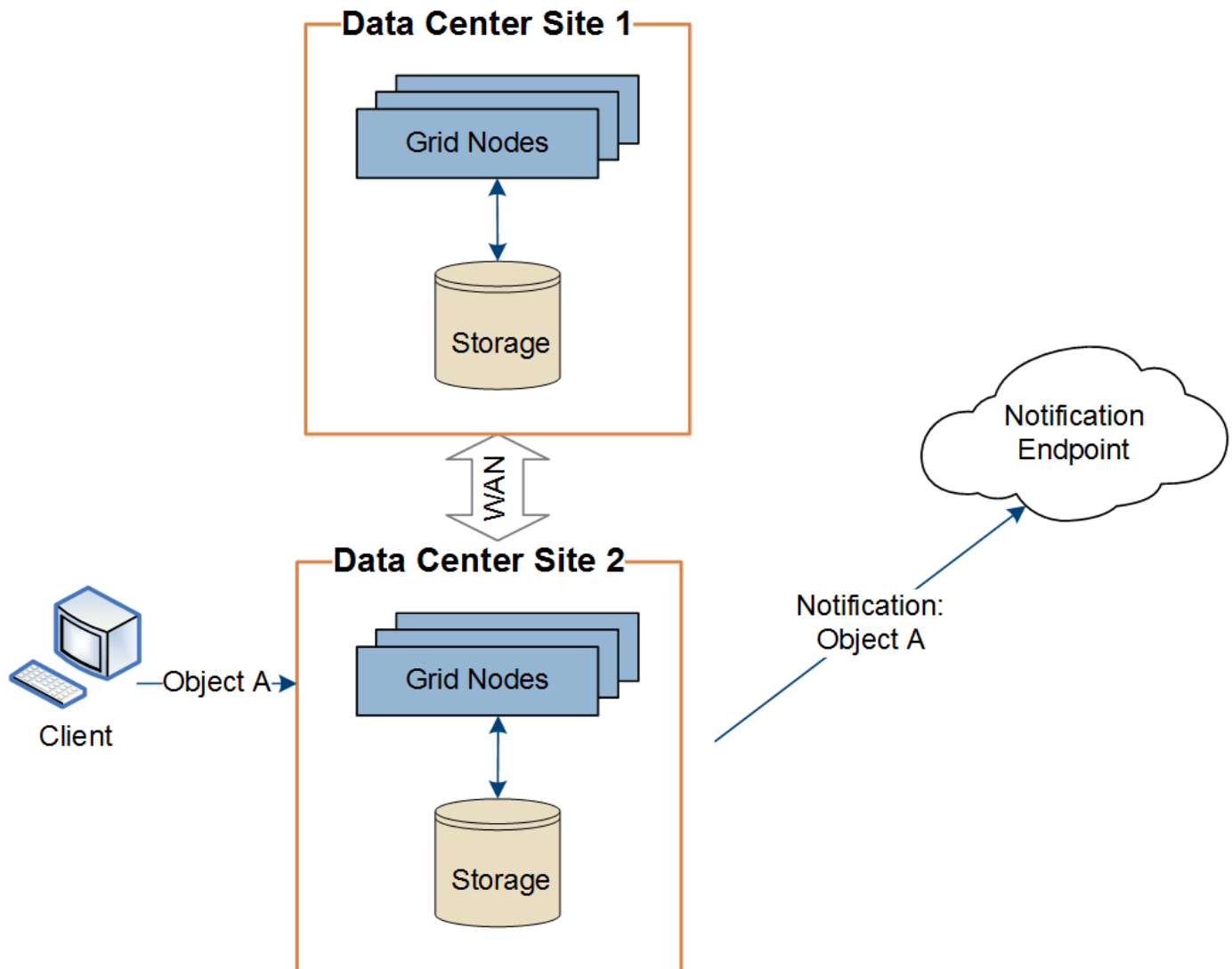
Entrega de mensajes de servicios de plataforma por sitio

Todas las operaciones de servicios de la plataforma se realizan sitio por sitio.

Es decir, si un inquilino utiliza un cliente para realizar una operación de creación de API S3 en un objeto conectándose a un nodo de puerta de enlace en el sitio del centro de datos 1, la notificación sobre esa acción se activa y se envía desde el sitio del centro de datos 1.



Si posteriormente el cliente realiza una operación de eliminación de API S3 en ese mismo objeto desde el sitio del centro de datos 2, la notificación sobre la acción de eliminación se activa y se envía desde el sitio del centro de datos 2.



Asegúrese de que la red en cada sitio esté configurada de manera tal que los mensajes de servicios de la plataforma puedan enviarse a sus destinos.

Solucionar problemas de servicios de la plataforma

Los puntos finales utilizados en los servicios de plataforma son creados y mantenidos por usuarios inquilinos en el Administrador de inquilinos; sin embargo, si un inquilino tiene problemas al configurar o usar los servicios de plataforma, es posible que pueda usar el Administrador de cuadrícula para ayudar a resolver el problema.

Problemas con los nuevos puntos finales

Antes de que un inquilino pueda utilizar los servicios de la plataforma, debe crear uno o más puntos finales mediante el Administrador de inquilinos. Cada punto final 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 punto final incluye tanto la ubicación del recurso externo como las credenciales necesarias para acceder a ese recurso.

Cuando un inquilino crea un punto final, el sistema StorageGRID valida que el punto final exista y que se pueda acceder a él utilizando las credenciales especificadas. La conexión al punto final se valida desde un

nodo en cada sitio.

Si falla la validación del punto final, aparecerá un mensaje de error que explica por qué. El usuario inquilino debe resolver el problema y luego intentar crear el punto final nuevamente.



La creación del punto final fallará si los servicios de la plataforma no están habilitados para la cuenta del inquilino.

Problemas con los puntos finales existentes

Si se produce un error cuando StorageGRID intenta acceder a un punto final existente, se muestra un mensaje en el panel del Administrador de inquilinos.

One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Los usuarios inquilinos pueden ir a la página Puntos finales para revisar el mensaje de error más reciente de cada punto final y determinar cuánto tiempo hace que ocurrió el error. La columna **Último error** muestra el mensaje de error más reciente para cada punto final e indica cuánto tiempo hace que ocurrió el error. Errores que incluyen el El icono apareció en los últimos 7 días.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints Create endpoint

Delete endpoint

☐	Display name	Last error	Type	URI	URN
☐	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
☐	my-endpoint-3	3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
☐	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
☐	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
☐	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



Algunos mensajes de error en la columna **Último error** pueden incluir un ID de registro entre paréntesis. Un administrador de red o soporte técnico puede usar esta ID para localizar información más detallada sobre el error en bycast.log.

Problemas relacionados con los servidores proxy

Si ha configurado un "proxy de almacenamiento" Entre los nodos de almacenamiento y los puntos finales del servicio de la plataforma, pueden ocurrir errores si su servicio proxy no permite mensajes de StorageGRID. Para resolver estos problemas, verifique la configuración de su servidor proxy para asegurarse de que los mensajes relacionados con el servicio de la plataforma no estén bloqueados.

Determinar si se ha producido un error

Si se produjo algún error en los puntos finales durante los últimos 7 días, el panel del Administrador de inquilinos mostrará un mensaje de alerta. Puede ir a la página de Puntos finales para ver más detalles sobre el error.

Las operaciones del cliente fallan

Algunos problemas con los servicios de la plataforma podrían provocar que las operaciones del cliente en el bucket S3 fallen. Por ejemplo, las operaciones del cliente S3 fallarán si el servicio de máquina de estado replicada (RSM) interno se detiene o si hay demasiados mensajes de servicios de plataforma en cola para su entrega.

Para comprobar el estado de los servicios:

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Seleccione **síto > Nodo de almacenamiento > SSM > Servicios**.

Errores de punto final recuperables e irrecuperables

Una vez creados los puntos finales, pueden producirse errores en las solicitudes de servicio de la plataforma por diversos motivos. Algunos errores se pueden recuperar con la intervención del usuario. Por ejemplo, podrían producirse errores recuperables por las siguientes razones:

- Las credenciales del usuario han sido eliminadas o han expirado.
- El depósito de destino no existe.
- No se puede entregar la notificación.

Si StorageGRID encuentra un error recuperable, se volverá a intentar la solicitud del servicio de la plataforma hasta que tenga éxito.

Otros errores son irrecuperables. Por ejemplo, se produce un error irrecuperable si se elimina el punto final.

Si StorageGRID encuentra un error de punto final irrecuperable:

- En el Administrador de cuadrícula, vaya a **Soporte > Herramientas > Métricas > Grafana > Descripción general de los servicios de plataforma** para ver los detalles del error.
- En el Administrador de inquilinos, vaya a **ALMACENAMIENTO (S3) > Puntos finales de servicios de plataforma** para ver los detalles del error.
- Compruebe el `/var/local/log/bycast-err.log` para errores relacionados. Los nodos de almacenamiento que tienen el servicio ADC contienen este archivo de registro.

No se pueden entregar los mensajes de servicios de la plataforma

Si el destino encuentra un problema que le impide aceptar mensajes de servicios de plataforma, la operación del cliente en el depósito se realiza correctamente, pero el mensaje de servicios de plataforma no se entrega.

Por ejemplo, este error podría ocurrir si las credenciales se actualizan en el destino de tal manera que StorageGRID ya no puede autenticarse en el servicio de destino.

Compruebe si hay alertas relacionadas.

Rendimiento más lento para solicitudes de servicio 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 excede la velocidad a la que el punto final de destino puede recibirlas. La limitación solo se produce cuando hay una acumulación de solicitudes en espera de ser enviadas al punto final de destino.

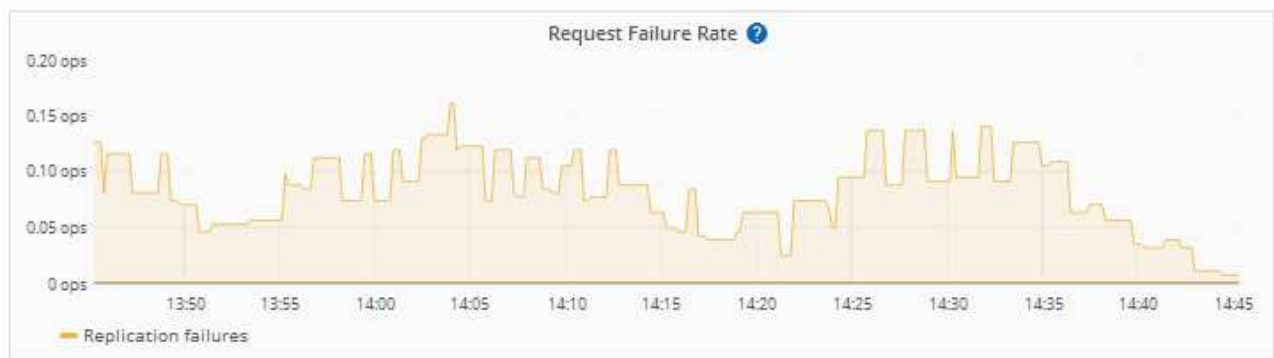
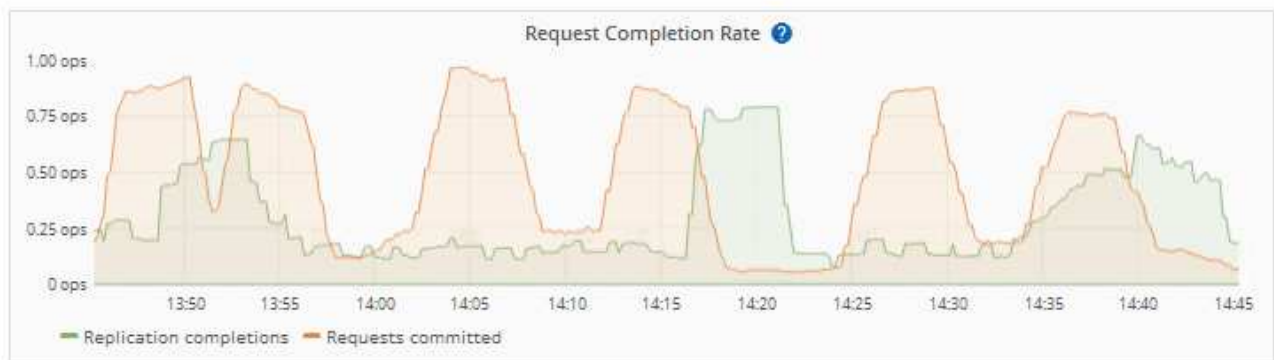
El único efecto visible es que las solicitudes S3 entrantes tardarán más en ejecutarse. Si comienza a detectar un rendimiento significativamente más lento, debe reducir la tasa de ingesta o utilizar un punto final con mayor capacidad. Si la acumulación de solicitudes continúa creciendo, las operaciones S3 del cliente (como las solicitudes PUT) eventualmente fallarán.

Es más probable que las solicitudes de CloudMirror se vean afectadas por el rendimiento del punto final de destino porque estas solicitudes generalmente implican más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.

Las solicitudes de servicio de la plataforma fallan

Para ver la tasa de fallas de solicitudes para los servicios de la plataforma:

1. Seleccione **NODOS**.
2. Seleccione **site > Servicios de plataforma**.
3. Vea el gráfico de tasa de error de solicitud.



Alerta de servicios de plataforma no disponibles

La alerta **Servicios de plataforma no disponibles** indica que no se pueden realizar operaciones de servicio de plataforma en un sitio porque hay 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 puntos finales.

Para resolver esta alerta, determine qué nodos de almacenamiento en el sitio incluyen el servicio RSM. (El servicio RSM está presente en los nodos de almacenamiento que también incluyen el servicio ADC). Luego, asegúrese de que una mayoría simple de esos nodos de almacenamiento estén en ejecución y disponibles.



Si más de un nodo de almacenamiento que contiene el servicio RSM falla en un sitio, perderá todas las solicitudes de servicio de plataforma pendientes para ese sitio.

Guía adicional para la resolución de problemas de los puntos finales de los servicios de la plataforma

Para obtener información adicional, consulte [Usar una cuenta de inquilino](#) > [Solucionar problemas de puntos finales de servicios de la plataforma](#).

Información relacionada

["Solucionar problemas del sistema StorageGRID"](#)

Administrar S3 Select para cuentas de inquilinos

Puede permitir que determinados inquilinos de S3 utilicen S3 Select para emitir solicitudes SelectObjectContent en objetos individuales.

S3 Select proporciona una forma eficiente de buscar en grandes cantidades de datos sin tener que implementar una base de datos y recursos asociados para habilitar las búsquedas. También reduce el coste y la latencia de la recuperación de datos.

¿Qué es S3 Select?

S3 Select permite a los clientes S3 utilizar solicitudes SelectObjectContent para filtrar y recuperar solo los datos necesarios de un objeto. La implementación de StorageGRID de S3 Select incluye un subconjunto de comandos y características de S3 Select.

Consideraciones y requisitos para el uso de S3 Select

Requisitos de administración de la red

El administrador de la red debe otorgar a los inquilinos la capacidad de selección S3. Seleccione **Permitir selección S3** cuando [creando un inquilino](#) o [editar un inquilino](#).

Requisitos de formato de objeto

El objeto que desea consultar debe estar en uno de los siguientes formatos:

- **CSV.** Se puede utilizar tal cual o comprimido 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 Parquet. Debe especificar el formato de salida como CSV o JSON.
 - El tamaño máximo del grupo de filas sin comprimir es 512 MB.
 - Debe utilizar los tipos de datos especificados en el esquema del objeto.
 - No se pueden utilizar los tipos lógicos INTERVAL, JSON, LIST, TIME o UUID.

Requisitos del punto final

La solicitud SelectObjectContent debe enviarse a un [Punto final del balanceador de carga de StorageGRID](#).

Los nodos de administración y de puerta de enlace utilizados por el punto final deben ser uno de los siguientes:

- Un nodo de dispositivo de servicios
- Un nodo de software basado en VMware
- Un nodo de metal desnudo que ejecuta un kernel con cgroup v2 habilitado

Consideraciones generales

Las consultas no se pueden enviar directamente a los nodos de almacenamiento.



Las solicitudes de SelectObjectContent pueden disminuir el rendimiento del equilibrador de carga para todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

Ver el ["Instrucciones para utilizar S3 Select"](#) .

Para ver ["Gráficos de Grafana"](#) Para seleccionar operaciones a lo largo del tiempo, seleccione **SOPORTE > Herramientas > Métricas** en el Administrador de cuadrícula.

Configurar conexiones de cliente

Configurar conexiones de cliente S3

Como administrador de la red, usted administra las opciones de configuración que controlan cómo las aplicaciones cliente S3 se conectan a su sistema StorageGRID para almacenar y recuperar datos.



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["StorageGRID 11.8: Configurar conexiones de cliente S3 y Swift"](#) .

Tareas de configuración

1. Realice tareas previas requeridas en StorageGRID, según cómo la aplicación cliente se conectará a StorageGRID.

Tareas requeridas

Debes obtener:

- Direcciones IP
- Nombres de dominio
- Certificado SSL

Tareas opcionales

Opcionalmente, configure:

- Federación de identidades
- SSO

1. Utilice StorageGRID para obtener los valores que la aplicación necesita para conectarse a la red. Puede utilizar el asistente de configuración de S3 o configurar cada entidad StorageGRID manualmente. +

Utilice el asistente de configuración de S3

Siga los pasos del asistente de configuración de S3.

Configurar manualmente

1. Crear un grupo de alta disponibilidad
2. Crear un punto final del balanceador de carga
3. Crear una cuenta de inquilino
4. Crear bucket y claves de acceso
5. Configurar reglas y políticas de ILM

1. Utilice la aplicación S3 para completar la conexión a StorageGRID. Cree entradas DNS para asociar direcciones IP a cualquier nombre de dominio que planee utilizar.

Según sea necesario, realice configuraciones adicionales de la aplicación.

2. Realice tareas continuas en la aplicación y en StorageGRID para administrar y monitorear el almacenamiento de objetos a lo largo del tiempo.

Información necesaria para adjuntar StorageGRID a una aplicación cliente

Antes de poder conectar StorageGRID a una aplicación cliente S3, debe realizar pasos de configuración en StorageGRID y obtener cierto valor.

¿Qué valores necesito?

La siguiente tabla muestra los valores que debe configurar en StorageGRID y dónde la aplicación S3 y el servidor DNS utilizan esos valores.

Valor	Donde se configura el valor	Dónde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto final del balanceador de carga	Aplicación cliente
Certificado SSL	StorageGRID > Punto final del balanceador de carga	Aplicación cliente
Nombre del servidor (FQDN)	StorageGRID > Punto final del balanceador de carga	• Aplicación cliente • Entrada DNS
ID de clave de acceso S3 y clave de acceso secreta	StorageGRID > Inquilino y depósito	Aplicación cliente

Valor	Donde se configura el valor	Dónde se utiliza el valor
Nombre del cubo/contenedor	StorageGRID > Inquilino y depósito	Aplicación cliente

¿Cómo obtengo estos valores?

Dependiendo de sus necesidades, puede realizar cualquiera de las siguientes acciones para obtener la información que necesita:

- *Utilice el ["Asistente de configuración de S3"](#) *. El asistente de configuración de S3 le ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera uno o dos archivos que puede usar al configurar la aplicación S3. El asistente lo guía a través de los pasos necesarios y lo ayuda a garantizar que su configuración se ajuste a las mejores prácticas de StorageGRID .



Si está configurando una aplicación S3, se recomienda utilizar el asistente de configuración S3 a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

- *Utilice el ["Asistente de configuración de FabricPool"](#) *. Similar al asistente de configuración de S3, el asistente de configuración de FabricPool lo ayuda a configurar rápidamente los valores requeridos y genera un archivo que puede usar cuando configura un nivel de nube de FabricPool en ONTAP.



Si planea utilizar StorageGRID como sistema de almacenamiento de objetos para un nivel de nube de FabricPool , se recomienda utilizar el asistente de configuración de FabricPool a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

- **Configurar elementos manualmente.** Si se conecta a una aplicación S3 y prefiere no utilizar el asistente de configuración S3, puede obtener los valores necesarios realizando la configuración manualmente. Siga estos pasos:
 - a. Configure el grupo de alta disponibilidad (HA) que desea utilizar para la aplicación S3. Ver ["Configurar grupos de alta disponibilidad"](#) .
 - b. Cree el punto final del equilibrador de carga que utilizará la aplicación S3. Ver ["Configurar los puntos finales del balanceador de carga"](#) .
 - c. Cree la cuenta de inquilino que utilizará la aplicación S3. Ver ["Crear una cuenta de inquilino"](#) .
 - d. Para un inquilino S3, inicie sesión en la cuenta del inquilino y genere una ID de clave de acceso y una clave de acceso secreta para cada usuario que accederá a la aplicación. Ver ["Crea tus propias claves de acceso"](#) .
 - e. Cree uno o más depósitos S3 dentro de la cuenta del inquilino. Para S3, consulte ["Crear un depósito S3"](#) .
 - f. Para agregar instrucciones de ubicación específicas para los objetos que pertenecen al nuevo inquilino o contenedor, cree una nueva regla ILM y active una nueva política ILM para usar esa regla. Ver ["Crear regla ILM"](#) y ["Crear una política ILM"](#) .

Seguridad para clientes S3

Las cuentas de inquilino de StorageGRID utilizan aplicaciones cliente S3 para guardar datos de objetos en StorageGRID. Debe revisar las medidas de seguridad implementadas para las aplicaciones cliente.

Resumen

La siguiente lista resume cómo se implementa la seguridad para la API REST de S3:

Seguridad de la conexión

TLS

Autenticación del servidor

Certificado de servidor X.509 firmado por la CA del sistema o certificado de servidor personalizado proporcionado por el administrador

Autenticación de cliente

ID de clave de acceso de la cuenta S3 y clave de acceso secreta

Autorización del cliente

Propiedad del depósito y todas las políticas de control de acceso aplicables

Cómo StorageGRID proporciona seguridad para las aplicaciones cliente

Las aplicaciones cliente S3 pueden conectarse al servicio Load Balancer en nodos de puerta de enlace o nodos de administración o directamente a nodos de almacenamiento.

- Los clientes que se conectan al servicio Load Balancer pueden usar HTTPS o HTTP, según cómo ["configurar el punto final del balanceador de carga"](#).

Se recomienda utilizar HTTPS para proporcionar una comunicación segura cifrada mediante TLS. Debe adjuntar un certificado de seguridad al punto final.

HTTP proporciona una comunicación menos segura y sin cifrar y solo debe usarse para redes que no sean de producción o de prueba.

- Los clientes que se conectan a los nodos de almacenamiento también pueden usar HTTPS o HTTP.

HTTPS es el predeterminado y se recomienda.

HTTP proporciona una comunicación menos segura y sin cifrar, pero puede ser opcional. ["activado"](#) para redes que no sean de producción o de prueba.

- Las comunicaciones entre StorageGRID y el cliente están cifradas mediante TLS.
- Las comunicaciones entre el servicio Load Balancer y los nodos de almacenamiento dentro de la red están cifradas independientemente de si el punto final del balanceador de carga está configurado para aceptar conexiones HTTP o HTTPS.
- Los clientes deben suministrar ["Encabezados de autenticación HTTP"](#) a StorageGRID para realizar operaciones de API REST.

Certificados de seguridad y aplicaciones cliente

En todos los casos, las aplicaciones cliente pueden realizar conexiones TLS utilizando un certificado de servidor personalizado cargado por el administrador de la red o un certificado generado por el sistema StorageGRID :

- Cuando las aplicaciones cliente se conectan al servicio Load Balancer, utilizan el certificado que se configuró para el punto final del balanceador de carga. Cada punto final del equilibrador de carga tiene su propio certificado: un certificado de servidor personalizado cargado por el administrador de la red o un

certificado que el administrador de la red generó en StorageGRID al configurar el punto final.

Ver "[Consideraciones 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 generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (que están firmados por la autoridad de certificación del sistema) o un único certificado de servidor personalizado que proporciona un administrador de la red para la red. Ver "[agregar un certificado API S3 personalizado](#)".

Los clientes deben configurarse para confiar en la autoridad de certificación que firmó el certificado que utilizan para establecer conexiones TLS.

Algoritmos de cifrado y hash compatibles con bibliotecas TLS

El sistema StorageGRID admite un conjunto de conjuntos de cifrado que las aplicaciones cliente pueden usar al establecer una sesión TLS. Para configurar cifrados, vaya a **CONFIGURACIÓN > Seguridad > Configuración de seguridad** y seleccione **Políticas TLS y SSH**.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3.



SSLv3 y TLS 1.1 (o versiones anteriores) ya no son compatibles.

Utilice el asistente de configuración de S3

Utilizar el asistente de configuración de S3: Consideraciones y requisitos

Puede utilizar el asistente de configuración de S3 para configurar StorageGRID como el sistema de almacenamiento de objetos para una aplicación S3.

Cuándo utilizar el asistente de configuración de S3

El asistente de configuración de S3 lo guía a través de cada paso de la configuración de StorageGRID para su uso con una aplicación S3. Como parte de completar el asistente, descargará archivos que puede usar para ingresar valores en la aplicación S3. Utilice el asistente para configurar su sistema más rápidamente y asegurarse de que sus configuraciones se ajusten a las mejores prácticas de StorageGRID.

Si tienes el "[Permiso de acceso root](#)" Puede completar el asistente de configuración de S3 cuando comience a utilizar StorageGRID Grid Manager o puede acceder al asistente y completarlo en cualquier momento posterior. Dependiendo de sus requisitos, también puede configurar algunos o todos los elementos necesarios manualmente y luego usar el asistente para reunir los valores que necesita una aplicación S3.

Antes de utilizar el asistente

Antes de utilizar el asistente, confirme que ha completado estos requisitos previos.

Obtener direcciones IP y configurar interfaces VLAN

Si configura un grupo de alta disponibilidad (HA), sabrá a qué nodos se conectará la aplicación S3 y qué red StorageGRID se utilizará. También sabe qué valores ingresar para el CIDR de subred, la dirección IP de puerta de enlace y las direcciones IP virtuales (VIP).

Si planea utilizar una LAN virtual para segregar el tráfico de la aplicación S3, ya ha configurado la interfaz

VLAN. Ver "[Configurar interfaces VLAN](#)".

Configurar la federación de identidades y el SSO

Si planea utilizar la federación de identidad o el inicio de sesión único (SSO) para su sistema StorageGRID, debe habilitar estas funciones. También sabe qué grupo federado debe tener acceso raíz para la cuenta de inquilino que utilizará la aplicación S3. Ver "[Utilizar la federación de identidades](#)" y "[Configurar el inicio de sesión único](#)".

Obtener y configurar nombres de dominio

Sabe qué nombre de dominio completo (FQDN) utilizar para StorageGRID. Las entradas del servidor de nombres de dominio (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad que cree mediante el asistente.

Si planea utilizar solicitudes alojadas virtuales de estilo S3, debe tener "[nombres de dominio de punto final S3 configurados](#)". Se recomienda utilizar solicitudes de estilo alojado virtual.

Revisar los requisitos del balanceador de carga y del certificado de seguridad

Si planea utilizar el balanceador de carga StorageGRID, ha revisado las consideraciones generales para el balanceo de carga. Tienes los certificados que cargarás o los valores que necesitas para generar un certificado.

Si planea utilizar un punto final de balanceador de carga externo (de terceros), debe tener el nombre de dominio completo (FQDN), el puerto y el certificado para ese balanceador de carga.

Configurar cualquier conexión de federación de red

Si desea permitir que el inquilino de S3 clone datos de cuenta y replique objetos de bucket a otra red mediante una conexión de federación de red, confirme lo siguiente antes de iniciar el asistente:

- Tienes "[configuró la conexión de la federación de red](#)".
- El estado de la conexión es **Conectado**.
- Tienes permiso de acceso root.

Acceda y complete el asistente de configuración de S3

Puede utilizar el asistente de configuración de S3 para configurar StorageGRID para su uso con una aplicación S3. El asistente de configuración proporciona los valores que la aplicación necesita para acceder a un depósito StorageGRID y guardar objetos.

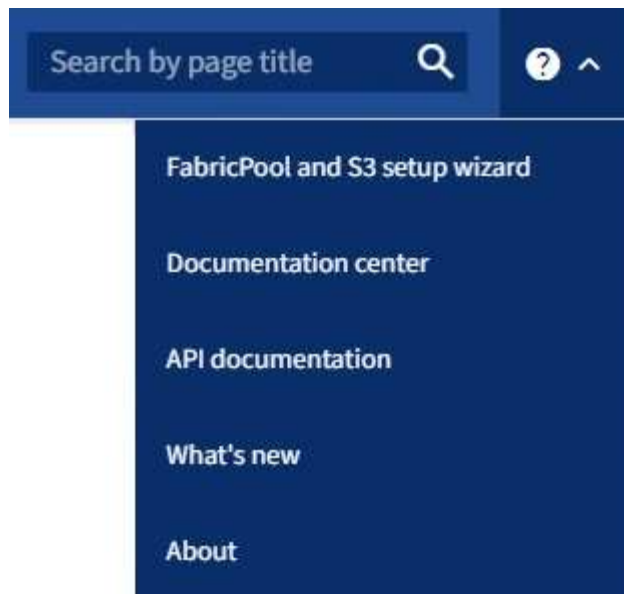
Antes de empezar

- Tú tienes el "[Permiso de acceso root](#)".
- Usted ha revisado el "[Consideraciones y requisitos](#)" para utilizar el asistente.

Acceder al asistente

Pasos

1. Sign in en Grid Manager usando un "[navegador web compatible](#)".
2. Si aparece el banner **Asistente de configuración de FabricPool y S3** en el panel, seleccione el enlace en el banner. Si el banner ya no aparece, seleccione el ícono de ayuda en la barra de encabezado en el Administrador de cuadrícula y seleccione **Asistente de configuración de FabricPool y S3**.



3. En la sección de aplicación S3 de la página del asistente de configuración de FabricPool y S3, seleccione **Configurar ahora**.

Paso 1 de 6: Configurar el grupo de alta disponibilidad

Un grupo de alta disponibilidad es una colección de nodos que contienen cada uno el servicio StorageGRID Load Balancer. Un grupo de alta disponibilidad puede contener nodos de puerta de enlace, nodos de administración o ambos.

Puede utilizar 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 administrar la carga de trabajo con poco impacto en las operaciones de S3.

Para obtener más detalles sobre esta tarea, consulte ["Administrar grupos de alta disponibilidad"](#) .

Pasos

1. Si planea utilizar un balanceador de carga externo, no necesita crear un grupo de alta disponibilidad. Seleccione **Omitir este paso** y vaya a [Paso 2 de 6: Configurar el punto final del balanceador de carga](#) .
2. Para utilizar el equilibrador de carga StorageGRID , puede crear un nuevo grupo de HA o utilizar un grupo de HA existente.

Crear un grupo de alta disponibilidad

- Para crear un nuevo grupo de HA, seleccione **Crear grupo de HA**.
- Para el paso **Ingresar detalles**, complete los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo HA.
Descripción (opcional)	La descripción de este grupo HA.

- Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo de HA.

Utilice los encabezados de columna para ordenar las filas o ingrese un término de búsqueda para localizar interfaces más rápidamente.

Puede seleccionar uno o más nodos, pero solo puede seleccionar una interfaz para cada nodo.

- Para el paso **Priorizar interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo de HA.

Arrastre filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.

Si el grupo HA incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de respaldo, y así sucesivamente. Cuando se resuelven las fallas, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

- Para el paso **Ingresar direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de 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 configurado. Por ejemplo, 192.16.0.0/22 .
Dirección IP de la puerta de enlace (opcional)	Si las direcciones IP de S3 utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID , ingrese la dirección IP de la puerta de enlace local VIP de StorageGRID . La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	Ingrese al menos una y no más de diez direcciones VIP para la interfaz activa en el grupo HA. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. Opcionalmente, puede especificar direcciones IPv4 e IPv6 adicionales.

f. Seleccione **Crear grupo HA** y luego seleccione **Finalizar** para regresar al asistente de configuración de S3.

g. Seleccione **Continuar** para ir al paso del balanceador de carga.

Utilizar el grupo HA existente

a. Para utilizar un grupo de HA existente, seleccione el nombre del grupo de HA en **Seleccionar un grupo de HA**.

b. Seleccione **Continuar** para ir al paso del balanceador de carga.

Paso 2 de 6: Configurar el punto final del balanceador de carga

StorageGRID utiliza un equilibrador de carga para administrar la carga de trabajo de las aplicaciones cliente. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en múltiples nodos de almacenamiento.

Puede utilizar el servicio StorageGRID Load Balancer, que existe en todos los nodos de puerta de enlace y de administración, o puede conectarse a un balanceador de carga externo (de terceros). Se recomienda utilizar el balanceador de carga StorageGRID .

Para obtener más detalles sobre esta tarea, consulte ["Consideraciones para el equilibrio de carga"](#) .

Para utilizar el servicio StorageGRID Load Balancer, seleccione la pestaña * StorageGRID load balancer* y luego cree o seleccione el punto final del balanceador de carga que desee utilizar. Para utilizar un balanceador de carga externo, seleccione la pestaña **Balanceador de carga externo** y proporcione detalles sobre el sistema que ya ha configurado.

Crear punto final

Pasos

1. Para crear un punto final de balanceador de carga, seleccione **Crear punto final**.
2. Para el paso **Ingresar detalles del punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final.
Puerto	El puerto StorageGRID que desea utilizar para equilibrar la carga. Este campo tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede ingresar cualquier puerto externo no utilizado. Si ingresa 80 o 443, el punto final se configura solo en los nodos de puerta de enlace, porque estos puertos están reservados en los nodos de administración. Nota: No se permiten los puertos utilizados por otros servicios de red. Ver el "Referencia del puerto de red".
Tipo de cliente	Debe ser S3 .
Protocolo de red	Seleccione HTTPS. Nota: Se admite la comunicación con StorageGRID sin cifrado TLS, pero no se recomienda.

3. Para el paso **Seleccionar modo de enlace**, especifique el modo de enlace. El modo de enlace controla cómo se accede al punto final utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice la configuración Global (predeterminada) a menos que necesite restringir la accesibilidad de este punto final.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o FQDN correspondiente) de un grupo de HA para acceder a este punto final. Todos los puntos finales con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de HA que seleccione para los puntos finales no se superpongan.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.

Modo	Descripción
Tipo de nodo	Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este punto final.

4. Para el paso de acceso de inquilino, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (predeterminado)	Todas las cuentas de inquilinos pueden usar este punto final para acceder a sus depósitos.
Permitir inquilinos seleccionados	Solo las cuentas de inquilinos seleccionadas pueden usar este punto final para acceder a sus depósitos.
Bloquear inquilinos seleccionados	Las cuentas de inquilinos seleccionadas no pueden usar este punto final para acceder a sus depósitos. Todos los demás inquilinos pueden utilizar este punto final.

5. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utilice esta opción para cargar un certificado de servidor firmado por una CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Utilice esta opción para generar un certificado autofirmado. Ver " Configurar los puntos finales del balanceador de carga " para obtener detalles de qué ingresar.
Utilice el certificado StorageGRID S3	Utilice esta opción solo si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID . Ver " Configurar certificados de API S3 " Para más detalles.

6. Seleccione **Finalizar** para regresar al asistente de configuración de S3.

7. Seleccione **Continuar** para ir al paso de inquilino y depósito.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utilice el punto final del balanceador de carga existente

Pasos

1. Para utilizar un punto final existente, seleccione su nombre en **Seleccionar un punto final del balanceador de carga**.
2. Seleccione **Continuar** para ir al paso de inquilino y depósito.

Utilice un balanceador de carga externo

Pasos

1. Para utilizar un balanceador de carga externo, complete los siguientes campos.

Campo	Descripción
Nombre de dominio completo (FQDN)	El nombre de dominio completo (FQDN) del balanceador de carga externo.
Puerto	El número de puerto que utilizará la aplicación S3 para conectarse al balanceador de carga externo.
Certificado	Copie el certificado del servidor para el balanceador de carga externo y péguelo en este campo.

2. Seleccione **Continuar** para ir al paso de inquilino y depósito.

Paso 3 de 6: Crear inquilino y depósito

Un inquilino es una entidad que puede utilizar aplicaciones S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, depósitos, objetos y un conjunto específico de capacidades.

Un bucket es un contenedor que se utiliza para almacenar objetos y metadatos de objetos de un inquilino. Aunque los inquilinos pueden tener muchos grupos, el asistente le ayuda a crear un inquilino y un grupo de la forma más rápida y sencilla. Si necesita agregar depósitos o configurar opciones más adelante, puede utilizar el Administrador de inquilinos.

Para obtener más detalles sobre esta tarea, consulte ["Crear una cuenta de inquilino"](#) y ["Crear un depósito S3"](#).

Pasos

1. Introduzca un nombre para la cuenta de inquilino.

Los nombres de los inquilinos no necesitan ser únicos. Cuando se crea la cuenta de inquilino, recibe un ID de cuenta numérico único.

2. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza ["federación de identidades"](#), ["inicio de sesión único \(SSO\)"](#), o ambos.

Opción	Haz esto
Si la federación de identidad no está habilitada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidad está habilitada	a. Seleccione un grupo federado existente para tener "Permiso de acceso root" para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.

Opción	Haz esto
Si tanto la federación de identidad como el inicio de sesión único (SSO) están habilitados	Seleccione un grupo federado existente para tener " Permiso de acceso root " para el inquilino. Ningún usuario local puede iniciar sesión.

- Si desea que el asistente cree la ID de clave de acceso y la clave de acceso secreta para el usuario raíz, seleccione **Crear clave de acceso S3 del usuario raíz automáticamente**.

Seleccione esta opción si el único usuario del inquilino será el usuario raíz. Si otros usuarios utilizarán este inquilino, "[utilizar el Administrador de inquilinos](#)" para configurar claves y permisos.

- Si desea crear un depósito para este inquilino ahora, seleccione **Crear depósito para este inquilino**.



Si el Bloqueo de objetos S3 está habilitado para la cuadrícula, el depósito creado en este paso no tendrá el Bloqueo de objetos S3 habilitado. Si necesita utilizar un depósito de bloqueo de objetos S3 para esta aplicación S3, no seleccione crear un depósito ahora. En su lugar, utilice el Administrador de inquilinos para "[crear el cubo](#)" más tarde.

- Introduzca el nombre del depósito que utilizará la aplicación S3. Por ejemplo, `s3-bucket`.

No puedes cambiar el nombre del depósito después de crearlo.

- Seleccione la **Región** para este bucket.

Utilice la región predeterminada (`us-east-1`) a menos que espere utilizar ILM en el futuro para filtrar objetos según la región del depósito.

- Seleccione **Crear y continuar**.

Paso 4 de 6: Descargar datos

En el paso de descarga de datos, puede descargar uno o dos archivos para guardar los detalles de lo que acaba de configurar.

Pasos

- Si seleccionó **Crear clave de acceso S3 de usuario raíz automáticamente**, realice una o ambas de las siguientes acciones:
 - Seleccione **Descargar claves de acceso** para descargar una `.csv` archivo que contiene el nombre de la cuenta del inquilino, el ID de la clave de acceso y la clave de acceso secreta.
 - Seleccione el icono de copia () para copiar el ID de la clave de acceso y la clave de acceso secreta al portapapeles.
- Seleccione **Descargar valores de configuración** para descargar un `.txt` archivo que contiene las configuraciones para el punto final del balanceador de carga, el inquilino, el depósito y el usuario raíz.
- Guarde esta información en un lugar seguro.



No cierre esta página hasta que haya copiado ambas claves de acceso. Las claves no estarán disponibles después de cerrar esta página. Asegúrese de guardar esta información en una ubicación segura porque puede usarse para obtener datos de su sistema StorageGRID.

4. Si se le solicita, seleccione la casilla de verificación para confirmar que ha descargado o copiado las claves.
5. Seleccione **Continuar** para ir al paso de reglas y políticas de ILM.

Paso 5 de 6: Revisar la regla y la política de ILM para S3

Las reglas de administración del ciclo de vida de la información (ILM) controlan la ubicación, la duración y el comportamiento de ingesta de todos los objetos en su sistema StorageGRID . La política ILM incluida con StorageGRID realiza dos copias replicadas de todos los objetos. Esta política estará vigente hasta que active al menos una nueva política.

Pasos

1. Revise la información proporcionada en la página.
2. Si desea agregar instrucciones específicas para los objetos que pertenecen al nuevo inquilino o depósito, cree una nueva regla y una nueva política. Ver "[Crear regla ILM](#)" y "[Utilice las políticas de ILM](#)".
3. Seleccione **He revisado estos pasos y entiendo lo que necesito hacer**.
4. Seleccione la casilla de verificación para indicar que comprende qué hacer a continuación.
5. Seleccione **Continuar** para ir a **Resumen**.

Paso 6 de 6: Revisar el resumen

Pasos

1. Revise el resumen.
2. Tome nota de los detalles en los próximos pasos, que describen la configuración adicional que podría ser necesaria antes de conectarse al cliente S3. Por ejemplo, si selecciona * Sign in como root*, accederá al Administrador de inquilinos, donde podrá agregar usuarios inquilinos, crear depósitos adicionales y actualizar la configuración de los depósitos.
3. Seleccione **Finalizar**.
4. Configure la aplicación utilizando el archivo que descargó de StorageGRID o los valores que obtuvo manualmente.

Administrar grupos de alta disponibilidad

¿Qué son los grupos de alta disponibilidad (HA)?

Los grupos de alta disponibilidad (HA) proporcionan conexiones de datos de alta disponibilidad para clientes S3 y conexiones de alta disponibilidad para Grid Manager y Tenant Manager.

Puede 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 en el grupo HA falla, una interfaz de respaldo puede administrar la carga de trabajo.

Cada grupo HA proporciona acceso a los servicios compartidos en los nodos seleccionados.

- Los grupos de alta disponibilidad que incluyen nodos de puerta de enlace, nodos de administración o ambos proporcionan conexiones de datos de alta disponibilidad para clientes S3.
- Los grupos de HA que incluyen solo nodos de administración proporcionan conexiones de alta disponibilidad al Administrador de red y al Administrador de inquilinos.

- Un grupo de alta disponibilidad que incluye solo dispositivos de servicios y nodos de software basados en VMware puede proporcionar conexiones de alta disponibilidad para ["Inquilinos de S3 que utilizan S3 Select"](#) . Se recomiendan grupos HA cuando se utiliza S3 Select, pero no son obligatorios.

¿Cómo se crea un grupo HA?

1. Selecciona una interfaz de red para uno o más nodos de administración o nodos de puerta de enlace. Puede utilizar una interfaz de red de cuadrícula (eth0), una interfaz de red de cliente (eth2), una interfaz VLAN o una interfaz de acceso que haya agregado al nodo.



No se puede agregar una interfaz a un grupo HA si tiene una dirección IP asignada por DHCP.

2. Debe especificar una interfaz para que sea la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.
3. Usted determina el orden de prioridad para cualquier interfaz de respaldo.
4. Asigna de una a diez direcciones IP virtuales (VIP) al grupo. Las aplicaciones clientes pueden usar cualquiera de estas direcciones VIP para conectarse a StorageGRID.

Para obtener instrucciones, consulte ["Configurar grupos de alta disponibilidad"](#) .

¿Qué es la interfaz activa?

Durante el funcionamiento normal, todas las direcciones VIP del grupo HA se agregan a la interfaz principal, que es la primera interfaz en el orden de prioridad. Mientras la interfaz principal permanezca disponible, se utilizará cuando los clientes se conecten a cualquier dirección VIP del grupo. Es decir, durante el funcionamiento normal, la interfaz principal es la interfaz "activa" para el grupo.

De manera similar, durante el funcionamiento normal, cualquier interfaz de menor prioridad para el grupo HA actúa como interfaz de "respaldo". Estas interfaces de respaldo no se utilizan a menos que la interfaz principal (actualmente activa) deje de estar disponible.

Ver el estado actual del grupo HA de un nodo

Para ver si un nodo está asignado a un grupo de alta disponibilidad y determinar su estado actual, seleccione **NODOS > nodo**.

Si la pestaña **Descripción general** incluye una entrada para **Grupos de HA**, el nodo se asigna a los grupos de HA enumerados. El valor después del nombre del grupo es el estado actual del nodo en el grupo HA:

- **Activo:** El grupo HA está alojado actualmente en este nodo.
- **Copia de seguridad:** El grupo HA no está utilizando actualmente este nodo; esta es una interfaz de copia de seguridad.
- **Detenido:** El grupo HA no se puede alojar en este nodo porque el servicio de alta disponibilidad (keepalived) se detuvo manualmente.
- **Error:** El grupo HA no se puede alojar en este nodo debido a uno o más de los siguientes motivos:
 - 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 caído.

En este ejemplo, el nodo de administración principal se ha agregado a dos grupos de alta disponibilidad. Este nodo es actualmente la interfaz activa para el grupo de clientes de administración y una interfaz de respaldo para el grupo de clientes de FabricPool .

DC1-ADM1 (Primary Admin Node) [🔗](#)

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Load balancer](#) [Tasks](#)

Node information [?](#)

Name:	DC1-ADM1
Type:	Primary Admin Node
ID:	ce00d9c8-8a79-4742-bdef-c9c658db5315
Connection state:	✔ Connected
Software version:	11.6.0 (build 20211207.1804.614bc17)
HA groups:	Admin clients (Active) FabricPool clients (Backup)
IP addresses:	172.16.1.225 - eth0 (Grid Network) 10.224.1.225 - eth1 (Admin Network) 47.47.0.2, 47.47.1.225 - eth2 (Client Network) Show additional IP addresses ▼

¿Qué sucede cuando falla la interfaz activa?

La interfaz que actualmente aloja las direcciones VIP es la interfaz activa. Si el grupo HA incluye más de una interfaz y la interfaz activa falla, las direcciones VIP se mueven a la primera interfaz de respaldo disponible en el orden de prioridad. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de respaldo disponible, y así sucesivamente.

La conmutación por error se puede activar por cualquiera de estos motivos:

- El nodo en el que está configurada la interfaz deja de funcionar.
- El nodo en el que está configurada la interfaz pierde 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 por fallas de red externas al nodo que aloja la interfaz activa. De manera similar, la conmutación por error no es activada por los servicios del Administrador de red o del Administrador de inquilinos.

El proceso de conmutación por error generalmente toma sólo unos segundos y es lo suficientemente rápido como para que las aplicaciones cliente experimenten poco impacto y puedan confiar en los comportamientos de reintento normales para continuar la operación.

Cuando se resuelve la falla y vuelve a estar disponible una interfaz de mayor prioridad, las direcciones VIP se mueven automáticamente a la interfaz de mayor prioridad que esté disponible.

¿Cómo se utilizan los grupos HA?

Puede utilizar grupos de alta disponibilidad (HA) para proporcionar conexiones de alta disponibilidad a StorageGRID para datos de objetos y para uso administrativo.

- Un grupo HA puede proporcionar conexiones administrativas de alta disponibilidad al administrador de red o al administrador de inquilinos.
- Un grupo HA puede proporcionar conexiones de datos de alta disponibilidad para clientes S3.
- Un grupo HA que contiene solo una interfaz le permite proporcionar muchas direcciones VIP y configurar explícitamente direcciones IPv6.

Un grupo de alta disponibilidad solo puede proporcionar alta disponibilidad si todos los nodos incluidos en el grupo brindan los mismos servicios. Al crear un grupo de alta disponibilidad, agregue interfaces de los tipos de nodos que brindan los servicios que necesita.

- **Nodos de administración:** incluye el servicio Load Balancer y habilita el acceso al Grid Manager o al Tenant Manager.
- **Nodos de puerta de enlace:** incluye el servicio Load Balancer.

Propósito del grupo HA	Agregue nodos de este tipo al grupo HA
Acceso al Administrador de Red	• Nodo de administración principal (Principal) • Nodos de administración no principales Nota: El nodo de administración principal debe ser la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.
Acceso únicamente al administrador de inquilinos	• Nodos de administración primarios o no primarios
Acceso de cliente S3: servicio Load Balancer	• Nodos de administración • Nodos de puerta de enlace
Acceso de cliente S3 para " S3 Seleccionar "	• Servicios de electrodomésticos • Nodos de software basados en VMware Nota: Se recomiendan grupos HA cuando se utiliza S3 Select, pero no son obligatorios.

Limitaciones del uso de grupos de alta disponibilidad con Grid Manager o Tenant Manager

Si falla un servicio de Grid Manager o Tenant Manager, no se activa la conmutación por error del grupo HA.

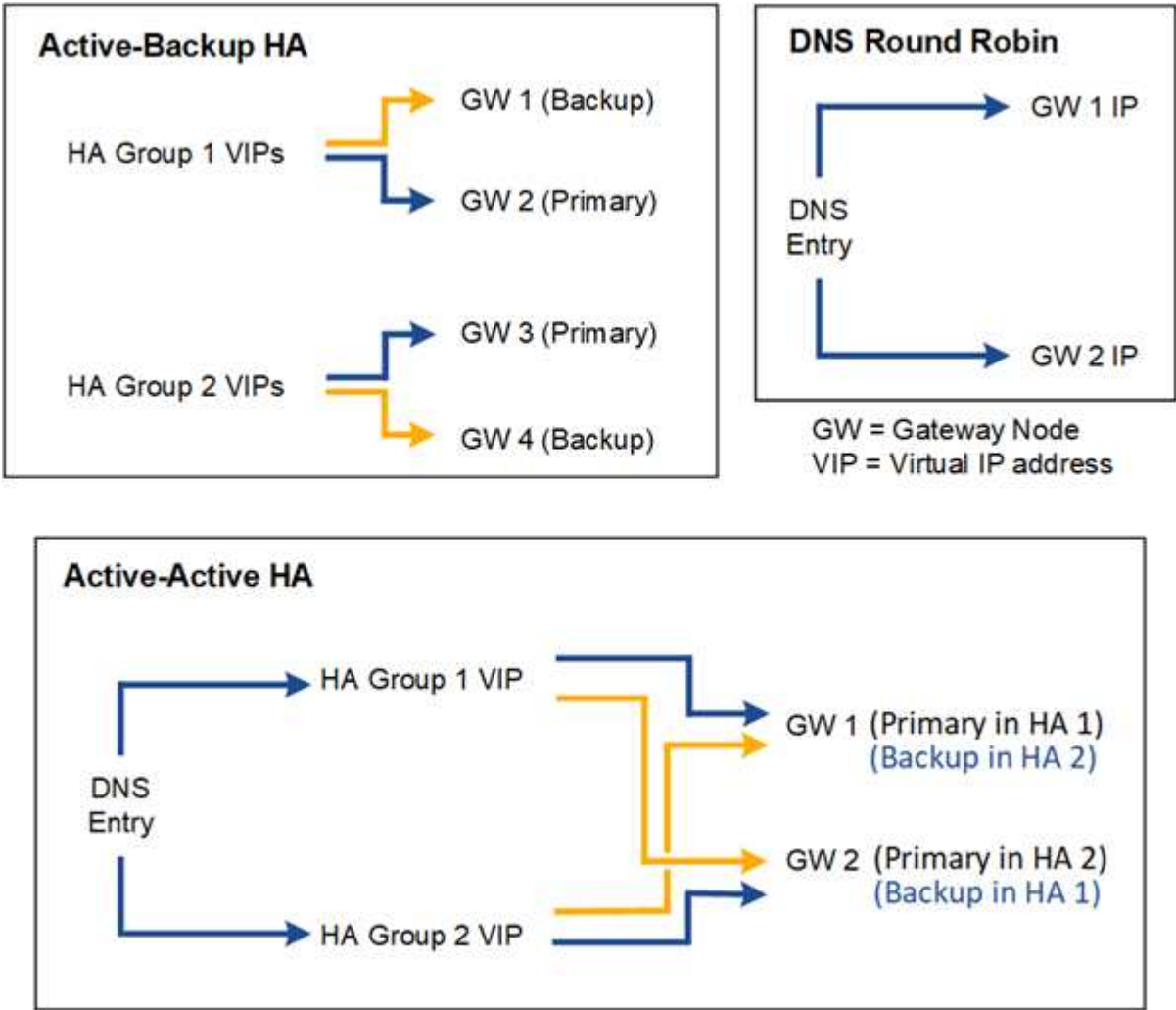
Si ha iniciado sesión en Grid Manager o Tenant Manager cuando se produce una conmutación por error, cerrará la sesión y deberá iniciar sesión nuevamente para reanudar su tarea.

Algunos procedimientos de mantenimiento no se pueden realizar cuando el nodo de administración principal no está disponible. Durante la conmutación por error, puede utilizar el Administrador de cuadrícula para supervisar su sistema StorageGRID .

Opciones de configuración para grupos de alta disponibilidad

Los siguientes diagramas proporcionan ejemplos de diferentes formas en las que se pueden configurar grupos de HA. Cada opción tiene ventajas y desventajas.

En los diagramas, el azul indica la interfaz principal en el grupo HA y el amarillo indica la interfaz de respaldo en el grupo HA.



La tabla resume los beneficios de cada configuración de HA que se muestra en el diagrama.

Configuración	Ventajas	Desventajas
Alta disponibilidad de respaldo activo	• Administrado por StorageGRID sin dependencias externas. • Conmutación por error rápida.	• Solo un nodo en un grupo HA está activo. Al menos un nodo por grupo HA estará inactivo.

Configuración	Ventajas	Desventajas
DNS Round Robin	• Aumento del rendimiento agregado. • No hay hosts inactivos.	• Conmutación por error lenta, que podría depender del comportamiento del cliente. • Requiere configuración de hardware fuera de StorageGRID. • Necesita un control de salud implementado por el cliente.
HA activo-activo	• El tráfico se distribuye entre varios grupos de alta disponibilidad. • Alto rendimiento agregado que escala con la cantidad de grupos de HA. • Conmutación por error rápida.	• Más complejo de configurar. • Requiere configuración de hardware fuera de StorageGRID. • Necesita un control de salud implementado por el cliente.

Configurar grupos de alta disponibilidad

Puede 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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Si planea utilizar una interfaz VLAN en un grupo HA, habrá creado la interfaz VLAN. Ver ["Configurar interfaces VLAN"](#) .
- Si planea utilizar una interfaz de acceso para un nodo en un grupo de alta disponibilidad, ha creado la interfaz:
 - **Red Hat Enterprise Linux (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Ubuntu o Debian (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Linux (después de instalar el nodo):** ["Linux: Agregar interfaces troncales o de acceso a un nodo"](#)
 - **VMware (después de instalar el nodo):** ["VMware: Agregar interfaces troncales o de acceso a un nodo"](#)

Crear un grupo de alta disponibilidad

Cuando se crea un grupo de alta disponibilidad, se selecciona una o más interfaces y se organizan en orden de prioridad. Luego, asigna una o más direcciones VIP al grupo.

Una interfaz debe ser para que un nodo de puerta de enlace o un nodo de administración se incluya en un grupo de alta disponibilidad. Un grupo de HA solo puede usar una interfaz para un nodo determinado; sin embargo, se pueden usar otras interfaces para el mismo nodo en otros grupos de HA.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
2. Seleccione **Crear**.

Introduzca detalles para el grupo HA

Pasos

1. Proporcione un nombre único para el grupo HA.
2. Opcionalmente, ingrese una descripción para el grupo HA.
3. Seleccione **Continuar**.

Agregar interfaces al grupo HA

Pasos

1. Seleccione una o más interfaces para agregar a este grupo de HA.

Utilice los encabezados de columna para ordenar las filas o ingrese un término de búsqueda para localizar interfaces más rápidamente.

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

?

Total interface count: 4

	Node	Interface	Site	IPv4 subnet	Node type
☐	DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
☐	DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
☐	DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
☐	DC2-ADM1-104-103	eth2	DC2	—	Admin Node

0 interfaces selected



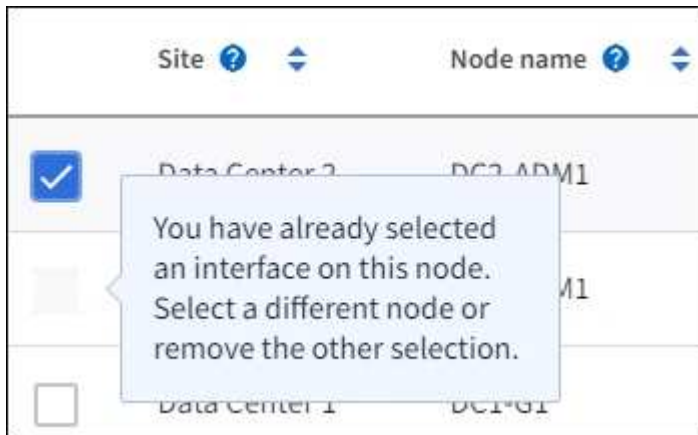
Después de crear una interfaz VLAN, espere hasta 5 minutos para que la nueva interfaz aparezca en la tabla.

Directrices para la selección de interfaces

- Debes seleccionar al menos una interfaz.
- Puede seleccionar solo una interfaz para un nodo.
- Si el grupo HA es para la protección de HA de los servicios del nodo de administración, que incluyen el administrador de red y el administrador de inquilinos, seleccione interfaces solo en los nodos de administración.
- Si el grupo HA es para la protección de HA del tráfico del cliente S3, seleccione interfaces en los

nodos de administración, los nodos de puerta de enlace o ambos.

- Si selecciona interfaces en diferentes tipos de nodos, aparece una nota informativa. Se le recuerda que si se produce una conmutación por error, es posible que los servicios proporcionados por el nodo previamente activo no estén disponibles en el nuevo nodo activo. Por ejemplo, un nodo de puerta de enlace de respaldo no puede brindar protección de alta disponibilidad a los servicios del nodo de administración. De manera similar, un nodo de administración de respaldo no puede realizar todos los procedimientos de mantenimiento que el nodo de administración principal puede proporcionar.
- Si no puede seleccionar una interfaz, su casilla de verificación estará deshabilitada. La información sobre herramientas proporciona más información.



- No puede seleccionar una interfaz si su valor de subred o puerta de enlace entra en conflicto con otra interfaz seleccionada.
- No puede seleccionar una interfaz configurada si no tiene una dirección IP estática.

2. Seleccione **Continuar**.

Determinar el orden de prioridad

Si el grupo HA incluye más de una interfaz, puede determinar cuál es la interfaz principal y cuáles son las interfaces de respaldo (conmutación por error). Si la interfaz principal falla, las direcciones VIP se mueven a la interfaz de mayor prioridad que esté disponible. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de mayor prioridad que esté disponible, y así sucesivamente.

Pasos

1. Arrastre filas en la columna **Orden de prioridad** para determinar la interfaz principal y cualquier interfaz de respaldo.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order ?	Node	Interface ?	Node type ?
1 (Primary interface)	⬆ DC1-ADM1-104-96	eth2	Primary Admin Node
2	⬆ DC2-ADM1-104-103	eth2	Admin Node



Si el grupo HA proporciona acceso al Administrador de red, debe seleccionar una interfaz en el Nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

2. Seleccione **Continuar**.

Introduzca direcciones IP

Pasos

1. En el campo **Subred CIDR**, especifique 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 configurado. Por ejemplo, 192.16.0.0/22.



Si utiliza un prefijo de 32 bits, la dirección de red VIP también sirve como dirección de puerta de enlace y dirección VIP.

Enter details for the HA group

Subnet CIDR ?

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional) ?

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address ?

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

- De manera opcional, si algún cliente administrativo o inquilino de S3 accederá a estas direcciones VIP desde una subred diferente, ingrese la **dirección IP de puerta de enlace**. La dirección de la puerta de enlace debe estar dentro de la subred VIP.

Los usuarios clientes y administradores utilizarán esta puerta de enlace para acceder a las direcciones IP virtuales.

- Ingrese al menos una y no más de diez direcciones VIP para la interfaz activa en el grupo HA. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa.

Debe proporcionar al menos una dirección IPv4. Opcionalmente, puede especificar direcciones IPv4 e IPv6 adicionales.

- Seleccione **Crear grupo HA** y seleccione **Finalizar**.

Se crea el grupo HA y ahora puede utilizar las direcciones IP virtuales configuradas.

Próximos pasos

Si va a utilizar este grupo HA para equilibrar la carga, cree un punto final del equilibrador de carga para determinar el puerto y el protocolo de red y para adjuntar los certificados necesarios. Ver ["Configurar los puntos finales del balanceador de carga"](#).

Editar un grupo de alta disponibilidad

Puede editar un grupo de alta disponibilidad (HA) para cambiar su nombre y descripción, agregar o eliminar interfaces, cambiar el orden de prioridad o agregar o actualizar direcciones IP virtuales.

Por ejemplo, es posible que necesite editar un grupo de alta disponibilidad si desea eliminar el nodo asociado

con una interfaz seleccionada en un procedimiento de desmantelamiento de sitio o nodo.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.

La página Grupos de alta disponibilidad muestra todos los grupos de alta disponibilidad existentes.

2. Seleccione la casilla de verificación del grupo HA que desea editar.
3. Realice una de las siguientes acciones, según lo que desee actualizar:
 - Seleccione **Acciones > Editar dirección IP virtual** para agregar o eliminar direcciones VIP.
 - Seleccione **Acciones > Editar grupo de HA** para actualizar el nombre o la descripción del grupo, agregar o eliminar interfaces, cambiar el orden de prioridad o agregar o eliminar direcciones VIP.
4. Si seleccionó **Editar dirección IP virtual**:
 - a. Actualice las direcciones IP virtuales para el grupo HA.
 - b. Seleccione **Guardar**.
 - c. Seleccione **Finalizar**.
5. Si seleccionó **Editar grupo HA**:
 - a. Opcionalmente, actualice el nombre o la descripción del grupo.
 - b. Opcionalmente, seleccione o desmarque las casillas de verificación para agregar o eliminar interfaces.



Si el grupo HA proporciona acceso al Administrador de red, debe seleccionar una interfaz en el Nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal

- c. Opcionalmente, arrastre filas para cambiar el orden de prioridad de la interfaz principal y cualquier interfaz de respaldo para este grupo de HA.
- d. Opcionalmente, actualice las direcciones IP virtuales.
- e. Seleccione **Guardar** y luego seleccione **Finalizar**.

Eliminar un grupo de alta disponibilidad

Puede eliminar uno o más grupos de alta disponibilidad (HA) a la vez.



No se puede eliminar un grupo de alta disponibilidad si está vinculado a un punto final del equilibrador de carga. Para eliminar un grupo de HA, debe quitarlo de todos los puntos finales del balanceador de carga que lo utilicen.

Para evitar interrupciones del cliente, actualice cualquier aplicación cliente S3 afectada antes de eliminar un grupo de alta disponibilidad. Actualice cada cliente para conectarse utilizando otra dirección IP, por ejemplo, la dirección IP virtual de un grupo de HA diferente o la dirección IP que se configuró para una interfaz durante la instalación.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
2. Revise la columna **Puntos finales del balanceador de carga** para cada grupo de HA que desee eliminar. Si se enumeran puntos finales del balanceador de carga:

- a. Vaya a **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
 - b. Seleccione la casilla de verificación para el punto final.
 - c. Seleccione **Acciones > Editar modo de enlace de punto final**.
 - d. Actualice el modo de enlace para eliminar el grupo HA.
 - e. Seleccione **Guardar cambios**.
3. Si no se enumeran puntos finales del balanceador de carga, seleccione la casilla de verificación para cada grupo de alta disponibilidad que desee eliminar.
 4. Seleccione **Acciones > Eliminar grupo HA**.
 5. Revise el mensaje y seleccione **Eliminar grupo HA** para confirmar su selección.

Se eliminan todos los grupos HA que seleccionó. Aparece un banner de éxito verde en la página de grupos de alta disponibilidad.

Gestionar el equilibrio de carga

Consideraciones para el equilibrio de carga

Puede utilizar el equilibrio de carga para gestionar cargas de trabajo de ingesta y recuperación de clientes S3.

¿Qué es el equilibrio de carga?

Cuando una aplicación cliente guarda o recupera datos de un sistema StorageGRID, StorageGRID utiliza un equilibrador de carga para administrar 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 múltiples nodos de almacenamiento.

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 seguridad de la capa de transporte (TLS) de las solicitudes de los clientes, inspecciona las solicitudes y establece nuevas conexiones seguras con los nodos de almacenamiento.

El servicio Load Balancer en cada nodo funciona de forma independiente al reenviar el tráfico del cliente 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.



Si bien el servicio StorageGRID Load Balancer es el mecanismo de equilibrio de carga recomendado, es posible que desee integrar un equilibrador de carga de terceros. Para obtener más información, comuníquese con su representante de cuenta de NetApp o consulte ["TR-4626: Balanceadores de carga globales y de terceros de StorageGRID"](#).

¿Cuántos nodos de equilibrio de carga necesito?

Como práctica recomendada general, cada sitio en su sistema StorageGRID debe incluir dos o más nodos con el servicio Load Balancer. Por ejemplo, un sitio puede incluir dos nodos de puerta de enlace o un nodo de administración y un nodo de puerta de enlace. Asegúrese de que haya una infraestructura de red, hardware o virtualización adecuada para cada nodo de equilibrio de carga, independientemente de que utilice dispositivos de servicios, nodos físicos o nodos basados en máquinas virtuales (VM).

¿Qué es un punto final de balanceador de carga?

Un punto final del balanceador de carga define el puerto y el protocolo de red (HTTPS o HTTP) que las solicitudes de aplicaciones cliente entrantes y salientes utilizarán para acceder a aquellos nodos que contienen el servicio del balanceador de carga. 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 punto final del balanceador de carga, seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga** o complete el asistente de configuración de FabricPool y S3. Para obtener instrucciones:

- ["Configurar los puntos finales del balanceador de carga"](#)
- ["Utilice el asistente de configuración de S3"](#)
- ["Utilice el asistente de configuración de FabricPool"](#)

Consideraciones para el puerto

El puerto para un punto final del balanceador de carga tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede especificar cualquier puerto externo no utilizado entre 1 y 65535. Si usa el puerto 80 o 443, el punto final utilizará el servicio Load Balancer solo en los nodos de puerta de enlace. Estos puertos están reservados en los nodos de administración. Si utiliza el mismo puerto para más de un punto final, debe especificar un modo de enlace diferente para cada punto final.

No se permiten puertos utilizados por otros servicios de la red. Ver el ["Referencia del puerto de red"](#).

Consideraciones para el protocolo de red

En la mayoría de los casos, las conexiones entre las aplicaciones cliente y StorageGRID deben utilizar el cifrado de seguridad de la capa de transporte (TLS). Se admite la conexión a StorageGRID sin cifrado TLS, pero no se recomienda, especialmente en entornos de producción. Al seleccionar el protocolo de red para el punto final del balanceador de carga StorageGRID, debe seleccionar **HTTPS**.

Consideraciones sobre los certificados de punto final del equilibrador de carga

Si selecciona **HTTPS** como protocolo de red para el punto final del balanceador de carga, deberá proporcionar un certificado de seguridad. Puede utilizar cualquiera de estas tres opciones al crear el punto final del equilibrador de carga:

- **Subir un certificado firmado (recomendado).** Este certificado puede estar firmado por una autoridad de certificación (CA) privada o de confianza pública. La mejor práctica es utilizar un certificado de servidor CA de confianza pública para proteger la conexión. A diferencia de los certificados generados, los certificados firmados por una CA se pueden rotar sin interrupciones, lo que puede ayudar a evitar problemas de vencimiento.

Debe obtener los siguientes archivos antes de crear el punto final del equilibrador de carga:

- El archivo de certificado de servidor personalizado.
- El archivo de 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.**
- **Utilice el certificado global StorageGRID S3.** Debe cargar o generar una versión personalizada de este

certificado antes de poder seleccionarlo para el punto final del balanceador de carga. Ver ["Configurar certificados de API S3"](#).

¿Qué valores necesito?

Para crear el certificado, debe conocer todos los nombres de dominio y direcciones IP que las aplicaciones cliente S3 usarán para acceder al punto final.

La entrada **DN del sujeto** (nombre distinguido) del certificado debe incluir el nombre de dominio completo que la aplicación cliente utilizará para StorageGRID. Por ejemplo:

```
Subject DN:
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

Según sea necesario, el certificado puede usar caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración y nodos de puerta de enlace que ejecutan el servicio Load Balancer. Por ejemplo, `*.storagegrid.example.com` utiliza el comodín `*` para representar `adm1.storagegrid.example.com` y `gn1.storagegrid.example.com`.

Si planea utilizar solicitudes alojadas virtuales de estilo S3, el certificado también debe incluir una entrada **Nombre alternativo** para cada una. ["Nombre de dominio del punto final S3"](#) que haya configurado, incluidos los nombres comodín. Por ejemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```



Si utiliza comodines para los nombres de dominio, revise la ["Pautas de refuerzo para certificados de servidor"](#).

También debe definir una entrada DNS para cada nombre en el certificado de seguridad.

¿Cómo gestiono los certificados que expiran?



Si el certificado utilizado para proteger la conexión entre la aplicación S3 y StorageGRID caduca, la aplicación podría perder temporalmente el acceso a StorageGRID.

Para evitar problemas de vencimiento de certificados, siga estas prácticas recomendadas:

- Supervise atentamente cualquier alerta que advierta sobre fechas de vencimiento de certificados próximas, como las alertas **Vencimiento del certificado del punto final del equilibrador de carga** y **Vencimiento del certificado del servidor global para la API de S3**.
- Mantenga siempre sincronizadas las versiones del certificado de StorageGRID y de la aplicación S3. Si reemplaza o renueva el certificado utilizado para un punto final del balanceador de carga, debe reemplazar o renovar el certificado equivalente utilizado por la aplicación S3.
- Utilice un certificado CA firmado públicamente. Si utiliza un certificado firmado por una CA, puede reemplazar certificados que estén próximos a vencer sin interrupciones.
- Si ha generado un certificado StorageGRID autofirmado y dicho certificado está a punto de caducar, debe reemplazarlo manualmente tanto en StorageGRID como en la aplicación S3 antes de que caduque el certificado existente.

Consideraciones para el modo de enlace

El modo de enlace le permite controlar qué direcciones IP se pueden usar para acceder a un punto final del balanceador de carga. Si un punto final utiliza un modo de enlace, las aplicaciones cliente solo pueden acceder al punto final si usan una dirección IP permitida o su nombre de dominio completo (FQDN) correspondiente. Las aplicaciones cliente que utilicen cualquier otra dirección IP o FQDN no pueden acceder al punto final.

Puede especificar cualquiera de los siguientes modos de enlace:

- **Global** (predeterminado): Las aplicaciones cliente pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice esta configuración a menos que necesite restringir la accesibilidad de un punto final.
- **IP virtuales de grupos HA**. Las aplicaciones cliente deben utilizar una dirección IP virtual (o FQDN correspondiente) de un grupo de alta disponibilidad.
- **Interfaces de nodo**. Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas.
- **Tipo de nodo**. Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace.

Consideraciones para el acceso de los inquilinos

El acceso de inquilinos es una función de seguridad opcional que le permite controlar qué cuentas de inquilinos de StorageGRID pueden usar un punto final del balanceador de carga para acceder a sus buckets. Puede permitir que todos los inquilinos accedan a un punto final (predeterminado) o puede especificar una lista de inquilinos permitidos o bloqueados para cada punto final.

Puede utilizar esta función para proporcionar un mejor aislamiento de seguridad entre los inquilinos y sus puntos finales. Por ejemplo, puede utilizar esta función para garantizar que los materiales altamente clasificados o de alto secreto propiedad de un inquilino permanezcan completamente inaccesibles para los demás inquilinos.



A los 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 en el caso del acceso anónimo), se utiliza el propietario del depósito para determinar el inquilino.

Ejemplo de acceso de inquilinos

Para comprender cómo funciona esta característica de seguridad, considere el siguiente ejemplo:

1. Ha creado dos puntos finales de equilibrador de carga, de la siguiente manera:
 - Punto final **público**: utiliza el puerto 10443 y permite el acceso a todos los inquilinos.
 - Punto final **alto secreto**: utiliza el puerto 10444 y permite el acceso únicamente al inquilino **alto secreto**. Todos los demás inquilinos tienen bloqueado el acceso a este punto final.
2. El `top-secret.pdf` está en un cubo propiedad del inquilino **alto secreto**.

Para acceder a la `top-secret.pdf`, un usuario en el inquilino **Top secret** puede emitir una solicitud GET a `https://w.x.y.z:10444/top-secret.pdf`. Debido a que a este inquilino se le permite usar el punto

final 10444, el usuario puede acceder al objeto. Sin embargo, si un usuario que pertenece a otro inquilino emite la misma solicitud a la misma URL, recibirá inmediatamente un mensaje de acceso denegado. Se deniega el acceso incluso si las credenciales y la firma son válidas.

Disponibilidad de CPU

El servicio Load Balancer en cada nodo de administración y nodo de puerta de enlace funciona de forma independiente al reenviar 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 mayor frecuencia. A todos los nodos de almacenamiento se les asigna un valor de peso base mínimo, incluso si un nodo informa una utilización del 100 % o no informa su utilización.

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

Configurar los puntos finales del balanceador de carga

Los puntos finales del balanceador de carga determinan los puertos y los protocolos de red que los clientes S3 pueden usar cuando se conectan al balanceador de carga StorageGRID en los nodos de puerta de enlace y de administración. También puede utilizar puntos finales para acceder al Administrador de red, al Administrador de inquilinos o a ambos.



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["Configurar conexiones de cliente S3 y Swift"](#).

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).
- Usted ha revisado el ["Consideraciones para el equilibrio de carga"](#).
- Si anteriormente reasignó un puerto que desea utilizar para el punto final del balanceador de carga, debe ["Se eliminó la reasignación del puerto"](#).
- Ha creado todos los grupos de alta disponibilidad (HA) que planea utilizar. Se recomiendan los grupos HA, pero no son obligatorios. Ver ["Administrar grupos de alta disponibilidad"](#).
- Si el punto final del balanceador de carga será utilizado por ["Inquilinos de S3 para S3 Select"](#), no debe utilizar las direcciones IP o FQDN de ningún nodo físico. Solo se permiten dispositivos de servicios y nodos de software basados en VMware para los puntos finales del equilibrador de carga utilizados para S3 Select.
- Ha configurado todas las interfaces VLAN que planea utilizar. Ver ["Configurar interfaces VLAN"](#).
- Si está creando un punto final HTTPS (recomendado), tiene la información del certificado del servidor.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

- Para cargar un certificado, necesita el certificado del servidor, la clave privada del certificado y, opcionalmente, un paquete de CA.
- Para generar un certificado, necesita todos los nombres de dominio y direcciones IP que los clientes S3 usarán para acceder al punto final. También debes conocer el tema (Nombre Distinguido).

- Si desea utilizar el certificado API S3 de StorageGRID (que también se puede usar para conexiones directas a nodos de almacenamiento), ya ha reemplazado el certificado predeterminado con un certificado personalizado firmado por una autoridad de certificación externa. Ver "[Configurar certificados de API S3](#)".

Crear un punto final de balanceador de carga

Cada punto final del balanceador de carga del cliente S3 especifica un puerto, un tipo de cliente (S3) y un protocolo de red (HTTP o HTTPS). Los puntos finales del balanceador de carga de la interfaz de administración especifican un puerto, un tipo de interfaz y una red de cliente no confiable.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
2. Para crear un punto final para un cliente S3 o Swift, seleccione la pestaña **Cliente S3 o Swift**.
3. Para crear un punto final para acceder al Administrador de red, al Administrador de inquilinos o a ambos, seleccione la pestaña **Interfaz de administración**.
4. Seleccione **Crear**.

Ingrese los detalles del punto final

Pasos

1. Seleccione las instrucciones adecuadas para ingresar detalles para el tipo de punto final que desea crear.

Cliente S3 o Swift

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final, que aparecerá en la tabla de la página Puntos finales del balanceador de carga.
Puerto	El puerto StorageGRID que desea utilizar para equilibrar la carga. Este campo tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede ingresar cualquier puerto externo no utilizado del 1 al 65535. Si ingresa 80 o 8443, el punto final se configura solo en los nodos de puerta de enlace, a menos que haya liberado el puerto 8443. Luego, puede usar el puerto 8443 como punto final S3, y el puerto se configurará tanto en los nodos de puerta de enlace como en los de administración.
Tipo de cliente	El tipo de aplicación cliente que utilizará este punto final, ya sea S3 o Swift .
Protocolo de red	El protocolo de red que utilizarán los clientes cuando se conecten a este punto final. • Seleccione HTTPS para una comunicación segura y cifrada con TLS (recomendado). Debe adjuntar un certificado de seguridad antes de poder guardar el punto final. • Seleccione HTTP para una comunicación menos segura y sin cifrar. Utilice HTTP únicamente para una cuadrícula que no sea de producción.

Interfaz de gestión

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final, que aparecerá en la tabla de la página Puntos finales del balanceador de carga.
Puerto	El puerto StorageGRID que desea utilizar para acceder al Administrador de Grid, al Administrador de inquilinos o a ambos. • Administrador de red: 8443 • Gerente de inquilinos: 9443 • Tanto el administrador de la red como el administrador de inquilinos: 443 Nota: Puede utilizar estos puertos preestablecidos u otros puertos disponibles.
Tipo de interfaz	Seleccione el botón de opción para la interfaz StorageGRID a la que accederá mediante este punto final.

Campo	Descripción
Red de clientes no confiables	Seleccione Sí si este punto final debe ser accesible para redes de clientes que no son de confianza. De lo contrario, seleccione No. Cuando selecciona Sí, el puerto se abre en todas las redes de cliente que no son de confianza. Nota: Solo puede configurar un puerto para que esté abierto o cerrado para redes de clientes que no sean de confianza cuando crea el punto final del balanceador de carga.

1. Seleccione **Continuar**.

Seleccionar un modo de enlace

Pasos

1. Seleccione un modo de enlace para el punto final para controlar cómo se accede a él utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Algunos modos de enlace están disponibles para puntos finales de cliente o puntos finales de interfaz de administración. Aquí se enumeran todos los modos para ambos tipos de puntos finales.

Modo	Descripción
Global (predeterminado para puntos finales del cliente)	Los clientes pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice la configuración Global a menos que necesite restringir la accesibilidad de este punto final.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o FQDN correspondiente) de un grupo de HA para acceder a este punto final. Todos los puntos finales con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de HA que seleccione para los puntos finales no se superpongan.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo (solo puntos finales del cliente)	Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este punto final.

Modo	Descripción
Todos los nodos de administración (predeterminado para los puntos finales de la interfaz de administración)	Los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración para acceder a este punto final.

Si más de un punto final usa el mismo puerto, StorageGRID usa este orden de prioridad para decidir qué punto final usar: **IP virtuales de grupos de alta disponibilidad > Interfaces de nodo > Tipo de nodo > Global**.

Si está creando puntos finales de interfaz de administración, solo se permiten nodos de administración.

2. Si seleccionó **IP virtuales de grupos de HA**, seleccione uno o más grupos de HA.

Si está creando puntos finales de interfaz de administración, seleccione VIP asociados únicamente con nodos de administración.

3. Si seleccionó **Interfaces de nodo**, seleccione una o más interfaces de nodo para cada nodo de administración o nodo de puerta de enlace que desee asociar con este punto final.
4. Si seleccionó **Tipo de nodo**, seleccione Nodos de administración, que incluye tanto el nodo de administración principal como cualquier nodo de administración no principal, o Nodos de puerta de enlace.

Controlar el acceso de los inquilinos



Un punto final de interfaz de administración puede controlar el acceso de los inquilinos solo cuando el punto final tiene la [Tipo de interfaz del administrador de inquilinos](#).

Pasos

1. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (predeterminado)	Todas las cuentas de inquilinos pueden usar este punto final para acceder a sus depósitos. Debe seleccionar esta opción si aún no ha creado ninguna cuenta de inquilino. Después de agregar cuentas de inquilino, puede editar el punto final del balanceador de carga para permitir o bloquear cuentas específicas.
Permitir inquilinos seleccionados	Solo las cuentas de inquilinos seleccionadas pueden usar este punto final para acceder a sus depósitos.
Bloquear inquilinos seleccionados	Las cuentas de inquilinos seleccionadas no pueden usar este punto final para acceder a sus depósitos. Todos los demás inquilinos pueden utilizar este punto final.

2. Si está creando un punto final **HTTP**, no necesita adjuntar un certificado. Seleccione **Crear** para agregar el

nuevo punto final del balanceador de carga. Luego, ve a [Después de terminar](#) . De lo contrario, seleccione **Continuar** para adjuntar el certificado.

Adjuntar certificado

Pasos

1. Si está creando un punto final **HTTPS**, seleccione el tipo de certificado de seguridad que desea adjuntar al punto final.

El certificado protege las conexiones entre los clientes S3 y el servicio Load Balancer en los nodos de administración o de puerta de enlace.

- **Subir certificado.** Seleccione esta opción si tiene certificados personalizados para cargar.
- **Generar certificado.** Seleccione esta opción si tiene los valores necesarios para generar un certificado personalizado.
- **Utilice el certificado StorageGRID S3.** Seleccione esta opción si desea utilizar el certificado API S3 global, que también se puede usar para conexiones directas a nodos de almacenamiento.

No puede seleccionar esta opción a menos que haya reemplazado el certificado API S3 predeterminado, que está firmado por la CA de la red, con un certificado personalizado firmado por una autoridad de certificación externa. Ver "[Configurar certificados de API S3](#)".

- **Utilizar certificado de interfaz de administración.** Seleccione esta opción si desea utilizar el certificado de interfaz de administración global, que también se puede utilizar para conexiones directas a los nodos de administración.
2. Si no está utilizando el certificado StorageGRID S3, cargue o genere el certificado.

Subir certificado

a. Seleccione **Subir certificado**.

b. Cargue los archivos de certificado de servidor necesarios:

- **Certificado de servidor:** el archivo de certificado de servidor personalizado en codificación PEM.
- **Clave privada del certificado:** El archivo de clave privada del certificado del servidor personalizado(`.key`).



Las claves privadas EC deben tener 224 bits o más. Las claves privadas RSA deben tener 2048 bits o más.

- **Paquete 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 certificado CA codificados en PEM, concatenados en el orden de la cadena de certificados.

c. Expande **Detalles del certificado** para ver los metadatos de cada certificado que hayas cargado. Si cargó un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Seleccione **Crear**. + Se crea el punto final del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones posteriores entre los clientes S3 o la interfaz de administración y el punto final.

Generar certificado

a. Seleccione **Generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más nombres de dominio completos para incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
Propiedad intelectual	Una o más direcciones IP para incluir en el certificado.
Asunto (opcional)	Sujeto X.509 o nombre distinguido (DN) del propietario del certificado. Si no se ingresa ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o dirección IP como nombre común del sujeto (CN).

Campo	Descripción
Días válidos	Número de días después de su creación que expira el certificado.
Agregar extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y uso de clave extendido se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. Nota: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **Generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Seleccione **Crear**.

Se crea el punto final del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones posteriores entre los clientes S3 o la interfaz de administración y este punto final.

Después de terminar

Pasos

1. Si utiliza un DNS, asegúrese de que el DNS incluya un registro para asociar el nombre de dominio completo (FQDN) de StorageGRID a cada dirección IP que los clientes usarán para realizar conexiones.

La dirección IP que ingrese en el registro DNS depende de si está utilizando un grupo HA de nodos de equilibrio de carga:

- Si ha configurado un grupo de alta disponibilidad, los clientes se conectarán a las direcciones IP virtuales de ese grupo de alta disponibilidad.
- Si no utiliza un grupo de alta disponibilidad, los clientes se conectarán al servicio StorageGRID Load Balancer mediante la dirección IP de un nodo de puerta de enlace o de administración.

También debe asegurarse de que el registro DNS haga referencia a todos los nombres de dominio de punto final requeridos, incluidos todos los nombres comodín.

2. Proporcionar a los clientes S3 la información necesaria para conectarse al punto final:

- Número de puerto
- Nombre de dominio completo o dirección IP
- Cualquier detalle del certificado requerido

Ver y editar puntos finales del balanceador de carga

Puede ver los detalles de los puntos finales del balanceador de carga existentes, incluidos los metadatos del certificado para un punto final seguro. Puede cambiar ciertas configuraciones para un punto final.

- Para ver información básica de todos los puntos finales del balanceador de carga, revise las tablas en la página Puntos finales del balanceador de carga.
- Para ver todos los detalles sobre un punto final específico, incluidos los metadatos del certificado, seleccione el nombre del punto final en la tabla. La información mostrada varía según el tipo de punto final y cómo esté configurado.

S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb

Remove

Binding mode

Certificate

Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

Edit binding mode

Binding mode: Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- Para editar un punto final, utilice el menú **Acciones** en la página Puntos finales del balanceador de carga.



Si pierde el acceso a Grid Manager mientras edita el puerto de un punto final de la interfaz de administración, actualice la URL y el puerto para recuperar el acceso.



Después de editar un punto final, es posible que deba esperar hasta 15 minutos para que los cambios se apliquen a todos los nodos.

Tarea	Menú de acciones	Página de detalles
Editar el nombre del punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar nombre del punto final. c. Introduzca el nuevo nombre. d. Seleccione Guardar.	a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione el icono de edición  . c. Introduzca el nuevo nombre. d. Seleccione Guardar.
Editar el puerto del punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar puerto de punto final c. Introduzca un número de puerto válido. d. Seleccione Guardar.	<i>n / A</i>
Editar el modo de enlace del punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar modo de enlace de punto final. c. Actualice el modo de enlace según sea necesario. d. Seleccione Guardar cambios.	a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione Editar modo de enlace. c. Actualice el modo de enlace según sea necesario. d. Seleccione Guardar cambios.
Editar el certificado del punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar certificado de punto final. c. Cargue o genere un nuevo certificado personalizado o comience a utilizar el certificado S3 global, según sea necesario. d. Seleccione Guardar cambios.	a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione la pestaña Certificado. c. Seleccione Editar certificado. d. Cargue o genere un nuevo certificado personalizado o comience a utilizar el certificado S3 global, según sea necesario. e. Seleccione Guardar cambios.

Tarea	Menú de acciones	Página de detalles
Editar el acceso de los inquilinos	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar acceso de inquilino . c. Elija una opción de acceso diferente, seleccione o elimine inquilinos de la lista, o haga ambas cosas. d. Seleccione Guardar cambios .	a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione la pestaña Acceso de inquilinos . c. Seleccione Editar acceso de inquilino . d. Elija una opción de acceso diferente, seleccione o elimine inquilinos de la lista, o haga ambas cosas. e. Seleccione Guardar cambios .

Eliminar puntos finales del balanceador de carga

Puede eliminar uno o más puntos finales mediante el menú **Acciones**, o puede eliminar un solo punto final desde la página de detalles.



Para evitar interrupciones del cliente, actualice cualquier aplicación cliente S3 afectada antes de eliminar un punto final del balanceador de carga. Actualice cada cliente para conectarse usando un puerto asignado a otro punto final del balanceador de carga. Asegúrese de actualizar también cualquier información del certificado requerida.



Si pierde el acceso a Grid Manager mientras elimina un punto final de la interfaz de administración, actualice la URL.

- Para eliminar uno o más puntos finales:
 - Desde la página Balanceador de carga, seleccione la casilla de verificación para cada punto final que desee eliminar.
 - Seleccione **Acciones > Eliminar**.
 - Seleccione **Aceptar**.
- Para eliminar un punto final de la página de detalles:
 - Desde la página Balanceador de carga, seleccione el nombre del punto final.
 - Seleccione **Eliminar** en la página de detalles.
 - Seleccione **Aceptar**.

Configurar nombres de dominio de puntos finales S3

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



No se admite el uso de una dirección IP para un nombre de dominio de punto final. Las versiones futuras evitarán esta configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Ha confirmado que no hay ninguna actualización de la red en curso.



No realice ningún cambio en la configuración del nombre de dominio cuando haya una actualización de la red en curso.

Acerca de esta tarea

Para permitir que los clientes utilicen nombres de dominio de punto final S3, debe realizar todo lo siguiente:

- Utilice Grid Manager para agregar los nombres de dominio del punto final S3 al sistema StorageGRID .
- Asegúrese de que el ["Certificado que el cliente utiliza para conexiones HTTPS a StorageGRID"](#) Está firmado para todos los nombres de dominio que requiera el cliente.

Por ejemplo, si el punto final es `s3.company.com` , debe asegurarse de que el certificado utilizado para las conexiones HTTPS incluya el `s3.company.com` punto final y el nombre alternativo del sujeto (SAN) comodín del punto final: `*.s3.company.com` .

- Configurar el servidor DNS utilizado por el cliente. Incluya registros DNS para las direcciones IP que los clientes usan para realizar conexiones y asegúrese de que los registros hagan referencia a todos los nombres de dominio de punto final S3 requeridos, incluidos todos los nombres comodín.



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. Debe comprender cómo se conectan las aplicaciones cliente a la red para incluir las direcciones IP correctas en los registros DNS.

Los clientes que utilizan conexiones HTTPS (recomendadas) a la red pueden usar cualquiera de estos certificados:

- Los clientes que se conectan a un punto final del equilibrador de carga pueden usar un certificado personalizado para ese punto final. Cada punto final del equilibrador de carga se puede configurar para reconocer diferentes nombres de dominio de punto final S3.
- Los clientes que se conectan a un punto final del balanceador de carga o directamente a un nodo de almacenamiento pueden personalizar el certificado API S3 global para incluir todos los nombres de dominio de punto final S3 requeridos.



Si no agrega nombres de dominio de punto final S3 y la lista está vacía, se deshabilita la compatibilidad con solicitudes de estilo alojado virtualmente S3.

Agregar un nombre de dominio de punto final S3

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Nombres de dominio de punto final S3**.
2. Introduzca el nombre de dominio en el campo **Nombre de dominio 1**. Seleccione **Agregar otro nombre de dominio** para agregar más nombres de dominio.
3. Seleccione **Guardar**.

4. Asegúrese de que los certificados de servidor que utilizan los clientes coincidan con los nombres de dominio de punto final S3 requeridos.
 - Si los clientes se conectan a un punto final del balanceador de carga que utiliza su propio certificado, ["Actualizar el certificado asociado con el punto final"](#) .
 - Si los clientes se conectan a un punto final del balanceador de carga que utiliza el certificado de API S3 global o directamente a los nodos de almacenamiento, ["actualizar el certificado API global de S3"](#) .
5. Agregue los registros DNS necesarios para garantizar que se puedan resolver las solicitudes de nombre de dominio del punto final.

Resultado

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

Cambiar el nombre de un dominio de punto final S3

Si cambia un nombre utilizado por aplicaciones S3, las solicitudes de estilo alojado virtualmente fallarán.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Nombres de dominio de punto final S3**.
2. Seleccione el campo de nombre de dominio que desea editar y realice los cambios necesarios.
3. Seleccione **Guardar**.
4. Seleccione **Sí** para confirmar su cambio.

Eliminar un nombre de dominio de punto final S3

Si elimina un nombre utilizado por aplicaciones S3, las solicitudes de estilo alojado virtualmente fallarán.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Nombres de dominio de punto final S3**.
2. Seleccione el icono de eliminar  junto al nombre de dominio.
3. Seleccione **Sí** para confirmar la eliminación.

Información relacionada

- ["Utilice la API REST de S3"](#)
- ["Ver direcciones IP"](#)
- ["Configurar grupos de alta disponibilidad"](#)

Resumen: Direcciones IP y puertos para conexiones de cliente

Para almacenar o recuperar objetos, las aplicaciones cliente S3 se conectan al servicio Load Balancer, que está incluido en todos los nodos de administración y nodos de puerta de enlace, o al servicio Local Distribution Router (LDR), que está incluido en todos los nodos de almacenamiento.

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, puede crear grupos de alta disponibilidad (HA) de nodos de equilibrio de carga para proporcionar conexiones de alta disponibilidad que utilicen direcciones IP virtuales (VIP). Si desea conectarse a StorageGRID utilizando un nombre de dominio completo (FQDN) en

lugar de una dirección IP o VIP, puede 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 ha creado puntos finales de equilibrador de carga y grupos de alta disponibilidad (HA), consulte [Dónde encontrar direcciones IP](#) para localizar estos valores en el Administrador de cuadrícula.

Donde se establece la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Grupo HA	Balanceador de carga	Dirección IP virtual de un grupo de alta disponibilidad	Puerto asignado al punto final del balanceador de carga
Nodo de administración	Balanceador de carga	Dirección IP del nodo de administración	Puerto asignado al punto final del balanceador de carga
Nodo de puerta de enlace	Balanceador de carga	Dirección IP del nodo de enlace	Puerto asignado al punto final del balanceador de carga
Nodo de almacenamiento	LDR	Dirección IP del nodo de almacenamiento	Puertos S3 predeterminados: • HTTPS: 18082 • HTTP: 18084

URL de ejemplo

Para conectar una aplicación cliente al punto final del balanceador de carga de un grupo de alta disponibilidad de nodos de puerta de enlace, utilice una URL estructurada como se muestra a continuación:

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

Por ejemplo, si la dirección IP virtual del grupo HA es 192.0.2.5 y el número de puerto del punto final del balanceador de carga es 10443, entonces una aplicación podría usar la siguiente URL para conectarse a StorageGRID:

`https://192.0.2.5:10443`

Dónde encontrar direcciones IP

1. Sign in en Grid Manager usando un ["navegador web compatible"](#).
2. Para encontrar la dirección IP de un nodo de la red:
 - a. Seleccione **NODOS**.
 - b. Seleccione el nodo de administración, el nodo de puerta de enlace o el nodo de almacenamiento al que desea conectarse.
 - c. Seleccione la pestaña **Descripción general**.
 - d. En la sección Información del nodo, anote las direcciones IP del nodo.

- e. Seleccione **Mostrar más** para ver las direcciones IPv6 y las asignaciones de interfaces.

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

- **eth0**: Red de cuadrícula
- **eth1**: Red de administración (opcional)
- **eth2**: Red de cliente (opcional)



Si está viendo un nodo de administración o un nodo de puerta de enlace y es el nodo activo en un grupo de alta disponibilidad, la dirección IP virtual del grupo de alta disponibilidad se muestra en eth2.

3. Para encontrar la dirección IP virtual de un grupo de alta disponibilidad:
 - a. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
 - b. En la tabla, anote la dirección IP virtual del grupo HA.
4. Para encontrar el número de puerto de un punto final del balanceador de carga:
 - a. Seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
 - b. Anote el número de puerto del punto final que desea utilizar.



Si el número de puerto es 80 o 443, el punto final se configura solo en los nodos de puerta de enlace, porque esos puertos están reservados en los nodos de administración. Todos los demás puertos se configuran tanto en los nodos de puerta de enlace como en los nodos de administración.

- c. Seleccione el nombre del punto final de la tabla.
- d. Confirme que el **Tipo de cliente** (S3) coincida con la aplicación cliente que utilizará el punto final.

Administrar redes y conexiones

Configurar los ajustes de red

Puede configurar varias configuraciones de red desde Grid Manager para ajustar el funcionamiento de su sistema StorageGRID .

Configurar interfaces VLAN

Puede [crear interfaces de LAN virtual \(VLAN\)](#) para aislar y particionar el tráfico para garantizar la seguridad, la flexibilidad y el rendimiento. Cada interfaz VLAN está asociada con una o más interfaces principales en los nodos de administración y los nodos de puerta de enlace. Puede usar interfaces VLAN en grupos de alta disponibilidad y en puntos finales del balanceador de carga para segregar el tráfico de clientes o administradores por aplicación o inquilino.

Políticas de clasificación de tráfico

Puedes utilizar [políticas de clasificación de tráfico](#) para identificar y gestionar diferentes tipos de tráfico de red, incluido el tráfico relacionado con buckets, inquilinos, subredes de clientes o puntos finales de balanceador de carga específicos. Estas políticas pueden ayudar a limitar y monitorear el tráfico.

Directrices para redes StorageGRID

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

Ver "[Configurar conexiones de cliente S3](#)" para aprender cómo conectar clientes S3.

Redes StorageGRID predeterminadas

De forma predeterminada, StorageGRID admite tres interfaces de red por nodo de red, lo que le permite configurar la red para cada nodo de red individual para que coincida con sus requisitos de seguridad y acceso.

Para obtener más información sobre la topología de red, consulte "[Pautas para establecer redes](#)".

Red de cuadrícula

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

Red de administración

Opcional. La red de administración normalmente se utiliza para la administración y el mantenimiento del sistema. También se puede utilizar para acceder al protocolo de cliente. La red de administración normalmente es una red privada y no necesita ser enrutable entre sitios.

Red de clientes

Opcional. La red de cliente es una red abierta que normalmente se utiliza para proporcionar acceso a aplicaciones de cliente S3, de modo que la red de cuadrícula se puede aislar y proteger. La red del cliente puede comunicarse con cualquier subred accesible a través de la puerta de enlace local.

Pautas

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

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

- Si el nodo está conectado a un dispositivo StorageGRID , se utilizan puertos específicos para cada red. Para obtener más detalles, consulte las instrucciones de instalación de su aparato.
- La ruta predeterminada se genera automáticamente, por nodo. Si eth2 está habilitado, entonces 0.0.0.0/0

usa la red del cliente en eth2. Si eth2 no está habilitado, entonces 0.0.0.0/0 usa la red Grid en eth0.

- La red del cliente no estará operativa hasta que el nodo de la red se haya unido 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

Opcionalmente, puede agregar interfaces adicionales a un nodo. Por ejemplo, es posible que desee agregar una interfaz troncal a un nodo de administración o de puerta de enlace, para poder usar ["Interfaces VLAN"](#) para segregar el tráfico perteneciente a diferentes aplicaciones o inquilinos. O bien, es posible que desee agregar una interfaz de acceso para usar en un ["grupo de alta disponibilidad \(HA\)"](#).

Para agregar interfaces troncales o de acceso, consulte lo siguiente:

- **VMware (después de instalar el nodo):** ["VMware: Agregar interfaces troncales o de acceso a un nodo"](#)
 - **Red Hat Enterprise Linux (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Ubuntu o Debian (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **RHEL, Ubuntu o Debian (después de instalar el nodo):** ["Linux: Agregar interfaces troncales o de acceso a un nodo"](#)

Ver direcciones IP

Puede ver la dirección IP de cada nodo de la red en su sistema StorageGRID. Luego puede utilizar esta dirección IP para iniciar sesión en el nodo de la red en la línea de comando y realizar varios procedimientos de mantenimiento.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).

Acerca de esta tarea

Para obtener información sobre cómo cambiar direcciones IP, consulte ["Configurar direcciones IP"](#).

Pasos

1. Seleccione **NODOS > nodo de cuadrícula > Descripción general**.
2. Seleccione **Mostrar más** a la derecha del título Direcciones IP.

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

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  Connected

Storage used:

Object data		7%	?
Object metadata		5%	?

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) ^

Interface ⬆	IP address ⬆
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name ⬆	Severity ? ⬆	Time triggered ⬆	Current values
ILM placement unachievable 🔗	 Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

Configurar interfaces VLAN

Puede crear interfaces de LAN virtual (VLAN) en nodos de administración y nodos de puerta de enlace y usarlas en grupos de alta disponibilidad y puntos finales de equilibrador de carga para aislar y particionar el tráfico para lograr seguridad, flexibilidad y rendimiento. Los nodos seleccionados en el grupo HA pueden usar las interfaces VLAN para compartir hasta 10 direcciones IP virtuales, de modo que si un nodo deja de funcionar, otro nodo se hace cargo del tráfico hacia y desde las direcciones IP virtuales.

Consideraciones para las interfaces VLAN

- Para crear una interfaz VLAN, ingrese una ID de VLAN y elija una interfaz principal en uno o más nodos.
- Se debe configurar una interfaz principal como interfaz troncal en el conmutador.

- Una interfaz principal puede ser la red de cuadrícula (eth0), la red de cliente (eth2) o una interfaz troncal adicional para la máquina virtual o el host físico (por ejemplo, ens256).
- Para cada interfaz VLAN, puede seleccionar solo una interfaz principal para un nodo determinado. Por ejemplo, no puede utilizar la interfaz de red de cuadrícula y la interfaz de red de cliente en el mismo nodo de puerta de enlace que la interfaz principal para la misma VLAN.
- Si la interfaz VLAN es para el tráfico del nodo de administración, que incluye el tráfico relacionado con el administrador de red y el administrador de inquilinos, seleccione interfaces solo en los nodos de administración.
- Si la interfaz VLAN es para el tráfico del cliente S3, seleccione interfaces en los nodos de administración o en los nodos de puerta de enlace.
- Si necesita agregar interfaces troncales, consulte lo siguiente para obtener más detalles:
 - **VMware (después de instalar el nodo):** ["VMware: Agregar interfaces troncales o de acceso a un nodo"](#)
 - **RHEL (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Ubuntu o Debian (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **RHEL, Ubuntu o Debian (después de instalar el nodo):** ["Linux: Agregar interfaces troncales o de acceso a un nodo"](#)

Crear una interfaz VLAN

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).
- Se ha configurado una interfaz troncal en la red y se ha conectado al nodo VM o Linux. Conoces el nombre de la interfaz troncal.
- Conoces el ID de la VLAN que estás configurando.

Acerca de esta tarea

Es posible que su administrador de red haya configurado una o más interfaces troncales y una o más VLAN para segregar el tráfico de cliente o administrador que pertenece a diferentes aplicaciones o inquilinos. Cada VLAN se identifica mediante una etiqueta o ID numérico. Por ejemplo, su red podría usar VLAN 100 para el tráfico de FabricPool y VLAN 200 para una aplicación de archivo.

Puede utilizar Grid Manager para crear interfaces VLAN que permitan a los clientes acceder a StorageGRID en una VLAN específica. Cuando crea interfaces VLAN, especifica el ID de VLAN y selecciona interfaces principales (troncales) en uno o más nodos.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Interfaces VLAN**.
2. Seleccione **Crear**.

Introduzca detalles para las interfaces VLAN

Pasos

1. Especifique el ID de la VLAN en su red. Puede ingresar cualquier valor entre 1 y 4094.

Los ID de VLAN no necesitan ser únicos. Por ejemplo, puede utilizar el ID de VLAN 200 para el tráfico de administrador en un sitio y el mismo ID de VLAN para el tráfico de cliente en otro sitio. Puede crear interfaces VLAN independientes con diferentes conjuntos de interfaces principales en cada sitio. Sin embargo, dos interfaces VLAN con el mismo ID no pueden compartir la misma interfaz en un nodo. Si especifica un ID que ya se ha utilizado, aparecerá un mensaje.

2. Opcionalmente, ingrese una breve descripción para la interfaz VLAN.
3. Seleccione **Continuar**.

Seleccionar interfaces principales

La tabla enumera las interfaces disponibles para todos los nodos de administración y nodos de puerta de enlace en cada sitio de su red. Las interfaces de red de administración (eth1) no se pueden usar como interfaces principales y no se muestran.

Pasos

1. Seleccione una o más interfaces principales para conectar esta VLAN.

Por ejemplo, es posible que desee conectar una VLAN a la interfaz de red de cliente (eth2) para un nodo de puerta de enlace y un nodo de administración.

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.

	Site ?	Node name ?	Interface ?	Description ?	Node type ?	Attached VLANs ?
☐	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
☒	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
☐	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
☒	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
☐	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

[Previous](#)[Continue](#)

2. Seleccione **Continuar**.

Confirmar la configuración

Pasos

1. Revise la configuración y realice los cambios necesarios.
 - Si necesita cambiar la ID o la descripción de la VLAN, seleccione **Ingresar detalles de VLAN** en la parte superior de la página.

- Si necesita cambiar una interfaz principal, seleccione **Elegir interfaces principales** en la parte superior de la página o seleccione **Anterior**.
- Si necesita eliminar una interfaz principal, seleccione la papelera  .

2. Seleccione **Guardar**.

3. Espere hasta 5 minutos para que la nueva interfaz aparezca como una selección en la página Grupos de alta disponibilidad y se incluya en la tabla **Interfaces de red** del nodo (**NODES > parent interface node > Network**).

Editar una interfaz VLAN

Al editar una interfaz VLAN, puede realizar los siguientes tipos de cambios:

- Cambiar la ID o descripción de la VLAN.
- Agregar o eliminar interfaces principales.

Por ejemplo, es posible que desee eliminar una interfaz principal de una interfaz VLAN si planea dismantelar el nodo asociado.

Tenga en cuenta lo siguiente:

- No se puede cambiar una ID de VLAN si la interfaz de VLAN se utiliza en un grupo de alta disponibilidad.
- No se puede eliminar una interfaz principal si dicha interfaz principal se utiliza en un grupo de alta disponibilidad.

Por ejemplo, supongamos que VLAN 200 está conectada a las interfaces principales de 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, puede eliminar la interfaz principal no utilizada para el nodo B, pero no puede eliminar la interfaz principal utilizada para el nodo A.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Interfaces VLAN**.
2. Seleccione la casilla de verificación de la interfaz VLAN que desea editar. Luego, seleccione **Acciones > Editar**.
3. Opcionalmente, actualice el ID de VLAN o la descripción. Luego, seleccione **Continuar**.

No se puede actualizar una ID de VLAN si la VLAN se utiliza en un grupo de alta disponibilidad.

4. Opcionalmente, seleccione o desmarque las casillas de verificación para agregar interfaces principales o eliminar interfaces no utilizadas. Luego, seleccione **Continuar**.
5. Revise la configuración y realice los cambios necesarios.
6. Seleccione **Guardar**.

Eliminar una interfaz VLAN

Puede eliminar una o más interfaces VLAN.

No se puede eliminar una interfaz VLAN si actualmente se utiliza en un grupo HA. Debe eliminar la interfaz VLAN del grupo HA antes de poder eliminarla.

Para evitar interrupciones en el tráfico de clientes, considere realizar una de las siguientes acciones:

- Agregue una nueva interfaz VLAN al grupo HA antes de eliminar esta interfaz VLAN.
- Cree un nuevo grupo HA que no utilice esta interfaz VLAN.
- Si la interfaz VLAN que desea eliminar es actualmente la interfaz activa, edite el grupo HA. Mueva la interfaz VLAN que desea eliminar al final de la lista de prioridades. Espere hasta que se establezca la comunicación en la nueva interfaz principal y luego elimine la interfaz anterior del grupo HA. Por último, elimine la interfaz VLAN en ese nodo.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Interfaces VLAN**.
2. Seleccione la casilla de verificación para cada interfaz VLAN que desee eliminar. Luego, seleccione **Acciones > Eliminar**.
3. Seleccione **Sí** para confirmar su selección.

Se eliminarán todas las interfaces VLAN que seleccionó. Aparece un banner de éxito verde en la página de interfaces VLAN.

Administrar políticas de clasificación de tráfico

¿Qué son las políticas de clasificación de tráfico?

Las políticas de clasificación de tráfico le permiten identificar y monitorear diferentes tipos de tráfico de red. Estas políticas pueden ayudar a limitar y monitorear el tráfico para mejorar sus ofertas de calidad de servicio (QoS).

Las políticas de clasificación de tráfico se aplican a los puntos finales en el servicio StorageGRID Load Balancer para los nodos de puerta de enlace y los nodos de administración. Para crear políticas de clasificación de tráfico, es necesario que ya haya creado puntos finales del balanceador de carga.

Reglas de coincidencia

Cada política de clasificación de tráfico contiene una o más reglas de coincidencia para identificar el tráfico de red relacionado con una o más de las siguientes entidades:

- Cubos
- Subred
- Arrendatario
- Puntos finales del balanceador de carga

StorageGRID monitorea el tráfico que coincide con cualquier regla dentro de la política según los objetivos de la regla. Cualquier tráfico que coincida con alguna regla de una política es manejado por esa política. Por el contrario, puedes establecer reglas para que coincidan con todo el tráfico excepto una entidad específica.

Limitación del tráfico

Opcionalmente, puede agregar los siguientes tipos de límites a una política:

- Ancho de banda agregado
- Ancho de banda por solicitud
- Solicitudes concurrentes

- Tarifa de solicitud

Los valores límite se aplican según cada equilibrador de carga. Si el tráfico se distribuye simultáneamente entre varios balanceadores de carga, las velocidades máximas totales son un múltiplo de los límites de velocidad que especifique.



Puede crear políticas para limitar el ancho de banda agregado o para limitar el ancho de banda por solicitud. Sin embargo, StorageGRID no puede limitar ambos tipos de ancho de banda al mismo tiempo. Los límites de ancho de banda agregados pueden imponer un impacto menor adicional en el rendimiento del tráfico no limitado.

Para límites de ancho de banda agregados o por solicitud, las solicitudes entran o salen a la velocidad que usted establezca. 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 se tiene en cuenta para otras políticas de coincidencia menos específicas que contienen políticas de límite de ancho de banda agregado. Para todos los demás tipos de límites, las solicitudes de los clientes se retrasan 250 milisegundos y reciben una respuesta 503 Slow Down para las solicitudes que exceden cualquier límite de política coincidente.

En el Administrador de cuadrícula, puede ver gráficos de tráfico y verificar que las políticas estén aplicando los límites de tráfico esperados.

Utilice políticas de clasificación de tráfico con SLA

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

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

Nivel de servicio	Capacidad	Protección de datos	Máximo rendimiento permitido	Costo
Oro	Se permite 1 PB de almacenamiento	3 copia la regla ILM	25 K solicitudes/seg Ancho de banda de 5 GB/seg (40 Gbps)	\$\$\$ por mes
Plata	Se permiten 250 TB de almacenamiento	2 copia la regla ILM	10 K solicitudes/seg 1,25 GB/seg (10 Gbps) de ancho de banda	\$\$ por mes
Bronce	Se permiten 100 TB de almacenamiento	2 copia la regla ILM	5 K solicitudes/seg 1 GB/seg (8 Gbps) de ancho de banda	\$ por mes

Crear políticas de clasificación de tráfico

Puede crear políticas de clasificación de tráfico si desea monitorear y, opcionalmente, limitar el tráfico de red por depósito, expresión regular de depósito, CIDR, punto final del balanceador de carga o inquilino. Opcionalmente, puede establecer límites para una política en función del ancho de banda, la cantidad de solicitudes simultáneas o la tasa de solicitudes.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Ha creado todos los puntos finales del balanceador de carga que desea que coincidan.
- Has creado todos los inquilinos que quieres emparejar.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.
2. Seleccione **Crear**.
3. Ingrese un nombre y una descripción (opcional) para la política y seleccione **Continuar**.

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

4. Seleccione **Agregar regla** y especifique los siguientes detalles para crear una o más reglas coincidentes para la política. Cualquier política que cree debe tener al menos una regla coincidente. Seleccione **Continuar**.

Campo	Descripción
Tipo	Seleccione los tipos de tráfico a los que se aplica la regla de coincidencia. Los tipos de tráfico son bucket, regex de bucket, CIDR, punto final del equilibrador de carga e inquilino.

Campo	Descripción
Valor de coincidencia	Introduzca el valor que coincida con el tipo seleccionado. • Cubo: Ingrese uno o más nombres de cubo. • Expresión regular de depósito: ingrese una o más expresiones regulares utilizadas para hacer coincidir un conjunto de nombres de depósito. La expresión regular no está anclada. Utilice el ancla ^ para que coincida al principio del nombre del depósito, y utilice el ancla \$ para que coincida al final del nombre. La coincidencia de expresiones regulares admite un subconjunto de la sintaxis PCRE (expresión regular compatible con Perl). • CIDR: ingrese una o más subredes IPv4, en notación CIDR, que coincidan con la subred deseada. • Punto final del equilibrador de carga: seleccione un nombre de punto final. Estos son los puntos finales del balanceador de carga que definió en el "Configurar los puntos finales del balanceador de carga". • Inquilino: la coincidencia de inquilinos utiliza el ID de la clave de acceso. Si la solicitud no contiene un ID de clave de acceso (por ejemplo, acceso anónimo), se utiliza la propiedad del depósito al que se accede para determinar el inquilino.
Partido inverso	Si desea hacer coincidir todo el tráfico de la red <i>excepto</i> el tráfico consistente con el Tipo y el Valor de coincidencia que acaba de definir, seleccione la casilla de verificación Coincidencia inversa. De lo contrario, deje la casilla de verificación sin marcar. Por ejemplo, si desea que esta política se aplique a todos los puntos finales del balanceador de carga excepto uno, especifique el punto final del balanceador de carga que se excluirá y seleccione Coincidencia inversa. Para una política que contiene varios comparadores donde al menos uno es un comparador inverso, tenga cuidado de no crear una política que coincida con todas las solicitudes.

5. Opcionalmente, seleccione **Agregar un límite** y seleccione los siguientes detalles para agregar uno o más límites para controlar el tráfico de red que coincide con una regla.



StorageGRID recopila métricas incluso si no agrega ningún límite, para que pueda comprender las tendencias de tráfico.

Campo	Descripción
Tipo	El tipo de límite que desea aplicar al tráfico de red que coincide con la regla. Por ejemplo, puede limitar el ancho de banda o la velocidad de solicitud. Nota: Puede crear políticas para limitar el ancho de banda agregado o para limitar el ancho de banda por solicitud. Sin embargo, StorageGRID no puede limitar ambos tipos de ancho de banda al mismo tiempo. Cuando se utiliza el ancho de banda agregado, el ancho de banda por solicitud no está disponible. Por el contrario, cuando se utiliza el ancho de banda por solicitud, el ancho de banda agregado no está disponible. Los límites de ancho de banda agregados pueden imponer un impacto menor adicional en el rendimiento del tráfico no limitado. Para los límites de ancho de banda, StorageGRID aplica la política que mejor coincide con el tipo de límite establecido. Por ejemplo, si tiene una política que limita el tráfico en una sola dirección, entonces el tráfico en la dirección opuesta será ilimitado, incluso si hay tráfico que coincida con políticas adicionales que tienen límites de ancho de banda. StorageGRID implementa 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 cubo • Arrendatario • Punto final • Coincidencias CIDR no exactas (no /32) • Coincidencias inversas
Se aplica a	Si este límite se aplica a solicitudes de lectura del cliente (GET o HEAD) o solicitudes de escritura (PUT, POST o DELETE).
Valor	El valor al que se limitará el tráfico de red, según la unidad que seleccione. Por ejemplo, ingrese 10 y seleccione MiB/s para evitar que el tráfico de red que coincide con esta regla supere los 10 MiB/s. Nota: Dependiendo de la configuración de las unidades, las unidades disponibles serán binarias (por ejemplo, GiB) o decimales (por ejemplo, GB). Para cambiar la configuración de las unidades, seleccione el menú desplegable de usuario en la parte superior derecha del Administrador de cuadrícula, luego seleccione Preferencias de usuario.
Unidad	La unidad que describe el valor ingresado.

Por ejemplo, si desea crear un límite de ancho de banda de 40 GB/s para un nivel de SLA, cree dos límites de ancho de banda agregados: GET/HEAD a 40 GB/s y PUT/POST/DELETE a 40 GB/s.

6. Seleccione **Continuar**.

7. Lea y revise la política de clasificación de tráfico. Utilice el botón **Anterior** para volver atrás y realizar los cambios necesarios. Cuando esté satisfecho con la política, seleccione **Guardar y continuar**.

El tráfico del cliente S3 ahora se maneja de acuerdo con la política de clasificación de tráfico.

Después de terminar

"[Ver métricas de tráfico de red](#)" para verificar que las políticas estén haciendo cumplir los límites de tráfico esperados.

Editar la política de clasificación de tráfico

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tú tienes el "[Permiso de acceso root](#)".

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Clasificación de tráfico**.

Aparece la página de Políticas de clasificación de tráfico y las políticas existentes se enumeran en una tabla.

2. Edite la política utilizando el menú Acciones o la página de detalles. Ver "[crear políticas de clasificación de tráfico](#)" para qué entrar.

Menú de acciones

- a. Seleccione la casilla de verificación de la política.
- b. Seleccione **Acciones > Editar**.

Página de detalles

- a. Seleccione el nombre de la política.
- b. Seleccione el botón **Editar** junto al nombre de la política.

3. Para el paso Ingresar nombre de política, opcionalmente edite el nombre o la descripción de la política y seleccione **Continuar**.
4. Para el paso Agregar reglas coincidentes, opcionalmente agregue una regla o edite el **Tipo** y el **Valor de coincidencia** de la regla existente y seleccione **Continuar**.
5. Para el paso Establecer límites, opcionalmente agregue, edite o elimine un límite y seleccione **Continuar**.
6. Revise la política actualizada y seleccione **Guardar y continuar**.

Los cambios realizados en la política se guardan y el tráfico de red ahora se maneja de acuerdo con las políticas de clasificación de tráfico. Puede ver los gráficos de tráfico y verificar que las políticas estén aplicando los límites de tráfico esperados.

Eliminar una política de clasificación de tráfico

Puede eliminar una política de clasificación de tráfico si ya no la necesita. Asegúrese de eliminar la política correcta porque una política no se puede recuperar una vez eliminada.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Clasificación de tráfico**.

La página de Políticas de clasificación de tráfico aparece con las políticas existentes enumeradas en una tabla.

2. Elimine la política mediante el menú Acciones o la página de detalles.

Menú de acciones

- a. Seleccione la casilla de verificación de la política.
- b. Seleccione **Acciones > Eliminar**.

Página de detalles de la política

- a. Seleccione el nombre de la política.
- b. Seleccione el botón **Eliminar** junto al nombre de la política.

3. Seleccione **Sí** para confirmar que desea eliminar la política.

La política se elimina.

Ver métricas de tráfico de red

Puede supervisar el tráfico de la red viendo los gráficos disponibles en la página Políticas de clasificación de tráfico.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso de root o de cuentas de inquilino"](#) .

Acerca de esta tarea

Para cualquier política de clasificación de tráfico existente, puede ver las métricas del servicio de balanceador de carga para determinar si la política está limitando exitosamente el tráfico en la red. Los datos en los gráficos pueden ayudarle a determinar si necesita ajustar la política.

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

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Clasificación de tráfico**.

Aparece la página de Políticas de clasificación de tráfico y las políticas existentes se enumeran en la tabla.

2. Seleccione el nombre de la política de clasificación de tráfico cuyas métricas desea ver.
3. Seleccione la pestaña **Métricas**.

Aparecen los gráficos de la política de clasificación de tráfico. Los gráficos muestran métricas solo para el tráfico que coincide con la política seleccionada.

Los siguientes gráficos se incluyen en la página.

- Tasa de solicitud: este gráfico proporciona la cantidad de ancho de banda que coincide con esta política manejada por todos los balanceadores de carga. Los datos recibidos incluyen los encabezados de solicitud para todas las solicitudes y el tamaño de los datos del cuerpo para las respuestas que tienen datos del cuerpo. Enviado incluye encabezados de respuesta para todas las solicitudes y el tamaño de los datos del cuerpo de respuesta para las solicitudes que incluyen datos del cuerpo en la respuesta.



Cuando se completan las solicitudes, este gráfico solo muestra el uso del ancho de banda. Para solicitudes de objetos grandes o lentos, el ancho de banda instantáneo real puede diferir de los valores informados en este gráfico.

- Tasa de respuesta de error: este gráfico proporciona una tasa aproximada a la que las solicitudes que coinciden con esta política devuelven errores (código de estado HTTP ≥ 400) a los clientes.
 - Duración promedio de la solicitud (sin errores): este gráfico proporciona una duración promedio de las solicitudes exitosas que coinciden con esta política.
 - Uso del ancho de banda de la política: este gráfico proporciona la cantidad de ancho de banda que coincide con esta política manejada por todos los balanceadores de carga. Los datos recibidos incluyen los encabezados de solicitud para todas las solicitudes y el tamaño de los datos del cuerpo para las respuestas que tienen datos del cuerpo. Enviado incluye encabezados de respuesta para todas las solicitudes y el tamaño de los datos del cuerpo de respuesta para las solicitudes que incluyen datos del cuerpo en la respuesta.
4. Coloque el cursor sobre un gráfico de líneas para ver una ventana emergente de valores en una parte específica del gráfico.
 5. Seleccione **Panel de Grafana** justo debajo del título Métricas para ver todos los gráficos de una política. Además de los cuatro gráficos de la pestaña **Métricas**, puedes ver dos gráficos más:
 - Tasa de solicitud de escritura por tamaño de objeto: la tasa de solicitudes PUT/POST/DELETE que coinciden con esta política. El posicionamiento en una celda individual muestra las velocidades por segundo. Las tarifas que se muestran en la vista flotante se truncan a recuentos de números enteros y pueden informar 0 cuando hay solicitudes distintas de cero en el depósito.
 - Tasa de solicitud de lectura por tamaño de objeto: la tasa de solicitudes GET/HEAD que coinciden con esta política. El posicionamiento en una celda individual muestra las velocidades por segundo. Las tarifas que se muestran en la vista flotante se truncan a recuentos de números enteros y pueden informar 0 cuando hay solicitudes distintas de cero en el depósito.
 6. Alternativamente, acceda a los gráficos desde el menú **SOPORTE**.
 - a. Seleccione **SOPORTE > Herramientas > Métricas**.
 - b. Seleccione **Política de clasificación de tráfico** en la sección **Grafana**.
 - c. Seleccione la política del menú en la parte superior izquierda de la página.
 - d. Coloque el cursor sobre un gráfico para ver una ventana emergente que muestra la fecha y la hora de la muestra, los tamaños de los objetos que se agregan en el recuento y la cantidad de solicitudes por

segundo durante ese período de tiempo.

Las políticas de clasificación de tráfico se identifican por su ID. Los ID de políticas se enumeran en la página de políticas de clasificación de tráfico.

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

Cifrados compatibles para conexiones TLS salientes

El sistema StorageGRID admite un conjunto limitado de conjuntos de cifrados para conexiones de seguridad de la capa de transporte (TLS) a los sistemas externos utilizados para la federación de identidades y los grupos de almacenamiento en la nube.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3 para conexiones a sistemas externos utilizados para la federación de identidades y grupos de almacenamiento en la nube.

Los cifrados TLS compatibles con el uso de sistemas externos se han seleccionado para garantizar la compatibilidad con una variedad de sistemas externos. La lista es más grande que la lista de cifrados compatibles para su uso con aplicaciones cliente S3. Para configurar cifrados, vaya a **CONFIGURACIÓN > Seguridad > Configuración de seguridad** y seleccione **Políticas TLS y SSH**.



Las opciones de configuración de TLS, como versiones de protocolo, cifrados, algoritmos de intercambio de claves y algoritmos MAC, no se pueden configurar en StorageGRID. Comuníquese con su representante de cuenta de NetApp si tiene solicitudes específicas sobre estas configuraciones.

Beneficios de las conexiones HTTP activas, inactivas y simultáneas

La forma en que configura las conexiones HTTP puede afectar el rendimiento del sistema StorageGRID. Las configuraciones difieren dependiendo de si la conexión HTTP está activa o inactiva o si tiene múltiples conexiones simultáneas.

Puede identificar los beneficios de rendimiento para los siguientes tipos de conexiones HTTP:

- Conexiones HTTP inactivas
- Conexiones HTTP activas
- Conexiones HTTP concurrentes

Beneficios de mantener abiertas las conexiones HTTP inactivas

Debe mantener abiertas las conexiones HTTP incluso cuando las aplicaciones cliente estén inactivas para permitir que las aplicaciones cliente realicen transacciones posteriores a través de la conexión abierta. Según las mediciones del sistema y la experiencia de integración, debe mantener una conexión HTTP inactiva abierta durante un máximo de 10 minutos. StorageGRID podría cerrar automáticamente una conexión HTTP que permanezca abierta e inactiva durante más de 10 minutos.

Las conexiones HTTP abiertas e inactivas proporcionan los siguientes beneficios:

- Latencia reducida desde el momento en que el sistema StorageGRID determina que debe realizar una transacción HTTP hasta el momento en que el sistema StorageGRID puede realizar la transacción

La latencia reducida es la principal ventaja, especialmente por el tiempo necesario para establecer conexiones TCP/IP y TLS.

- Aumento de la velocidad de transferencia de datos al activar el algoritmo de inicio lento TCP/IP con transferencias realizadas previamente
- Notificación instantánea de varias clases de condiciones de falla que interrumpen la conectividad entre la aplicación cliente y el sistema StorageGRID

Determinar cuánto tiempo mantener abierta una conexión inactiva es una cuestión de equilibrio entre los beneficios del inicio lento asociado con la conexión existente y la asignación ideal de la conexión a los recursos internos del sistema.

Beneficios de las conexiones HTTP activas

Para las conexiones directas a los nodos de almacenamiento, debe limitar la duración de una conexión HTTP activa a un máximo de 10 minutos, incluso si la conexión HTTP realiza transacciones continuamente.

Determinar la duración máxima que una conexión debe mantenerse abierta es un equilibrio entre los beneficios de la persistencia de la conexión y la asignación ideal de la conexión a los recursos internos del sistema.

Para las conexiones de clientes a nodos de almacenamiento, limitar las conexiones HTTP activas proporciona los siguientes beneficios:

- Permite un equilibrio de carga óptimo en todo el sistema StorageGRID .

Con el tiempo, una conexión HTTP puede dejar de ser óptima a medida que cambian los requisitos de equilibrio de carga. El sistema logra su mejor equilibrio de carga cuando las aplicaciones cliente establecen una conexión HTTP separada para cada transacción, pero esto anula las ganancias mucho más valiosas asociadas con las conexiones persistentes.

- Permite que las aplicaciones cliente dirijan transacciones HTTP a servicios LDR que tengan espacio disponible.
- Permite iniciar procedimientos de mantenimiento.

Algunos procedimientos de mantenimiento comienzan solo después de que se hayan completado todas las conexiones HTTP en curso.

Para las conexiones de clientes al servicio Load Balancer, limitar la duración de las conexiones abiertas puede ser útil para permitir que algunos procedimientos de mantenimiento se inicien rápidamente. Si la duración de las conexiones del cliente no está limitada, es posible que pasen varios minutos hasta que las conexiones activas finalicen automáticamente.

Beneficios de las conexiones HTTP concurrentes

Debe mantener abiertas varias conexiones TCP/IP al sistema StorageGRID para permitir el paralelismo, lo que aumenta el rendimiento. El número óptimo de conexiones paralelas depende de una variedad de factores.

Las conexiones HTTP simultáneas proporcionan los siguientes beneficios:

- Latencia reducida

Las transacciones pueden comenzar inmediatamente en lugar de esperar a que se completen otras transacciones.

- Mayor rendimiento

El sistema StorageGRID puede realizar transacciones paralelas y aumentar el rendimiento de las transacciones agregadas.

Las aplicaciones cliente deben establecer múltiples conexiones HTTP. Cuando una aplicación cliente tiene que realizar una transacción, puede seleccionar y utilizar inmediatamente cualquier conexión establecida que no esté procesando actualmente una transacción.

La topología de cada sistema StorageGRID tiene un rendimiento máximo diferente para transacciones y conexiones simultáneas antes de que el rendimiento comience a degradarse. El rendimiento máximo depende de factores como los recursos informáticos, los recursos de red, los recursos de almacenamiento y los enlaces WAN. La cantidad de servidores y servicios y la cantidad de aplicaciones que admite el sistema StorageGRID también son factores.

Los sistemas StorageGRID suelen admitir múltiples aplicaciones cliente. Debe tener esto en cuenta al determinar la cantidad máxima de conexiones simultáneas utilizadas por una aplicación cliente. Si la aplicación cliente consta de varias entidades de software que establecen conexiones con el sistema StorageGRID, debe sumar todas las conexiones entre las entidades. Es posible que tengas que ajustar el número máximo de conexiones simultáneas en las siguientes situaciones:

- La topología del sistema StorageGRID afecta la cantidad máxima de transacciones y conexiones simultáneas que el sistema puede admitir.
- Las aplicaciones cliente que interactúan con el sistema StorageGRID a través de una red con ancho de banda limitado podrían tener que reducir el grado de simultaneidad para garantizar que las transacciones individuales se completen en un tiempo razonable.
- Cuando muchas aplicaciones cliente comparten el sistema StorageGRID, es posible que deba reducir el grado de simultaneidad para evitar exceder los límites del sistema.

Separación de grupos de conexiones HTTP para operaciones de lectura y escritura

Puede utilizar grupos separados de conexiones HTTP para operaciones de lectura y escritura y controlar qué parte de un grupo utilizar para cada una. Los grupos separados de conexiones HTTP le permiten controlar mejor las transacciones y equilibrar las cargas.

Las aplicaciones cliente pueden crear cargas que sean dominantes en la recuperación (lectura) o dominantes en el almacenamiento (escritura). Con grupos separados de conexiones HTTP para transacciones de lectura y escritura, puede ajustar qué parte de cada grupo dedicar a transacciones de lectura o escritura.

Administrar los costos de los enlaces

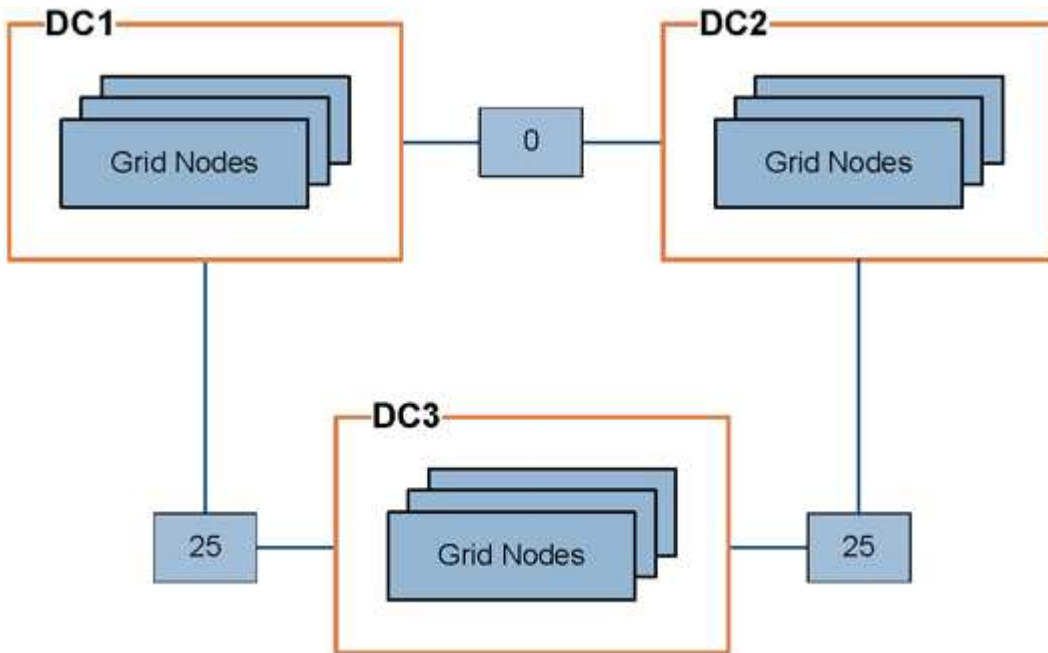
Los costos de enlace le permiten priorizar qué sitio del centro de datos proporciona un servicio solicitado cuando existen dos o más sitios de centros de datos. Puede ajustar los costos de los enlaces para reflejar la latencia entre sitios.

¿Qué son los costos de enlace?

- Los costos de enlace se utilizan para priorizar qué copia de objeto se utiliza para completar las recuperaciones de objetos.
- La API de administración de red y la API de administración de inquilinos utilizan los costos de enlace para determinar qué servicios internos de StorageGRID utilizar.
- El servicio Load Balancer utiliza los costos de enlace en los nodos de administración y los nodos de puerta

de enlace para dirigir las conexiones de los clientes. Ver "[Consideraciones para el equilibrio de carga](#)".

El diagrama muestra una cuadrícula de tres sitios que tiene costos de enlace configurados entre sitios:



- El servicio Load Balancer en los nodos de administración y los nodos de puerta de enlace distribuye equitativamente las conexiones de los clientes a todos los nodos de almacenamiento en el mismo sitio del centro de datos y a cualquier sitio del centro de datos con un costo de enlace de 0.

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

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

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 costo del enlace de DC1 a DC2 es 0, que es menor que el costo del enlace de DC3 a DC2 (25).

Los costos de enlace son números relativos arbitrarios sin una unidad de medida específica. Por ejemplo, un coste de enlace de 50 se utiliza con menos preferencia que un coste de enlace de 25. La tabla muestra los costos de enlaces más utilizados.

Enlace	Costo del enlace	Notas
Entre sitios de centros de datos físicos	25 (predeterminado)	Centros de datos conectados mediante un enlace WAN.
Entre sitios de 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.

Costos de actualización de enlaces

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible" .
- Tú tienes el "Permiso de configuración de la página de topología de cuadrícula" .

Pasos

1. Seleccione **SOPORTE > Otro > Costo del enlace**.

The screenshot shows the 'Link Cost' configuration page. At the top, there's a header with a 'Link Cost' title and a timestamp 'Updated: 2023-02-15 18:09:28 MST'. Below the header, there's a section for 'Site Names' showing a list of three sites: Site ID 10 (Data Center 1), Site ID 20 (Data Center 2), and Site ID 30 (Data Center 3). Each site has an edit icon. Below the list, there's a 'Show 50 Records Per Page' dropdown and a 'Refresh' button. To the right, there are 'Previous', '1', and 'Next' navigation links. Below the 'Site Names' section, there's a 'Link Costs' section. It features a table with columns for 'Link Source', 'Link Destination', and 'Actions'. The 'Link Source' column has a dropdown menu currently set to 'Data Center 1'. The 'Link Destination' column has three sub-columns for destinations 10, 20, and 30. The values in these cells are 0, 25, and 25 respectively. There is an 'Apply Changes' button with a right arrow icon at the bottom right of the table.

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	
30	Data Center 3	

Show 50 Records Per Page Refresh Previous 1 Next

Link Source	Link Destination	Actions
Data Center 1	10: 0, 20: 25, 30: 25	

Apply Changes

2. Seleccione un sitio en **Fuente del enlace** e ingrese un valor de costo entre 0 y 100 en **Destino del enlace**.

No puedes cambiar el costo del enlace si el origen es el mismo que el destino.

Para cancelar los cambios, seleccione **Revertir**.

3. Seleccione **Aplicar cambios**.

Utilice AutoSupport

¿Qué es AutoSupport?

La función AutoSupport permite que StorageGRID envíe paquetes de estado y salud al soporte técnico de NetApp .

El uso de AutoSupport puede acelerar significativamente la determinación y resolución de problemas. El soporte técnico también puede monitorear las necesidades de almacenamiento de su sistema y ayudarlo a determinar si necesita agregar nuevos nodos o sitios. Opcionalmente, puede configurar los paquetes de

AutoSupport para que se envíen a un destino adicional.

StorageGRID tiene dos tipos de AutoSupport:

- * StorageGRID AutoSupport* informa problemas de software de StorageGRID . Habilitado de forma predeterminada cuando instala StorageGRID por primera vez. Puede ["cambiar la configuración predeterminada de AutoSupport"](#) Si es necesario.



Si StorageGRID AutoSupport no está habilitado, aparecerá un mensaje en el panel de Grid Manager. El mensaje incluye un enlace a la página de configuración de AutoSupport . Si cierra el mensaje, no volverá a aparecer hasta que se borre la memoria caché de su navegador, incluso si AutoSupport permanece deshabilitado.

- * AutoSupport de hardware del dispositivo* informa problemas con el dispositivo StorageGRID . Usted debe ["Configurar AutoSupport de hardware en cada dispositivo"](#) .

¿Qué es Active IQ?

Active IQ es un asesor digital basado en la nube que aprovecha el análisis predictivo y la sabiduría de la comunidad de la base instalada de NetApp. Sus evaluaciones de riesgos continuas, alertas predictivas, orientación prescriptiva y acciones automatizadas lo ayudan a prevenir problemas antes de que ocurran, lo que genera una mejor salud del sistema y una mayor disponibilidad del sistema.

Si desea utilizar los paneles y la funcionalidad de Active IQ en el sitio de soporte de NetApp , debe habilitar AutoSupport.

["Documentación del Digital Advisor Active IQ"](#)

Información incluida en el paquete AutoSupport

Un paquete de AutoSupport contiene los siguientes archivos y detalles.

Nombre del archivo	Campos	Descripción
HISTORIAL DE AUTOSOPORTE.XML	Número de secuencia de AutoSupport + Destino para este AutoSupport + Estado de 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
AUTOSOPORTE.XML	Nodo + Protocolo para contactar con soporte + URL de soporte para HTTP/HTTPS + Dirección de soporte + Estado de AutoSupport OnDemand + URL del servidor de AutoSupport OnDemand + Intervalo de sondeo de AutoSupport OnDemand	Archivo de estado de AutoSupport . Proporciona detalles del protocolo utilizado, la URL y la dirección de soporte técnico, el intervalo de sondeo y el AutoSupport a pedido si está habilitado o deshabilitado.
CUBOS.XML	ID de bucket + ID de cuenta + Versión de compilación + Configuración de restricción de ubicación + Cumplimiento habilitado + Configuración de cumplimiento + Bloqueo de objetos S3 habilitado + Configuración de bloqueo de objetos S3 + Configuración de consistencia + CORS habilitado + Configuración de CORS + Hora del último acceso habilitada + Política habilitada + Configuración de política + Notificaciones habilitadas + Configuración de notificaciones + Espejo en la nube habilitado + Configuración de espejo en la nube + Búsqueda habilitada + Configuración de búsqueda + Etiquetado de bucket habilitado + Configuración de etiquetado de bucket + Configuración de control de versiones	Proporciona detalles de configuración y estadísticas a nivel de depósito. Algunos ejemplos de configuraciones de bucket incluyen servicios de plataforma, cumplimiento y consistencia de bucket.
CONFIGURACIONES DE RED.XML	ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Archivo de información de configuración de toda la red. Contiene información sobre certificados de red, espacio reservado de metadatos, configuraciones de toda la red (cumplimiento, bloqueo de objetos S3, compresión de objetos, alertas, syslog y configuración de ILM), detalles del perfil de codificación de borrado, nombre DNS y "Nombre NMS" .

Nombre del archivo	Campos	Descripción
GRID-SPEC.XML	Especificaciones de la cuadrícula, XML sin procesar	Se utiliza para configurar e implementar StorageGRID. Contiene especificaciones de la red, IP del servidor NTP, IP del servidor DNS, topología de red y perfiles de hardware de los nodos.
GRID-TAREAS.XML	Nodo + Ruta de servicio + ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Archivo de estado de tareas de red (procedimientos de mantenimiento). Proporciona detalles de las tareas activas, finalizadas, completadas, fallidas y pendientes de la red.
CUADRÍCULA.JSON	Grid + Revisión + Versión de software + Descripción + Licencia + Contraseñas + DNS + NTP + Sitios + Nodos	Información de la cuadrícula.
ILM-CONFIGURACIÓN.XML	ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Lista de atributos para configuraciones de ILM.
ILM-STATUS.XML	Nodo + Ruta de servicio + ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Archivo de información de métricas ILM. Contiene tasas de evaluación de ILM para cada nodo y métricas de toda la red.
ILM.XML	XML sin procesar de ILM	Archivo de política activa de ILM. Contiene detalles sobre las políticas ILM activas, como ID de grupo de almacenamiento, comportamiento de ingesta, filtros, reglas y descripción.
REGISTRO.TGZ	<i>n / A</i>	Archivo de registro descargable. Contiene <code>broadcast-err.log</code> y <code>servermanager.log</code> desde cada nodo.
MANIFIESTO.XML	Orden de recopilación + Nombre del archivo de contenido de AutoSupport para estos datos + Descripción de este elemento de datos + Número de bytes recopilados + Tiempo dedicado a la recopilación + Estado de este elemento de datos + Descripción del error + Tipo de contenido de AutoSupport para estos datos +	Contiene metadatos de AutoSupport y breves descripciones de todos los archivos de AutoSupport .

Nombre del archivo	Campos	Descripción
ENTIDADES NMS.XML	Índice de atributo + OID de entidad + ID de nodo + ID de modelo de dispositivo + Versión de modelo de dispositivo + Nombre de entidad	Entidades de grupo y de servicios en el " Árbol NMS ". Proporciona detalles de la topología de la red. El nodo se puede determinar en función de los servicios que se ejecutan en el nodo.
OBJETOS-ESTADO.XML	Nodo + Ruta de servicio + ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Estado del objeto, incluido el estado de escaneo en segundo plano, transferencia activa, velocidad de transferencia, transferencias totales, velocidad de eliminación, fragmentos dañados, objetos perdidos, objetos faltantes, reparación intentada, velocidad de escaneo, período de escaneo estimado y estado de finalización de la reparación.
ESTADO DEL SERVIDOR.XML	Nodo + Ruta de servicio + ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Configuraciones del servidor. Contiene estos detalles para cada nodo: tipo de plataforma, sistema operativo, memoria instalada, memoria disponible, conectividad de almacenamiento, número de serie del chasis del dispositivo de almacenamiento, recuento de unidades fallidas 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.
ESTADO DEL SERVICIO.XML	Nodo + Ruta de servicio + ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Archivo de información del nodo de servicio. Contiene detalles como espacio de tabla asignado, espacio de tabla libre, métricas de Reaper de la base de datos, duración de reparación de segmento, duración del trabajo de reparación, reinicios automáticos de trabajos y finalización automática de trabajos.
GRADOS DE ALMACENAMIENTO.XML	ID de grado de almacenamiento + Nombre de grado de almacenamiento + ID de nodo de almacenamiento + Ruta del nodo de almacenamiento	Archivo de definiciones de grado de almacenamiento para cada nodo de almacenamiento.

Nombre del archivo	Campos	Descripción
RESUMEN-ATRIBUTOS.XML	OID de grupo + Ruta de grupo + ID de atributo de resumen + Nombre de atributo de resumen + Valor + Índice + ID de tabla + Nombre de tabla	Datos de estado del sistema de alto nivel que resumen la información de uso de StorageGRID . Proporciona detalles como el nombre de la red, los nombres de los sitios, la cantidad de nodos de almacenamiento por red y por sitio, el tipo de licencia, la capacidad y el uso de la licencia, los términos de soporte del software y los detalles de las operaciones de S3.
ALERTAS DEL SISTEMA.XML	Nombre + Gravedad + Nombre del nodo + Estado de la alerta + Nombre del sitio + Hora de activación de la alerta + Hora de resolución de la alerta + ID de regla + ID del nodo + ID del sitio + Silenciado + Otras anotaciones + Otras etiquetas	Alertas actuales del sistema que indican problemas potenciales en el sistema StorageGRID .
USERAGENTS.XML	Agente de usuario + Número de días + Total de solicitudes HTTP + Total de bytes ingeridos + Total de bytes recuperados + Solicitudes PUT + Solicitudes GET + Solicitudes DELETE + Solicitudes HEAD + Solicitudes POST + Solicitudes OPTIONS + Tiempo promedio de solicitud (ms) + Tiempo promedio de solicitud PUT (ms) + Tiempo promedio de solicitud GET (ms) + Tiempo promedio de solicitud DELETE (ms) + Tiempo promedio de solicitud HEAD (ms) + Tiempo promedio de solicitud POST (ms) + Tiempo promedio de solicitud OPTIONS (ms)	Estadísticas basadas en los agentes de usuario de la aplicación. Por ejemplo, la cantidad de operaciones PUT/GET/DELETE/HEAD por agente de usuario y el tamaño total de bytes de cada operación.
DATOS DEL ENCABEZADO X	X-Netapp-asup-generado-en + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name +	Datos de encabezado de AutoSupport .

Configurar AutoSupport

De forma predeterminada, la función StorageGRID AutoSupport está habilitada cuando instala StorageGRID por primera vez. Sin embargo, debe configurar AutoSupport de hardware en cada dispositivo. Según sea necesario, puede cambiar la configuración de AutoSupport .

Si desea cambiar la configuración de StorageGRID AutoSupport, realice los cambios solo en el nodo de administración principal. Usted debe [configurar hardware AutoSupport](#) en cada aparato.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Si va a utilizar HTTPS para enviar paquetes de AutoSupport , ha proporcionado acceso a Internet saliente al nodo de administración principal, ya sea de manera directa o ["utilizando un servidor proxy"](#) (no se requieren conexiones entrantes).
- Si se selecciona HTTP en la página StorageGRID AutoSupport , tiene ["configuró un servidor proxy"](#) para reenviar paquetes de AutoSupport como HTTPS. Los servidores AutoSupport de NetApp rechazarán los paquetes enviados mediante HTTP.
- Si va a utilizar SMTP como protocolo para los paquetes de AutoSupport , habrá configurado un servidor de correo SMTP.

Acerca de esta tarea

Puede utilizar cualquier combinación de las siguientes opciones para enviar paquetes de AutoSupport al soporte técnico:

- **Semanal:** envía automáticamente paquetes de AutoSupport una vez por semana. Configuración predeterminada: habilitado.
- **Activado por eventos:** envía automáticamente paquetes de AutoSupport cada hora o cuando ocurren eventos importantes del sistema. Configuración predeterminada: habilitado.
- **A pedido:** permite que el soporte técnico solicite que su sistema StorageGRID envíe paquetes de AutoSupport automáticamente, lo que resulta útil cuando están trabajando activamente en un problema (requiere el protocolo de transmisión AutoSupport HTTPS). Configuración predeterminada: deshabilitado.
- **Activado por el usuario:** envía manualmente paquetes de AutoSupport en cualquier momento.

Especifique el protocolo para los paquetes de AutoSupport

Puede utilizar cualquiera de los siguientes protocolos para enviar paquetes de AutoSupport :

- **HTTPS:** Esta es la configuración predeterminada y recomendada para nuevas instalaciones. Este protocolo utiliza el puerto 443. Si quieres [Habilitar la función AutoSupport on Demand](#) , debes utilizar HTTPS.
- **HTTP:** Si selecciona HTTP, debe configurar un servidor proxy para reenviar los paquetes de AutoSupport como HTTPS. Los servidores AutoSupport de NetApp rechazan los paquetes enviados mediante HTTP. Este protocolo utiliza el puerto 80.
- **SMTP:** utilice esta opción si desea que los paquetes de AutoSupport se envíen por correo electrónico.

El protocolo que configure se utiliza para enviar todo tipo de paquetes de AutoSupport .

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Seleccione el protocolo que desea utilizar para enviar paquetes de AutoSupport .
3. Si seleccionó **HTTPS**, seleccione si desea utilizar un certificado de soporte de NetApp (certificado TLS) para proteger la conexión al servidor de soporte técnico.
 - **Verificar certificado** (predeterminado): garantiza que la transmisión de paquetes de AutoSupport sea segura. El certificado de soporte de NetApp ya está instalado con el software StorageGRID .
 - **No verificar el certificado**: seleccione esta opción solo cuando tenga una buena razón para no utilizar la validación del certificado, como cuando hay un problema temporal con un certificado.
4. Seleccione **Guardar**. Todos los paquetes semanales, activados por el usuario y activados por eventos se envían mediante el protocolo seleccionado.

Desactivar el AutoSupport semanal

De forma predeterminada, el sistema StorageGRID está configurado para enviar un paquete de AutoSupport al soporte técnico una vez por semana.

Para determinar cuándo se enviará el paquete de AutoSupport semanal, vaya a la pestaña *** AutoSupport* > Resultados**. En la sección *** AutoSupport semanal***, observe el valor de **Próxima hora programada**.

Puede desactivar el envío automático de paquetes semanales de AutoSupport en cualquier momento.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Desmarque la casilla de verificación **Habilitar AutoSupport semanal**.
3. Seleccione **Guardar**.

Deshabilitar el AutoSupport activado por eventos

De forma predeterminada, el sistema StorageGRID está configurado para enviar un paquete de AutoSupport al soporte técnico cada hora.

Puede desactivar el AutoSupport activado por eventos en cualquier momento.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Desmarque la casilla de verificación **Habilitar AutoSupport activado por eventos**.
3. Seleccione **Guardar**.

Habilitar AutoSupport a pedido

AutoSupport on Demand puede ayudar a resolver problemas en los que el soporte técnico está trabajando activamente.

De forma predeterminada, AutoSupport on Demand está deshabilitado. Al habilitar esta función, el soporte técnico puede solicitar que su sistema StorageGRID envíe paquetes de AutoSupport automáticamente. El soporte técnico también puede establecer el intervalo de tiempo de sondeo para las consultas de AutoSupport on Demand.

El soporte técnico no puede habilitar ni deshabilitar AutoSupport on Demand.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Seleccione **HTTPS** para el protocolo.
3. Seleccione la casilla de verificación **Habilitar AutoSupport semanal**.
4. Seleccione la casilla de verificación **Habilitar AutoSupport a pedido**.
5. Seleccione **Guardar**.

AutoSupport on Demand está habilitado y el soporte técnico puede enviar solicitudes de AutoSupport on Demand a StorageGRID.

Deshabilitar las comprobaciones de actualizaciones de software

De forma predeterminada, StorageGRID se comunica con NetApp para determinar si hay actualizaciones de software disponibles para su sistema. Si hay una revisión o una nueva versión de StorageGRID disponible, la nueva versión se muestra en la página Actualización de StorageGRID .

Según sea necesario, puede desactivar opcionalmente la búsqueda de actualizaciones de software. Por ejemplo, si su sistema no tiene acceso WAN, debe deshabilitar la verificación para evitar errores de descarga.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Desmarque la casilla **Buscar actualizaciones de software**.
3. Seleccione **Guardar**.

Agregar un destino de AutoSupport adicional

Cuando habilita AutoSupport, los paquetes de estado y salud se envían al soporte técnico. Puede especificar un destino adicional para todos los paquetes de AutoSupport .

Para verificar o cambiar el protocolo utilizado para enviar paquetes de AutoSupport , consulte las instrucciones para [especificar el protocolo para los paquetes de AutoSupport](#) .



No puede utilizar el protocolo SMTP para enviar paquetes de AutoSupport a un destino adicional.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Seleccione **Habilitar destino de AutoSupport adicional**.
3. Especifique lo siguiente:

Nombre de host

El nombre de host del servidor o la dirección IP de un servidor de destino de AutoSupport adicional.



Sólo puedes introducir un destino adicional.

Puerto

El puerto utilizado para conectarse a un servidor de destino de AutoSupport adicional. El puerto predeterminado es el puerto 80 para HTTP o el puerto 443 para HTTPS.

Validación de certificados

Si se utiliza un certificado TLS para proteger la conexión al destino adicional.

- Seleccione **Verificar certificado** para utilizar la validación del certificado.
- Seleccione **No verificar certificado** para enviar sus paquetes de AutoSupport sin validación del certificado.

Seleccione esta opción solo cuando tenga un buen motivo para no utilizar la validación de certificados, como cuando hay un problema temporal con un certificado.

4. Si seleccionó **Verificar certificado**, haga lo siguiente:

- a. Busque la ubicación del certificado CA.
- b. Subir el archivo del certificado CA.

Aparecen los metadatos del certificado CA.

5. Seleccione **Guardar**.

Todos los paquetes futuros de AutoSupport activados por eventos, semanales o por el usuario se enviarán al destino adicional.

Configurar AutoSupport para dispositivos

AutoSupport para 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 sobre problemas de hardware y software. Debe configurar AutoSupport en cada dispositivo excepto el SGF6112, que no requiere configuración adicional. AutoSupport se implementa de manera diferente para los dispositivos de servicios y los dispositivos de almacenamiento.

Utilice SANtricity para habilitar AutoSupport para cada dispositivo de almacenamiento. Puede configurar SANtricity AutoSupport durante la configuración inicial del dispositivo o después de haberlo instalado:

- Para los dispositivos SG6000 y SG5700, "[Configurar AutoSupport en SANtricity System Manager](#)"

Los paquetes de AutoSupport de los dispositivos E-Series se pueden incluir en StorageGRID AutoSupport si configura la entrega de AutoSupport por proxy en "[SANtricity System Manager](#)".

StorageGRID AutoSupport no informa problemas de hardware, como fallas de DIMM o de tarjeta de interfaz de host (HIC). Sin embargo, algunas fallas de componentes podrían provocar "[alertas de hardware](#)". Para los dispositivos StorageGRID con un controlador de administración de placa base (BMC), puede configurar trampas de correo electrónico y SNMP para informar fallas de hardware:

- "[Configurar notificaciones por correo electrónico para alertas de BMC](#)"
- "[Configurar los ajustes de SNMP para BMC](#)"

Información relacionada

["Soporte de NetApp"](#)

Activar manualmente un paquete de AutoSupport

Para ayudar al soporte técnico a solucionar problemas con su sistema StorageGRID , puede activar manualmente el envío de un paquete de AutoSupport .

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Debe tener acceso de root u otro permiso de configuración de red.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport***.
2. En la pestaña **Acciones**, seleccione **Enviar AutoSupport activado por el usuario**.

StorageGRID intenta enviar un paquete de AutoSupport al sitio de soporte de NetApp . Si el intento es exitoso, se actualizan los valores **Resultado más reciente** y **Última vez exitoso** en la pestaña **Resultados**. Si hay un problema, el valor **Resultado más reciente** se actualiza a "Error" y StorageGRID no intenta enviar el paquete AutoSupport nuevamente.



Después de enviar un paquete de AutoSupport activado por el usuario, actualice la página de AutoSupport en su navegador después de 1 minuto para acceder a los resultados más recientes.

Solucionar problemas de paquetes de AutoSupport

Si falla un intento de enviar un paquete de AutoSupport , el sistema StorageGRID toma diferentes acciones según el tipo de paquete de AutoSupport . Puede comprobar el estado de los paquetes de AutoSupport seleccionando **SOPORTE > Herramientas > * AutoSupport* > Resultados**.

Cuando el paquete de AutoSupport no se puede enviar, aparece "Error" en la pestaña **Resultados** de la página *** AutoSupport***.



Si configuró un servidor proxy para reenviar paquetes de AutoSupport a NetApp, debe ["verificar que la configuración del servidor proxy sea correcta"](#) .

Falla del paquete de AutoSupport semanal

Si no se puede enviar un paquete de AutoSupport semanal, el sistema StorageGRID toma las siguientes acciones:

1. Actualiza el atributo Resultado más reciente a Reintentar.
2. Intenta reenviar el paquete de AutoSupport 15 veces cada cuatro minutos durante una hora.
3. Después de una hora de fallas de envío, actualiza el atributo Resultado más reciente a Fallido.
4. Intenta enviar un paquete de AutoSupport nuevamente en el próximo horario programado.
5. Mantiene la programación regular 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 vuelve a estar disponible, envía un paquete de AutoSupport inmediatamente si no se ha enviado un paquete durante siete días o más.

Error del paquete de AutoSupport activado por el usuario o por evento

Si un paquete de AutoSupport activado por el usuario o por evento no se puede enviar, el sistema StorageGRID toma las siguientes acciones:

1. Muestra un mensaje de error si se conoce el error. Por ejemplo, si un usuario selecciona el protocolo SMTP sin proporcionar la configuración de correo electrónico correcta, se muestra el siguiente error:
AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.
2. No intenta enviar el paquete nuevamente.
3. Registra el error en `nms.log`.

Si ocurre una falla y SMTP es el protocolo seleccionado, verifique que el servidor de correo electrónico del sistema StorageGRID esté configurado correctamente y que su servidor de correo electrónico esté ejecutándose (**SOPORTE > Alarmas (heredado) > Configuración de correo electrónico heredado**). El siguiente mensaje de error podría aparecer en la página de AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page`.

Aprenda a... ["configurar los ajustes del servidor de correo electrónico"](#).

Corregir una falla del paquete AutoSupport

Si ocurre una falla y SMTP es el protocolo seleccionado, verifique que el servidor de correo electrónico del sistema StorageGRID esté configurado correctamente y que su servidor de correo electrónico esté ejecutándose. El siguiente mensaje de error podría aparecer en la página de AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page`.

Envíe paquetes de AutoSupport de la serie E a través de StorageGRID

Puede enviar paquetes de AutoSupport de E-Series SANtricity System Manager al soporte técnico a través de un nodo de administración de StorageGRID en lugar de a través del puerto de administración del dispositivo de almacenamiento.

Ver ["AutoSupport de hardware de la serie E"](#) para obtener más información sobre el uso de AutoSupport con dispositivos de la serie E.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Administrador del dispositivo de almacenamiento o permiso de acceso raíz"](#).
- Ha configurado SANtricity AutoSupport:
 - Para los dispositivos SG6000 y SG5700, ["Configurar AutoSupport en SANtricity System Manager"](#)



Debe tener el firmware SANtricity 8.70 o superior para acceder a SANtricity System Manager mediante Grid Manager.

Acerca de esta tarea

Los paquetes AutoSupport de la serie E contienen detalles del hardware de almacenamiento y son más específicos que otros paquetes AutoSupport enviados por el sistema StorageGRID.

Puede 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 utilizar el puerto de administración del dispositivo. Los paquetes de AutoSupport transmitidos de esta manera son enviados por el ["Nodo de administración del remitente preferido"](#), y utilizan cualquier ["configuración del proxy de](#)

administración" que se han configurado en el Administrador de cuadrícula.

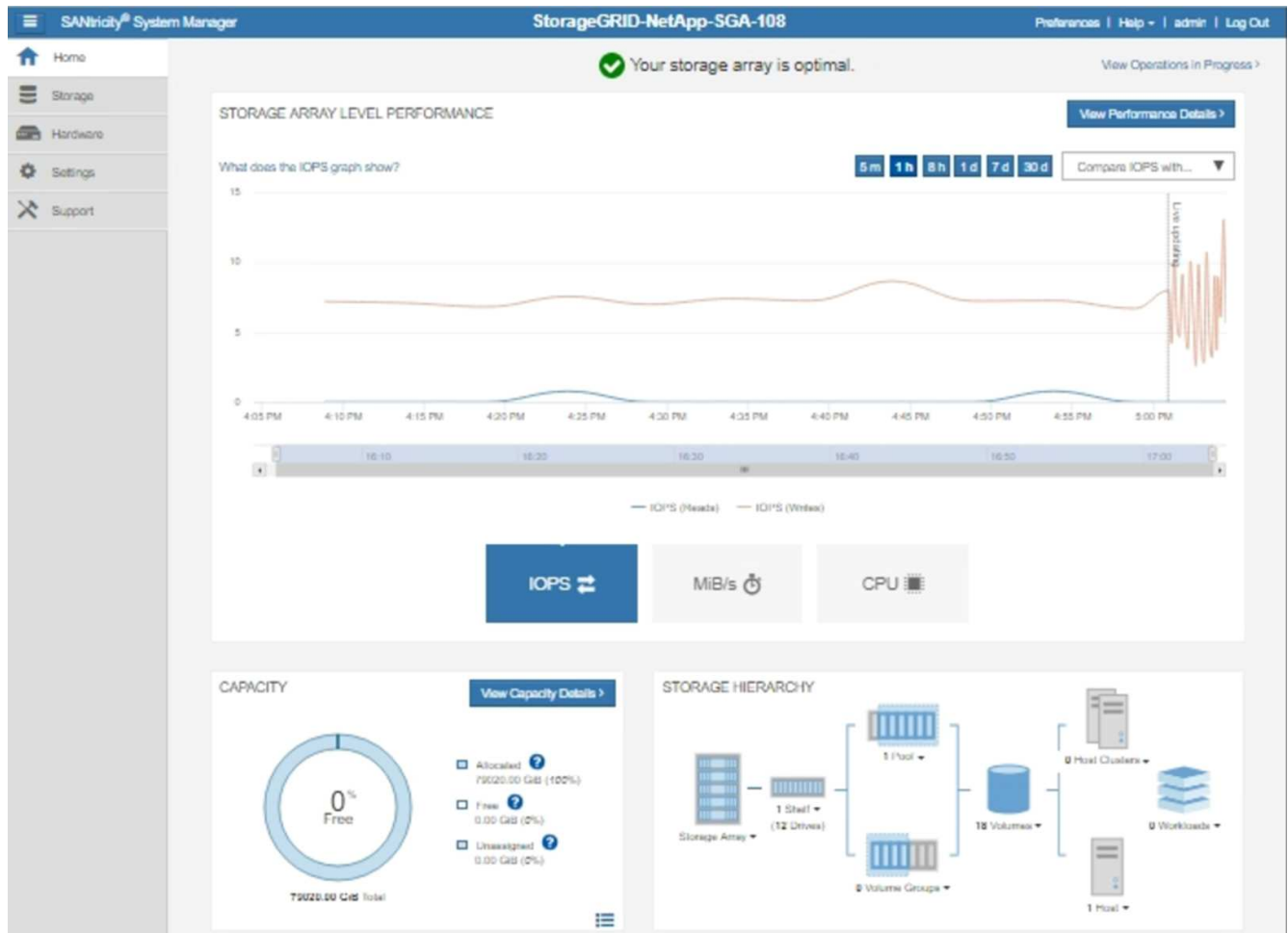


Este procedimiento es solo para configurar un servidor proxy StorageGRID para paquetes E-Series AutoSupport . Para obtener detalles adicionales sobre la configuración de AutoSupport de la serie E, consulte la "[Documentación de NetApp E-Series y SANtricity](#)".

Pasos

1. En el Administrador de cuadrícula, seleccione **NODOS**.
2. De la lista de nodos de la izquierda, seleccione el nodo del dispositivo de almacenamiento que desea configurar.
3. Seleccione * SANtricity System Manager*.

Aparece la página de inicio de SANtricity System Manager.



4. Seleccione **SOPORTE > Centro de soporte > * AutoSupport***.

Aparece la página de operaciones de AutoSupport .

Technical Support

Chassis serial number: 031517000693

 [NetApp My Support](#)

US/Canada 888.463.8277

[Other Contacts](#)

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled 

[Enable/Disable AutoSupport Features](#)
AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

[Configure AutoSupport Delivery Method](#)
Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

[Schedule AutoSupport Dispatches](#)
AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

[Send AutoSupport Dispatch](#)
Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

[View AutoSupport Log](#)
The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

[Enable AutoSupport Maintenance Window](#)
Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

[Disable AutoSupport Maintenance Window](#)
Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. Seleccione *Configurar método de entrega de AutoSupport*.

Aparece la página Configurar método de entrega de AutoSupport .

Configure AutoSupport Delivery Method [X]

Select AutoSupport dispatch delivery method...

☒ HTTPS

☐ HTTP

☐ Email

HTTPS delivery settings [Show destination address](#)

Connect to support team...

☐ Directly ?

☒ via Proxy server ?

Host address ?

tunnel-host

Port number ?

10225

☐ My proxy server requires authentication

☐ via Proxy auto-configuration script (PAC) ?

Save **Test Configuration** **Cancel**

6. Seleccione **HTTPS** como método de entrega.



El certificado que habilita HTTPS está preinstalado.

7. Seleccionar **a través del servidor proxy**.

8. Ingresar `tunnel-host` para la **Dirección del host**.

`tunnel-host` es la dirección especial para utilizar un nodo de administración para enviar paquetes de AutoSupport de la serie E.

9. Ingresar 10225 para el **Número de puerto**.

`10225` es el número de puerto en el servidor proxy StorageGRID que recibe paquetes de AutoSupport del controlador E-Series en el dispositivo.

10. Seleccione **Probar configuración** para probar el enrutamiento y la configuración de su servidor proxy de AutoSupport .

Si es correcto, aparecerá un mensaje en un banner verde: "Su configuración de AutoSupport ha sido

verificada".

Si la prueba falla, aparece un mensaje de error en un banner rojo. Verifique la configuración de DNS y la red de StorageGRID y asegúrese de que "[Nodo de administración del remitente preferido](#)" puede conectarse al sitio de soporte de NetApp e intentar la prueba nuevamente.

11. Seleccione **Guardar**.

La configuración se guarda y aparece un mensaje de confirmación: "Se ha configurado el método de entrega de AutoSupport".

Administrar nodos de almacenamiento

Administrar nodos de almacenamiento

Los nodos de almacenamiento proporcionan capacidad y servicios de almacenamiento en disco. La gestión de nodos de almacenamiento implica lo siguiente:

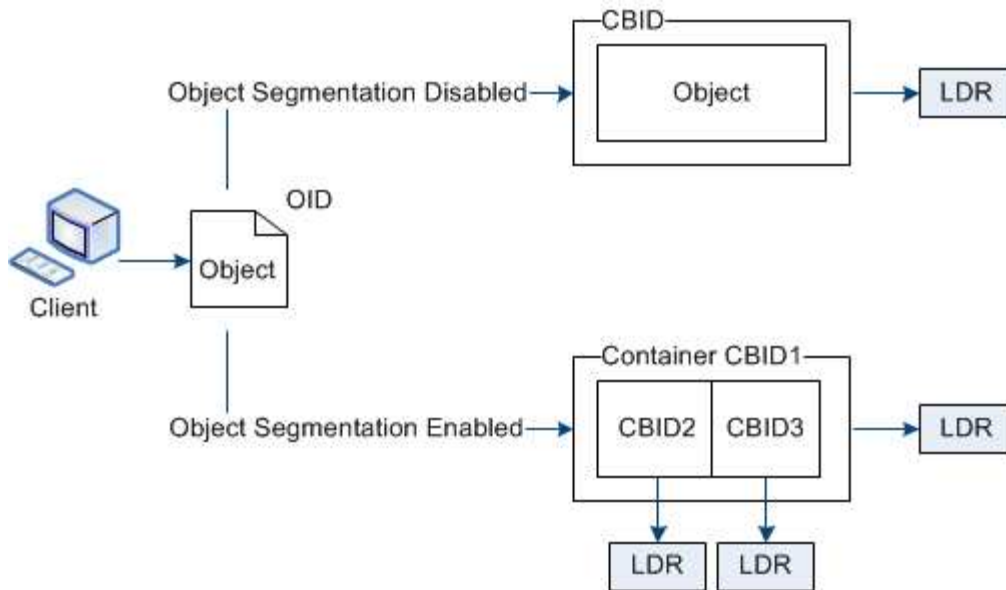
- Administrar las opciones de almacenamiento
- Comprender qué son las marcas de agua del volumen de almacenamiento y cómo puede usar las anulaciones de marcas de agua para controlar cuándo los nodos de almacenamiento se vuelven de solo lectura
- Monitoreo y gestión del espacio utilizado para los metadatos de los objetos
- Configuración de ajustes globales para objetos almacenados
- Aplicación de la configuración del nodo de almacenamiento
- Administración de nodos de almacenamiento completos

Utilice las opciones de almacenamiento

¿Qué es la segmentación de objetos?

La segmentación de objetos es el proceso de dividir un objeto en una colección de objetos más pequeños de tamaño fijo para optimizar el uso de almacenamiento y recursos para objetos grandes. La carga multiparte de S3 también crea objetos segmentados, con un objeto que representa cada parte.

Cuando se ingiere un objeto en el sistema StorageGRID, el servicio LDR divide el objeto en segmentos y crea un contenedor de segmentos que enumera la información del encabezado de todos los segmentos como contenido.



Al recuperar un contenedor de segmentos, el servicio LDR ensambla el objeto original a partir de sus segmentos y devuelve el objeto al cliente.

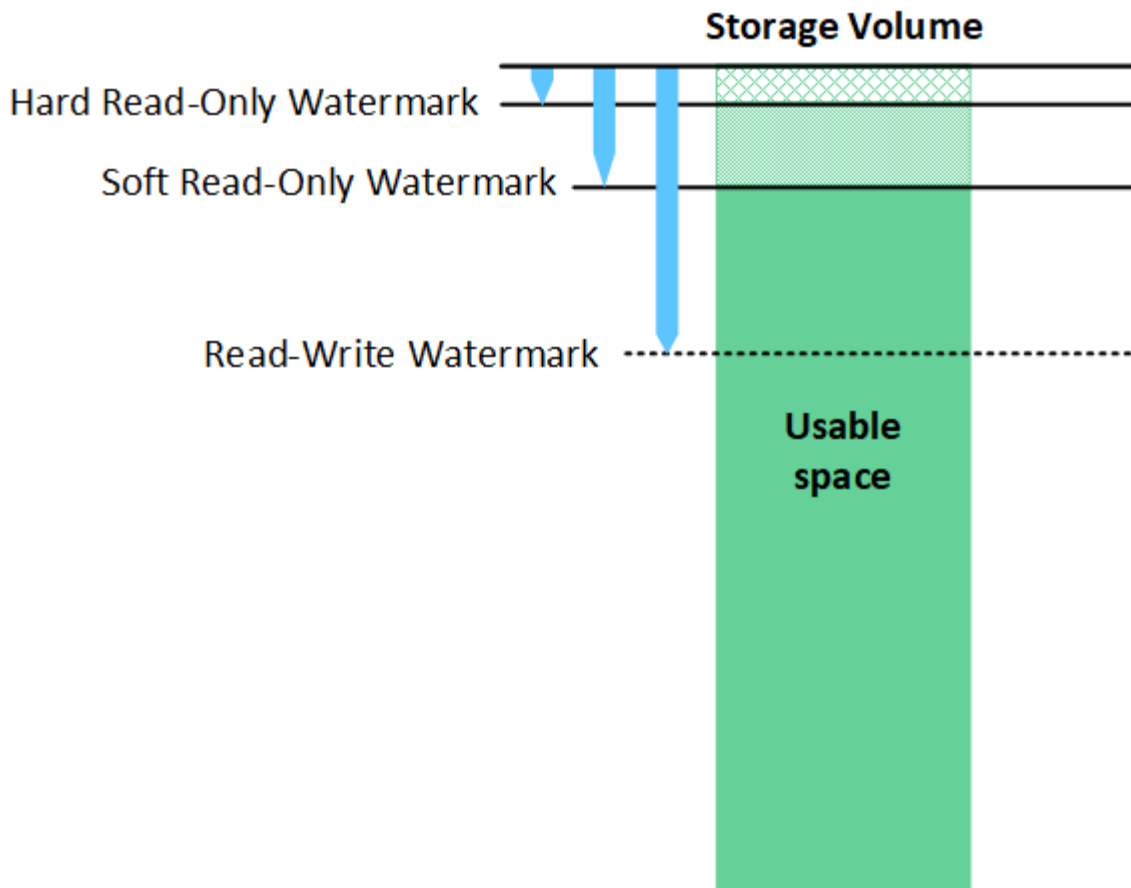
El contenedor y los segmentos no necesariamente se almacenan en el mismo nodo de almacenamiento. Los contenedores y segmentos se pueden almacenar en cualquier nodo de almacenamiento dentro del grupo de almacenamiento especificado en la regla ILM.

El sistema StorageGRID trata cada segmento de forma independiente y contribuye al recuento de atributos como objetos administrados y objetos almacenados. Por ejemplo, si un objeto almacenado en el sistema StorageGRID se divide en dos segmentos, el valor de Objetos administrados aumenta en tres después de que se completa la ingesta, de la siguiente manera:

`segment container + segment 1 + segment 2 = three stored objects`

¿Qué son las marcas de agua del volumen de almacenamiento?

StorageGRID utiliza tres marcas de agua 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 han pasado a un estado de solo lectura vuelvan a ser de lectura y escritura.



Las marcas de agua del volumen de almacenamiento solo se aplican al espacio utilizado para datos de objetos replicados y codificados para borrado. Para obtener más información sobre el espacio reservado para los metadatos de objetos en el volumen 0, vaya a ["Administrar el almacenamiento de metadatos de objetos"](#).

¿Qué es la marca de agua suave de solo lectura?

La **marca de agua de solo lectura suave del volumen de almacenamiento** es la primera marca de agua que indica que el espacio utilizable de un nodo de almacenamiento para los datos de objetos se está llenando.

Si cada volumen de un nodo de almacenamiento tiene menos espacio libre que la marca de agua de solo lectura de ese volumen, el nodo de almacenamiento pasa al *modo de solo lectura*. El modo de solo lectura significa que el nodo de almacenamiento anuncia servicios de solo lectura al resto del sistema StorageGRID, pero cumple con todas las solicitudes de escritura pendientes.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una marca de agua de solo lectura de 10 GB. Tan pronto como cada volumen tenga menos de 10 GB de espacio libre, el nodo de almacenamiento pasará al modo de solo lectura suave.

¿Qué es la marca de agua de sólo lectura?

La **marca de agua de solo lectura del volumen de almacenamiento** es la siguiente marca de agua que indica que el espacio utilizable de un nodo para los datos de objetos se está llenando.

Si el espacio libre en un volumen es menor que la marca de agua de solo lectura 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 menor que sus marcas de agua de solo lectura.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una marca de agua de solo lectura de 5 GB. Tan pronto como cada volumen tenga menos de 5 GB de espacio libre, el nodo de almacenamiento ya no aceptará ninguna solicitud de escritura.

La marca de agua de solo lectura dura siempre es menor que la marca de agua de solo lectura suave.

¿Qué es la marca de agua de lectura y escritura?

La **marca de agua de lectura y escritura del volumen de almacenamiento** se aplica únicamente a los nodos de almacenamiento que han pasado al modo de solo lectura. Determina cuándo el nodo puede volver a ser de lectura y escritura. Cuando el espacio libre en cualquier volumen de almacenamiento en un nodo de almacenamiento es mayor que la marca de agua de lectura y escritura de ese volumen, el nodo vuelve automáticamente al estado de lectura y escritura.

Por ejemplo, supongamos que el nodo de almacenamiento ha pasado al modo de solo lectura. Supongamos también que cada volumen tiene una marca de agua de lectura y escritura de 30 GB. Tan pronto como el espacio libre para cualquier volumen aumenta a 30 GB, el nodo vuelve a ser de lectura y escritura.

La marca de agua de lectura y escritura siempre es más grande que la marca de agua de solo lectura suave y que la marca de agua de solo lectura dura.

Ver marcas de agua del volumen de almacenamiento

Puede ver la configuración actual de la marca de agua y los valores optimizados del sistema. Si no se utilizan marcas de agua optimizadas, puede determinar si puede o debe ajustar la configuración.

Antes de empezar

- Ha completado la actualización a StorageGRID 11.6 o superior.
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).

Ver la configuración actual de la marca de agua

Puede ver la configuración actual de la marca de agua de almacenamiento en el Administrador de cuadrícula.

Pasos

1. Seleccione **SOPORTE > Otros > Marcas de agua de almacenamiento**.
2. En la página Marcas de agua de almacenamiento, mire la casilla de verificación Usar valores optimizados.
 - Si se selecciona la casilla de verificación, las tres marcas de agua se optimizan para cada volumen de almacenamiento en cada nodo de almacenamiento, según el tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

Esta es la configuración predeterminada y recomendada. No actualice estos valores. Opcionalmente, puedes [Ver marcas de agua de almacenamiento optimizadas](#).

- Si la casilla de verificación Usar valores optimizados no está seleccionada, se utilizarán marcas de agua personalizadas (no optimizadas). No se recomienda utilizar configuraciones de marca de agua personalizadas. Utilice las instrucciones para ["Solución de problemas de alertas de anulación de marca de agua de solo lectura baja"](#) para determinar si puede o debe ajustar la configuración.

Al especificar configuraciones de marca de agua personalizadas, debe ingresar valores mayores a 0.

Ver marcas de agua de almacenamiento optimizadas

StorageGRID utiliza dos métricas de Prometheus para mostrar los valores optimizados que ha calculado para la marca de agua de solo lectura del volumen de almacenamiento. Puede ver los valores mínimos y máximos optimizados para cada nodo de almacenamiento en su red.

1. Seleccione **SOPORTE > Herramientas > Métricas**.
2. En la sección Prometheus, seleccione el enlace para acceder a la interfaz de usuario de Prometheus.
3. Para ver la marca de agua de solo lectura mínima recomendada, ingrese la siguiente métrica de Prometheus y seleccione **Ejecutar**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

La última columna muestra el valor mínimo optimizado de la marca de agua de solo lectura suave para todos los volúmenes de almacenamiento en cada nodo de almacenamiento. Si este valor es mayor que la configuración personalizada para la marca de agua de solo lectura suave del volumen de almacenamiento, se activa la alerta **Anulación de marca de agua de solo lectura baja** para el nodo de almacenamiento.

4. Para ver la marca de agua de solo lectura suave máxima recomendada, ingrese la siguiente métrica de Prometheus y seleccione **Ejecutar**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

La última columna muestra el valor máximo optimizado de la marca de agua de solo lectura suave para todos los volúmenes de almacenamiento en cada nodo de almacenamiento.

Administrar el almacenamiento de metadatos de objetos

La capacidad de metadatos de objetos de un sistema StorageGRID controla la cantidad máxima de objetos que se pueden almacenar en ese sistema. Para garantizar que su sistema StorageGRID tenga espacio adecuado para almacenar nuevos objetos, debe comprender dónde y cómo StorageGRID almacena los metadatos de los objetos.

¿Qué son los metadatos de un objeto?

Los metadatos de un objeto son cualquier información que describe un objeto. StorageGRID utiliza metadatos de objetos para rastrear las ubicaciones de todos los objetos en la red y administrar el ciclo de vida de cada objeto a lo largo del tiempo.

Para un objeto en StorageGRID, los metadatos del objeto incluyen los siguientes tipos de información:

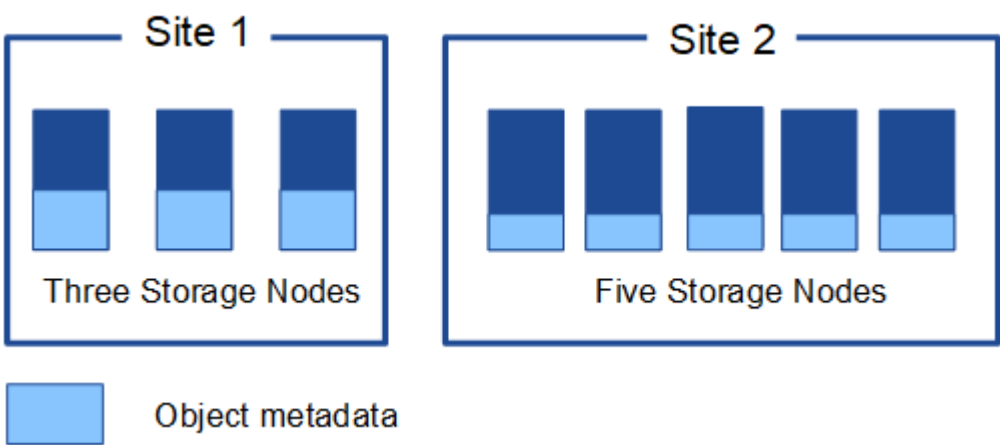
- Metadatos del sistema, incluido un ID único para cada objeto (UUID), el nombre del objeto, el nombre del depósito S3, el nombre o ID de la cuenta del inquilino, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez y la fecha y hora en que se modificó el objeto por última vez.
- Cualquier par clave-valor de metadatos de usuario personalizados asociados con el objeto.
- Para los objetos S3, cualquier par clave-valor de etiqueta de objeto asociado con el objeto.
- Para copias de objetos replicados, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos con código de borrado, la ubicación de almacenamiento actual de cada fragmento.

- Para las copias de objetos en un grupo de almacenamiento en la nube, la ubicación del objeto, incluido el nombre del depósito externo y el identificador único del objeto.
- Para objetos segmentados y objetos multiparte, identificadores de segmento y tamaños de datos.

¿Cómo se almacenan los metadatos de los objetos?

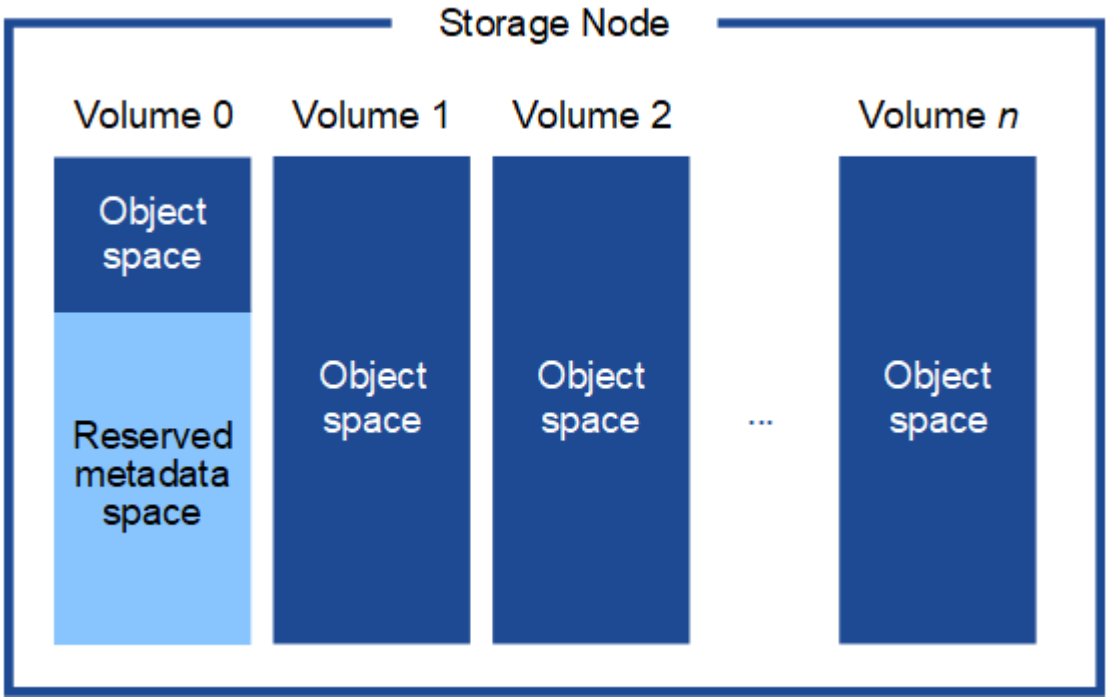
StorageGRID mantiene los metadatos de los objetos en una base de datos Cassandra, que se almacena independientemente de los datos de los objetos. Para proporcionar redundancia y proteger los metadatos de los objetos contra pérdidas, StorageGRID almacena tres copias de los metadatos de todos los objetos 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.



¿Dónde se almacenan los metadatos de los objetos?

Esta figura representa los volúmenes de almacenamiento para un solo 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 nodo de almacenamiento. Utiliza el espacio reservado para almacenar metadatos de objetos y realizar operaciones esenciales de la base de datos. Cualquier espacio restante en el volumen de almacenamiento 0 y todos los demás volúmenes de almacenamiento en el nodo de almacenamiento se utilizan exclusivamente para datos de objetos (copias replicadas y fragmentos con código de borrado).

La cantidad de espacio que se reserva para los metadatos de objetos en un nodo de almacenamiento en particular depende de varios factores, que se describen a continuación.

Configuración de espacio reservado para metadatos

El *Espacio reservado para metadatos* es una configuración 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 esta configuración se basa en:

- La versión del software que estaba utilizando cuando instaló StorageGRID inicialmente.
- La cantidad de RAM en cada nodo de almacenamiento.

Versión utilizada para la instalación inicial de StorageGRID	Cantidad de RAM en los nodos de almacenamiento	Configuración predeterminada del espacio reservado para metadatos
11,5 a 11,9	128 GB o más en cada nodo de almacenamiento de la red	8 TB (8000 GB)
	Menos de 128 GB en cualquier nodo de almacenamiento de la red	3 TB (3000 GB)
11.1 a 11.4	128 GB o más en cada nodo de almacenamiento en cualquier sitio	4 TB (4000 GB)
	Menos de 128 GB en cualquier nodo de almacenamiento en cada sitio	3 TB (3000 GB)
11.0 o anterior	Cualquier cantidad	2 TB (2000 GB)

Ver la configuración del espacio reservado de metadatos

Siga estos pasos para ver la configuración del espacio reservado de metadatos para su sistema StorageGRID .

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Configuración de almacenamiento**.
2. En la página de configuración de almacenamiento, expanda la sección **Espacio reservado de metadatos**.

Para StorageGRID 11.8 o superior, el valor del espacio reservado de metadatos debe ser de al menos 100 GB y no más de 1 PB.

La configuración predeterminada para una nueva instalación de StorageGRID 11.6 o superior en la que cada

nodo de almacenamiento tiene 128 GB o más de RAM es 8000 GB (8 TB).

Espacio reservado real para metadatos

A diferencia de la configuración de espacio reservado de metadatos de todo el sistema, el *espacio reservado real* para los metadatos de objetos se determina para cada nodo de almacenamiento. Para cualquier nodo de almacenamiento determinado, el espacio reservado real para metadatos depende del tamaño del volumen 0 del nodo y de la configuración del espacio reservado de metadatos de todo el sistema.

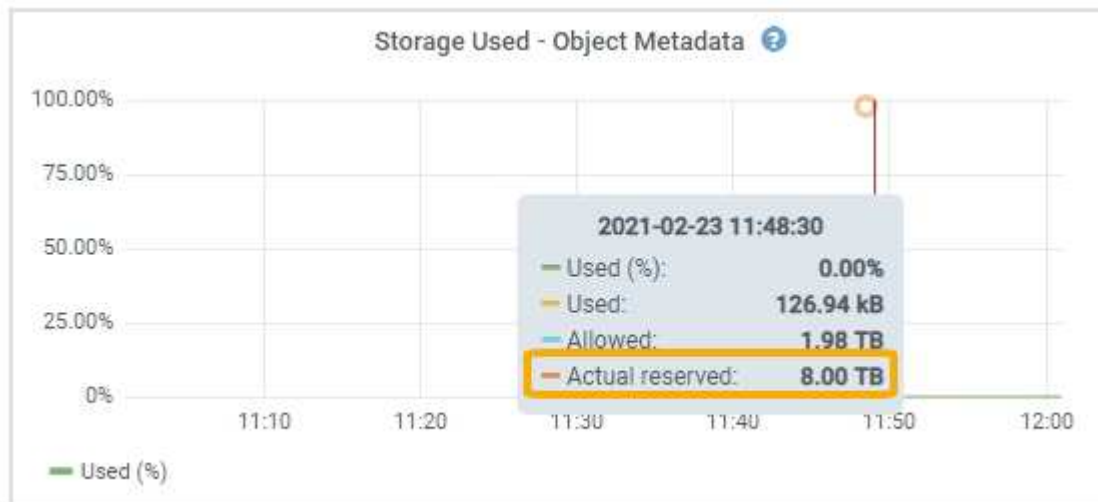
Tamaño del volumen 0 para el nodo	Espacio reservado real para metadatos
Menos de 500 GB (uso no productivo)	10% del volumen 0
500 GB o más + o + Nodos de almacenamiento solo de metadatos	El menor de estos valores: • Volumen 0 • Configuración de espacio reservado para metadatos Nota: Solo se requiere una rangedb para los nodos de almacenamiento de solo metadatos.

Ver el espacio reservado real para metadatos

Siga estos pasos para ver el espacio reservado real para metadatos en un nodo de almacenamiento en particular.

Pasos

1. Desde el Administrador de red, seleccione **NODOS** > **Nodo de almacenamiento**.
2. Seleccione la pestaña **Almacenamiento**.
3. Coloque el cursor sobre el gráfico Almacenamiento utilizado - Metadatos del objeto y localice el valor **Reservado real**.



En la captura de pantalla, el valor **real reservado** es 8 TB. Esta captura de pantalla es para un nodo de almacenamiento grande en una nueva instalación de StorageGRID 11.6. Debido a que la configuración de

espacio reservado de metadatos de todo el sistema es menor que el volumen 0 para este nodo de almacenamiento, el espacio reservado real para este nodo es igual a la configuración de espacio reservado de metadatos.

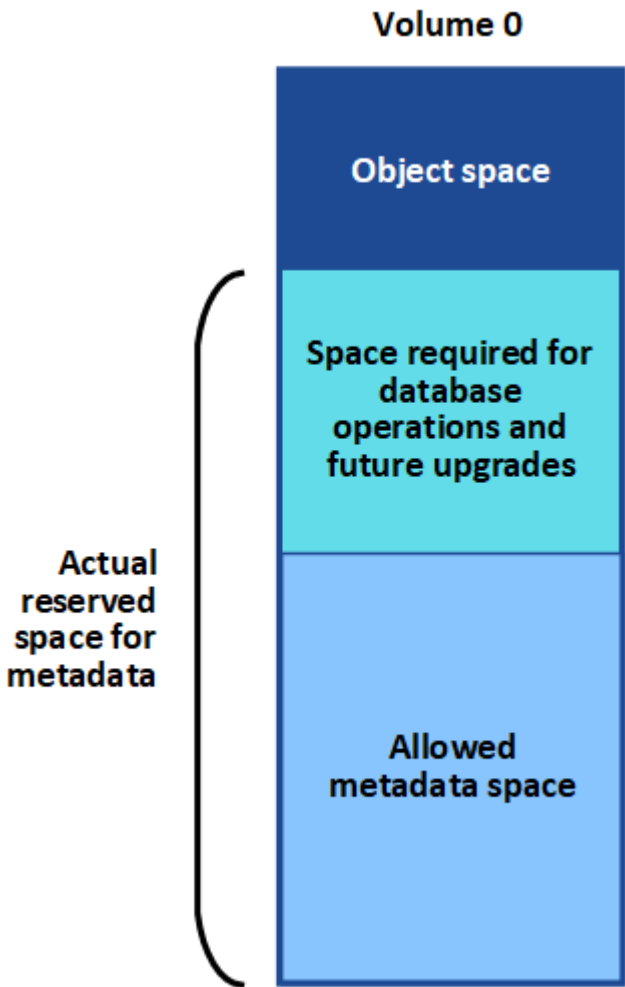
Ejemplo de espacio de metadatos reservado real

Supongamos que instala un nuevo sistema StorageGRID utilizando la versión 11.7 o posterior. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Basándonos en estos valores:

- El espacio reservado para metadatos de todo el sistema está establecido en 8 TB. (Este es el valor predeterminado para una nueva instalación de StorageGRID 11.6 o superior si cada nodo de almacenamiento tiene más de 128 GB de RAM).
- El espacio reservado real para metadatos para SN1 es de 6 TB. (Todo el volumen está reservado porque el volumen 0 es más pequeño que la configuración **Espacio reservado de metadatos**).

Espacio de metadatos permitido

El espacio reservado real de cada nodo de almacenamiento para metadatos se subdivide en el espacio disponible para metadatos de objetos (el *espacio de metadatos permitido*) y el espacio requerido para operaciones esenciales de la base de datos (como compactación y reparación) y futuras actualizaciones de hardware y software. El espacio de metadatos permitido determina la capacidad general del objeto.



La siguiente tabla muestra cómo StorageGRID calcula el **espacio de metadatos permitido** para diferentes

nodos de almacenamiento, en función de la cantidad de memoria del nodo y el espacio reservado real para metadatos.

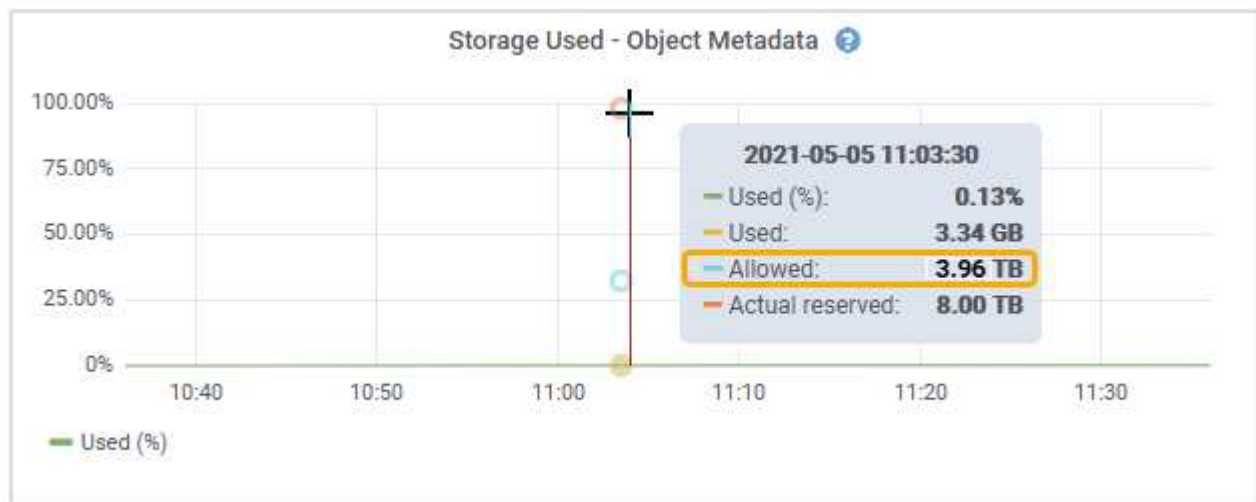
	Cantidad de memoria en el nodo de almacenamiento		
	< 128 GB	>= 128 GB	Espacio reservado real para metadatos
≤ 4 TB	60% del espacio real reservado para metadatos, hasta un máximo de 1,32 TB	60% del espacio real reservado para metadatos, hasta un máximo de 1,98 TB	4 TB

Ver el espacio de metadatos permitido

Siga estos pasos para ver el espacio de metadatos permitido para un nodo de almacenamiento.

Pasos

1. Desde el Administrador de cuadrícula, seleccione **NODOS**.
2. Seleccione el nodo de almacenamiento.
3. Seleccione la pestaña **Almacenamiento**.
4. Coloque el cursor sobre el gráfico de metadatos del objeto Almacenamiento utilizado y localice el valor **Permitido**.



En la captura de pantalla, el valor **Permitido** es 3,96 TB, que es el valor máximo para un nodo de almacenamiento cuyo espacio reservado real para metadatos es más de 4 TB.

El valor **Permitido** corresponde a esta métrica de Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Ejemplo de espacio de metadatos permitido

Supongamos que instala un sistema StorageGRID utilizando la versión 11.6. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Basándonos en estos valores:

- El espacio reservado para metadatos de todo el sistema está establecido en 8 TB. (Este es el valor predeterminado para StorageGRID 11.6 o superior cuando cada nodo de almacenamiento tiene más de 128 GB de RAM).
- El espacio reservado real para metadatos para SN1 es de 6 TB. (Todo el volumen está reservado porque el volumen 0 es más pequeño que la configuración **Espacio reservado de metadatos**).
- El espacio permitido para metadatos en SN1 es de 3 TB, según el cálculo que se muestra en [la tabla de espacio permitido para metadatos](#) : $(\text{Espacio reservado real para metadatos} - 1 \text{ TB}) \times 60 \%$, hasta un máximo de 3,96 TB.

Cómo los nodos de almacenamiento de diferentes tamaños afectan la capacidad de los objetos

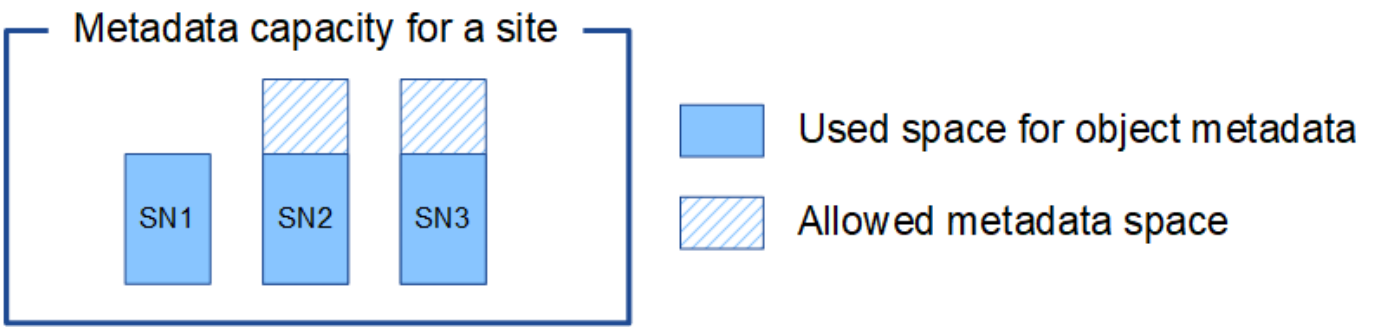
Como se describió anteriormente, StorageGRID distribuye uniformemente los metadatos de los objetos entre los nodos de almacenamiento en cada sitio. Por este motivo, si un sitio contiene nodos de almacenamiento de diferentes tamaños, el nodo más pequeño del sitio determina la capacidad de metadatos del sitio.

Consideremos el siguiente ejemplo:

- Tiene una cuadrícula de un solo sitio que contiene tres nodos de almacenamiento de diferentes tamaños.
- La configuración de **Espacio reservado para metadatos** es 4 TB.
- Los nodos de almacenamiento tienen los siguientes valores para el espacio de metadatos reservado real y el espacio de metadatos permitido.

Nodo de almacenamiento	Tamaño del volumen 0	Espacio de metadatos reservado real	Espacio de metadatos permitido
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

Debido a que los metadatos de los objetos se distribuyen de manera uniforme entre los nodos de almacenamiento de un sitio, cada nodo en este ejemplo solo puede contener 1,32 TB de metadatos. Los 0,66 TB adicionales de espacio de metadatos permitido para SN2 y SN3 no se pueden utilizar.



De manera similar, debido a que StorageGRID mantiene todos los metadatos de objetos de un sistema StorageGRID en cada sitio, la capacidad general de metadatos de un sistema StorageGRID está determinada por la capacidad de metadatos de objetos del sitio más pequeño.

Y como la capacidad de metadatos de un objeto controla el recuento máximo de objetos, cuando un nodo se queda sin capacidad de metadatos, la cuadrícula queda prácticamente llena.

Información relacionada

- Para aprender a monitorear la capacidad de metadatos de objetos para cada nodo de almacenamiento, consulte las instrucciones para ["Monitoreo de StorageGRID"](#) .
- Para aumentar la capacidad de metadatos de objetos para su sistema, ["expandir una cuadrícula"](#) agregando nuevos nodos de almacenamiento.

Aumentar la configuración del espacio reservado de metadatos

Es posible que pueda aumentar la configuración del sistema de espacio reservado de metadatos si sus nodos de almacenamiento cumplen requisitos específicos de RAM y espacio disponible.

Lo que necesitarás

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso raíz o la configuración de la página de topología de la red y otros permisos de configuración de la red"](#) .



La página de topología de cuadrícula ha quedado obsoleta y se eliminará en una versión futura.

Acerca de esta tarea

Es posible que pueda aumentar manualmente la configuración del Espacio reservado de metadatos de todo el sistema hasta 8 TB.

Solo puede aumentar el valor de la configuración de Espacio reservado de metadatos de todo el sistema si ambas afirmaciones son verdaderas:

- Los nodos de almacenamiento en cualquier sitio de su sistema tienen cada uno 128 GB o más de RAM.
- Cada uno de los nodos de almacenamiento de cualquier sitio de su sistema tiene suficiente espacio disponible en el volumen de almacenamiento 0.

Tenga en cuenta que si aumenta esta configuración, reducirá simultáneamente el espacio disponible para el almacenamiento de objetos en el volumen de almacenamiento 0 de todos los nodos de almacenamiento. Por este motivo, es posible que prefieras establecer el Espacio reservado de metadatos en un valor menor a 8 TB, en función de los requisitos de metadatos de tu objeto esperados.



En general, es mejor utilizar un valor más alto en lugar de un valor más bajo. Si la configuración de Espacio reservado de metadatos es demasiado grande, puede reducirla más tarde. Por el contrario, si aumenta el valor más adelante, es posible que el sistema necesite mover datos del objeto para liberar espacio.

Para obtener una explicación detallada de cómo la configuración del Espacio reservado de metadatos afecta el espacio permitido para el almacenamiento de metadatos de objetos en un nodo de almacenamiento en particular, consulte ["Administrar el almacenamiento de metadatos de objetos"](#) .

Pasos

1. Determinar la configuración actual del espacio reservado de metadatos.
 - a. Seleccione **CONFIGURACIÓN > Sistema > Opciones de almacenamiento**.
 - b. En la sección Marcas de agua de almacenamiento, anote el valor de **Espacio reservado de metadatos**.
2. Asegúrese de tener suficiente espacio disponible en el volumen de almacenamiento 0 de cada nodo de almacenamiento para aumentar este valor.
 - a. Seleccione **NODOS**.
 - b. Seleccione el primer nodo de almacenamiento en la cuadrícula.
 - c. Seleccione la pestaña Almacenamiento.
 - d. En la sección Volúmenes, busque la entrada **/var/local/rangedb/0**.
 - e. Confirme que el valor Disponible sea igual o mayor que la diferencia entre el nuevo valor que desea utilizar y el valor actual del Espacio reservado de metadatos.

Por ejemplo, si la configuración actual del Espacio reservado de metadatos es 4 TB y desea aumentarla a 6 TB, el valor Disponible debe ser 2 TB o más.

- f. Repita estos pasos para todos los nodos de almacenamiento.
 - Si uno o más nodos de almacenamiento no tienen suficiente espacio disponible, no se puede aumentar el valor del espacio reservado de metadatos. No continúe con este procedimiento.
 - Si cada nodo de almacenamiento tiene suficiente espacio disponible en el volumen 0, vaya al siguiente paso.
3. Asegúrese de tener al menos 128 GB de RAM en cada nodo de almacenamiento.
 - a. Seleccione **NODOS**.
 - b. Seleccione el primer nodo de almacenamiento en la cuadrícula.
 - c. Seleccione la pestaña **Hardware**.
 - d. Coloque el cursor sobre el gráfico de uso de memoria. Asegúrese de que la **Memoria total** sea de al menos 128 GB.
 - e. Repita estos pasos para todos los nodos de almacenamiento.
 - Si uno o más nodos de almacenamiento no tienen suficiente memoria total disponible, no se puede aumentar el valor del espacio reservado de metadatos. No continúe con este procedimiento.
 - Si cada nodo de almacenamiento tiene al menos 128 GB de memoria total, vaya al siguiente paso.
4. Actualice la configuración del espacio reservado de metadatos.
 - a. Seleccione **CONFIGURACIÓN > Sistema > Opciones de almacenamiento**.
 - b. Seleccione la pestaña Configuración.
 - c. En la sección Marcas de agua de almacenamiento, seleccione **Espacio reservado de metadatos**.
 - d. Introduzca el nuevo valor.

Por ejemplo, para ingresar 8 TB, que es el valor máximo admitido, ingrese **8000000000000** (8, seguido de 12 ceros)

Storage Options

Overview

Configuration



Configure Storage Options

Updated: 2021-12-10 13:48:23 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1000000000

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0
Storage Volume Soft Read-Only Watermark Override	0
Storage Volume Hard Read-Only Watermark Override	0
Metadata Reserved Space	800000000000

Apply Changes

a. Seleccione **Aplicar cambios**.

Comprimir objetos almacenados

Puede habilitar la compresión de objetos para reducir el tamaño de los objetos almacenados en StorageGRID, de modo que consuman menos almacenamiento.

Antes de empezar

- Ha 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 deshabilitada. Si habilita la compresión, StorageGRID intentará comprimir cada objeto al guardarlo, utilizando compresión sin pérdida.



Si cambia esta configuración, tomará aproximadamente un minuto para que se aplique la nueva configuración. El valor configurado se almacena en caché para mejorar el rendimiento y la escala.

Antes de habilitar la compresión de objetos, tenga en cuenta lo siguiente:

- No debe seleccionar **Comprimir objetos almacenados** a menos que sepa que los datos que se almacenan son comprimibles.
- Las aplicaciones que guardan objetos en StorageGRID pueden comprimirlos 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 seleccione **Comprimir objetos almacenados** si está utilizando NetApp FabricPool con StorageGRID.
- Si se selecciona **Comprimir objetos almacenados**, las aplicaciones cliente S3 deben evitar realizar operaciones GetObject que especifiquen un rango de bytes a devolver. Estas operaciones de "lectura de

rango" son ineficientes porque StorageGRID debe descomprimir efectivamente 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, es ineficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden expirar.



Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Configuración de almacenamiento > Compresión de objetos**.
2. Seleccione la casilla de verificación **Comprimir objetos almacenados**.
3. Seleccione **Guardar**.

Administrar nodos de almacenamiento completos

A medida que los nodos de almacenamiento alcanzan su capacidad, debe expandir el sistema StorageGRID mediante la incorporación de nuevo almacenamiento. Hay tres opciones disponibles: agregar volúmenes de almacenamiento, agregar estantes de expansión de almacenamiento y agregar nodos de almacenamiento.

Agregar volúmenes de almacenamiento

Cada nodo de almacenamiento admite una cantidad máxima de volúmenes de almacenamiento. El máximo definido varía según la plataforma. Si un nodo de almacenamiento contiene menos que la cantidad máxima de volúmenes de almacenamiento, puede agregar volúmenes para aumentar su capacidad. Vea las instrucciones para "[Ampliación de un sistema StorageGRID](#)".

Añadir estantes de expansión de almacenamiento

Algunos nodos de almacenamiento del dispositivo StorageGRID, como SG6060 o SG6160, pueden admitir estantes de almacenamiento adicionales. Si tiene dispositivos StorageGRID con capacidades de expansión que aún no se han ampliado a su capacidad máxima, puede agregar estantes de almacenamiento para aumentar la capacidad. Vea las instrucciones para "[Ampliación de un sistema StorageGRID](#)".

Agregar nodos de almacenamiento

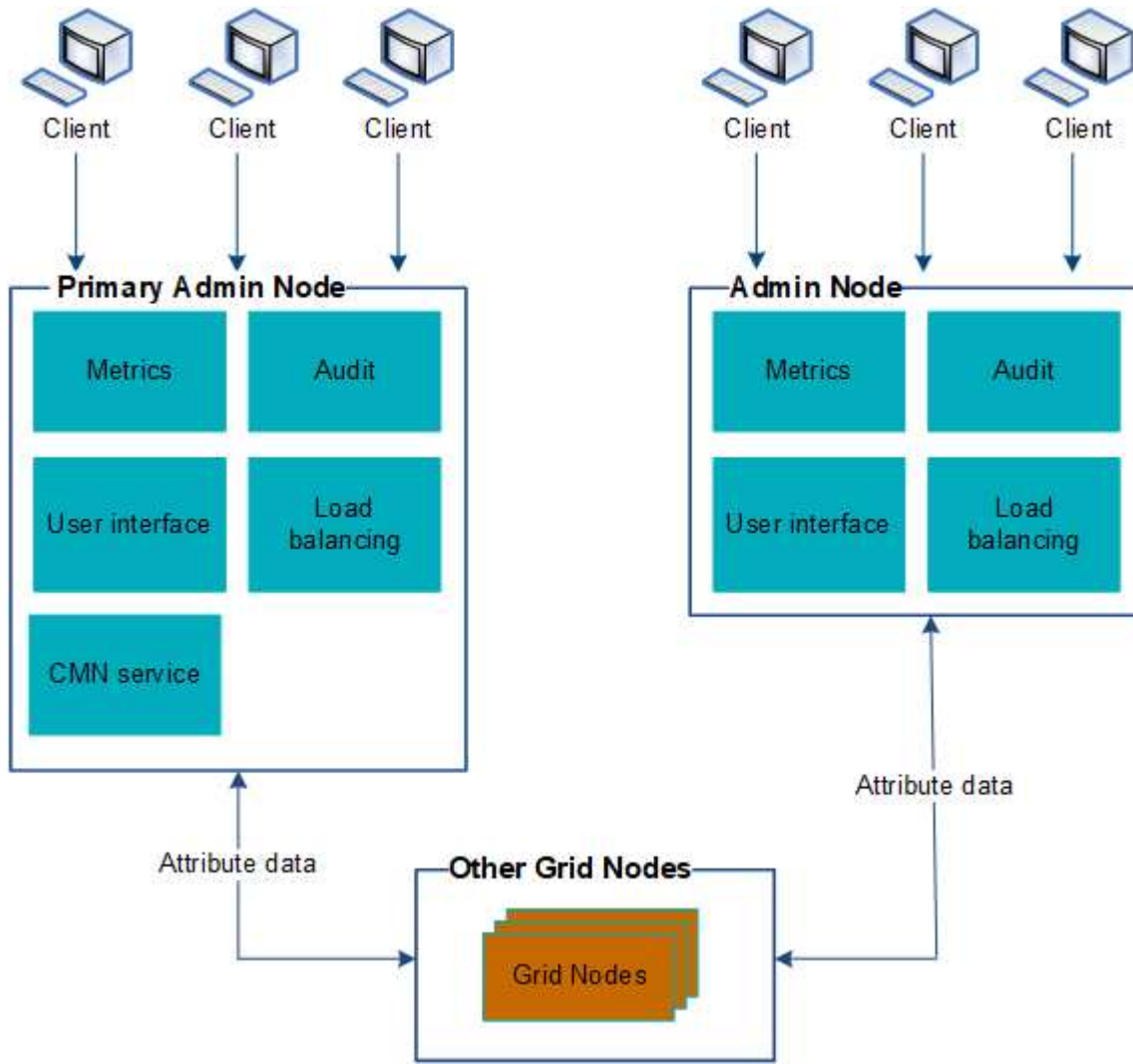
Puede aumentar la capacidad de almacenamiento agregando nodos de almacenamiento. Al agregar almacenamiento se debe tener en cuenta cuidadosamente las reglas ILM actualmente activas y los requisitos de capacidad. Vea las instrucciones para "[Ampliación de un sistema StorageGRID](#)".

Administrar nodos de administración

Utilice varios nodos de administración

Un sistema StorageGRID puede incluir varios nodos de administración para permitirle supervisar y configurar continuamente su sistema StorageGRID incluso si falla un nodo de administración.

Si un nodo de administración deja de estar disponible, el procesamiento de atributos continúa, se siguen activando alertas y se siguen enviando notificaciones por correo electrónico y paquetes de AutoSupport . Sin embargo, tener varios nodos de administración no proporciona protección contra conmutación por error, excepto para las notificaciones y los paquetes de AutoSupport .



Hay dos opciones para continuar viendo y configurando el sistema StorageGRID si falla un nodo de administración:

- Los clientes web pueden reconectarse 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 Administrador de red o al Administrador de inquilinos mediante la dirección IP virtual del grupo de alta disponibilidad. Ver ["Administrar grupos de alta disponibilidad"](#) .



Al utilizar un grupo HA, el acceso se interrumpe si falla el nodo de administración activo. Los usuarios deben iniciar sesión nuevamente después de que la dirección IP virtual del grupo HA se conmute a otro nodo de administración en el grupo.

Algunas tareas de mantenimiento solo se pueden realizar mediante el nodo de administración principal. Si el nodo de administración principal falla, debe recuperarse antes de que el sistema StorageGRID vuelva a funcionar por completo.

Identificar el nodo de administración principal

El nodo de administración principal proporciona más funciones 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, consulte "[¿Qué es un nodo de administración?](#)".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes "[permisos de acceso específicos](#)".

Pasos

1. Seleccione **NODOS**.
2. Introduzca **primary** en el cuadro de búsqueda.

En los resultados de la búsqueda, identifique el nodo con "Nodo de administración principal" que se muestra en la columna Tipo. Se debe incluir un nodo de administración principal.

Ver el estado de las notificaciones y las colas

El servicio del Sistema de administración de red (NMS) en los nodos de administración envía notificaciones al servidor de correo. Puede ver el estado actual del servicio NMS y el tamaño de su cola de notificaciones en la página Motor de interfaz.

Para acceder a la página Motor de interfaz, seleccione **SOPORTE > Herramientas > Topología de cuadrícula**. Luego seleccione **site > Admin Node > NMS > Interface Engine**.

The screenshot displays the 'Overview: NMS (170-176) - Interface Engine' page. At the top, there are tabs for 'Overview', 'Alarms', 'Reports', and 'Configuration'. Below the tabs, the page title is 'Overview: NMS (170-176) - Interface Engine' with a timestamp 'Updated: 2009-03-09 10:12:17 PDT'. The main content area is divided into three sections:

- NMS Interface Engine Status:** Shows 'Connected' with a green checkmark icon. Below it, 'Connected Services:' shows '15' with a green checkmark icon.
- E-mail Notification Events:** Shows 'E-mail Notifications Status:' as 'No Errors' and 'E-mail Notifications Queued:' as '0', both with green checkmark icons.
- Database Connection Pool:** Shows 'Maximum Supported Capacity:' as '100', 'Remaining Capacity:' as '95 %', and 'Active Connections:' as '5', all with green checkmark icons.

Las notificaciones se procesan a través de la cola de notificaciones por correo electrónico y se envían al servidor de correo una tras otra en el orden en que se activan. Si hay un problema (por ejemplo, un error de conexión de red) y el servidor de correo no está disponible cuando se intenta enviar la notificación, el máximo esfuerzo posible para reenviar la notificación al servidor de correo continúa durante un período de 60 segundos. Si la notificación no se envía al servidor de correo después de 60 segundos, la notificación se

elimina de la cola de notificaciones y se intenta enviar la siguiente notificación en la cola.

Administrar objetos con ILM

Administrar objetos con ILM

Las reglas de administración del ciclo de vida de la información (ILM) en una política ILM indican a StorageGRID cómo crear y distribuir copias de datos de objetos y cómo administrar esas copias a lo largo del tiempo.

Acerca de estas instrucciones

El diseño y la implementación de reglas y políticas de ILM requieren una planificación cuidadosa. Debe comprender sus requisitos operativos, la topología de su sistema StorageGRID, sus necesidades de protección de objetos y los tipos de almacenamiento disponibles. Luego, debes determinar cómo quieres que se copien, distribuyan y almacenen los diferentes tipos de objetos.

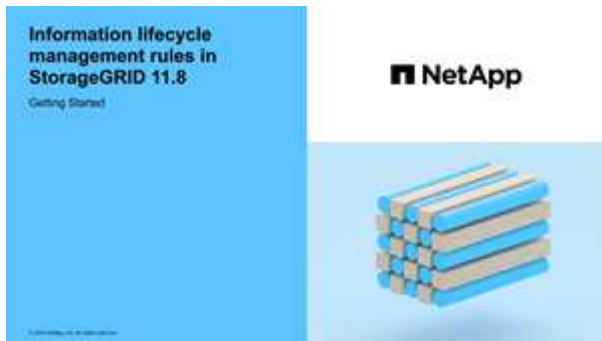
Utilice estas instrucciones para:

- Obtenga más información sobre StorageGRID ILM, incluido ["Cómo funciona ILM a lo largo de la vida de un objeto"](#).
- Aprenda a configurar ["grupos de almacenamiento"](#), ["Grupos de almacenamiento en la nube"](#), y ["Reglas de ILM"](#).
- Aprenda cómo ["crear, simular y activar una política ILM"](#) que protegerá los datos de los objetos en uno o más sitios.
- Aprenda cómo ["Administrar objetos con S3 Object Lock"](#), lo que ayuda a garantizar que los objetos en depósitos S3 específicos no se eliminen ni se sobrescriban durante un período de tiempo específico.

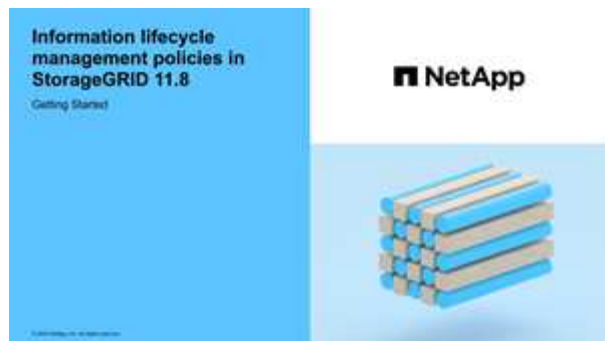
Más información

Para obtener más información, revise estos videos:

- ["Vídeo: Resumen de las reglas de ILM"](#).



- ["Vídeo: Resumen de las políticas de ILM"](#)



ILM y ciclo de vida de los objetos

Cómo funciona ILM a lo largo de la vida de un objeto

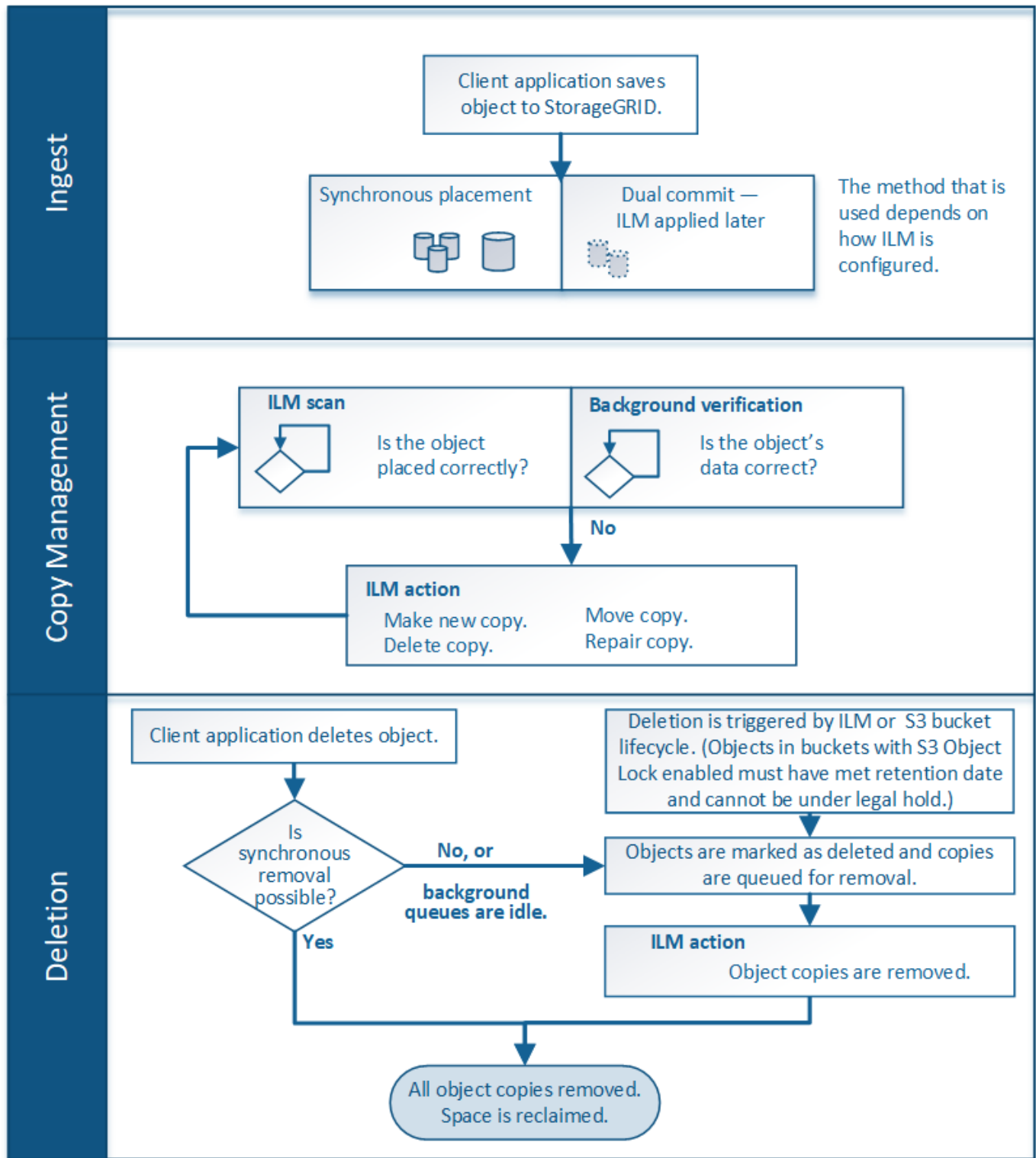
Comprender cómo StorageGRID utiliza ILM para administrar objetos durante cada etapa de su vida puede ayudarlo a diseñar una política más efectiva.

- **Ingesta:** la ingesta comienza cuando una aplicación cliente S3 establece una conexión para guardar un objeto en el sistema StorageGRID y se completa cuando StorageGRID devuelve un mensaje de "ingesta exitosa" al cliente. Los datos de los objetos se protegen durante la ingesta ya sea aplicando instrucciones ILM inmediatamente (colocación sincrónica) o creando copias provisionales y aplicando ILM más tarde (confirmación dual), dependiendo de cómo se especificaron los requisitos de ILM.
- **Administración de copias:** después de crear la cantidad y el tipo de copias de objetos que se especifican en las instrucciones de ubicación de ILM, StorageGRID administra las ubicaciones de los objetos y los protege contra pérdidas.
 - **Escaneo y evaluación de ILM:** StorageGRID escanea continuamente la lista de objetos almacenados en la red y verifica si las copias actuales cumplen con los requisitos de ILM. Cuando se requieren diferentes tipos, números o ubicaciones de copias de objetos, StorageGRID crea, elimina o mueve copias según sea necesario.
 - **Verificación en segundo plano:** StorageGRID realiza continuamente una verificación en segundo plano para comprobar la integridad de los datos de los objetos. Si se encuentra un problema, StorageGRID crea automáticamente una nueva copia del objeto o un fragmento de objeto con código de borrado de reemplazo en una ubicación que cumpla con los requisitos ILM actuales. Ver ["Verificar la integridad del objeto"](#).
- **Eliminación de objetos:** la administración de un objeto finaliza cuando se eliminan todas las copias del sistema StorageGRID. Los objetos se pueden eliminar como resultado de una solicitud de eliminación por parte de un cliente, o como resultado de una eliminación por parte de ILM o una eliminación causada por la expiración del ciclo de vida de un bucket de S3.



Los objetos de un bucket que tiene habilitado el bloqueo de objetos S3 no se pueden eliminar si están bajo una retención legal o si se ha especificado una fecha de retención pero aún no se cumple.

El diagrama resume cómo funciona ILM a lo largo del ciclo de vida de un objeto.



Cómo se ingieren los objetos

Opciones de ingesta

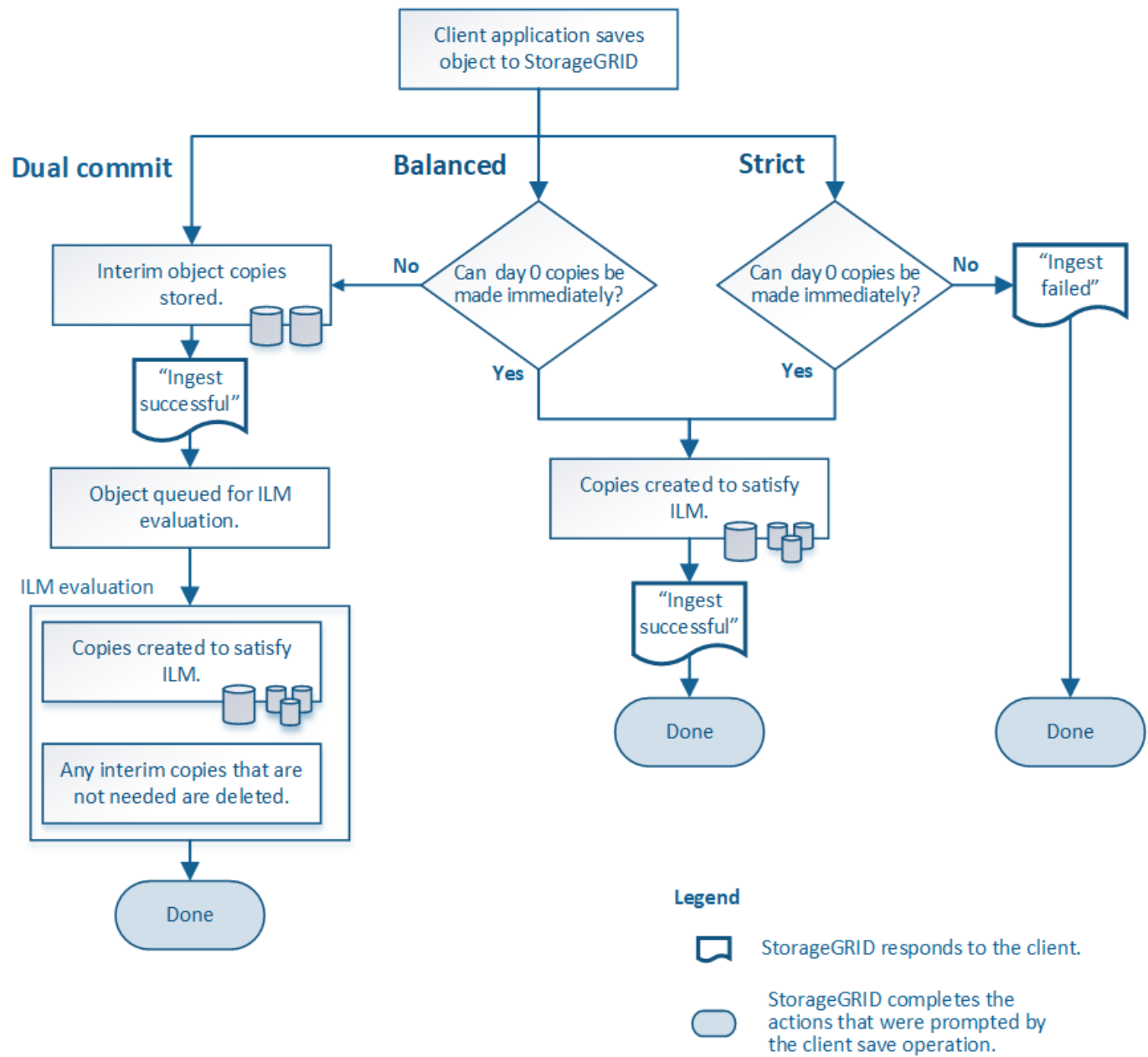
Cuando crea una regla ILM, especifica una de tres opciones para proteger objetos durante la ingesta: Confirmación dual, Estricta o Equilibrada.

Según su elección, StorageGRID realiza copias provisionales y pone en cola los objetos para una evaluación

ILM posterior, o utiliza la ubicación sincrónica y realiza copias inmediatamente para cumplir con los requisitos de ILM.

Diagrama de flujo de opciones de ingesta

El diagrama de flujo muestra lo que sucede cuando los objetos coinciden con una regla ILM que utiliza cada una de las tres opciones de ingesta.



Compromiso dual

Cuando selecciona la opción de confirmación dual, StorageGRID realiza inmediatamente copias de objetos provisionales en dos nodos de almacenamiento diferentes y devuelve un mensaje de "ingesta exitosa" al cliente. El objeto se pone en cola para la evaluación de ILM y luego se realizan copias que cumplen con las instrucciones de ubicación de la regla. Si la política ILM no se puede procesar inmediatamente después de la confirmación dual, la protección contra pérdida del sitio podría llevar tiempo.

Utilice la opción de confirmación dual en cualquiera de estos casos:

- Está utilizando reglas ILM de múltiples sitios y la latencia de ingesta del cliente es su consideración principal. Al usar la confirmación dual, debe asegurarse de que su cuadrícula pueda realizar el trabajo adicional de crear y eliminar las copias de confirmación dual si no satisfacen ILM. Específicamente:
 - La carga en la red debe ser lo suficientemente baja para evitar un retraso en la ILM.
 - La red debe tener recursos de hardware excedentes (IOPS, CPU, memoria, ancho de banda de red, etc.).
- Está utilizando reglas ILM de varios sitios y la conexión WAN entre los sitios generalmente tiene alta latencia o ancho de banda limitado. En este escenario, el uso de la opción de confirmación dual puede ayudar a evitar tiempos de espera del cliente. Antes de elegir la opción de confirmación dual, debe probar la aplicación cliente con cargas de trabajo realistas.

Equilibrado (predeterminado)

Cuando selecciona la opción Equilibrado, StorageGRID también utiliza la ubicación sincrónica en la ingesta y realiza inmediatamente todas las copias especificadas en las instrucciones de ubicación de la regla. A diferencia de la opción Estricta, si StorageGRID no puede realizar todas las copias inmediatamente, utiliza la confirmación dual en su lugar. Si la política ILM utiliza ubicaciones en varios sitios y no se puede lograr una protección inmediata contra pérdida de sitios, se activa la alerta **Ubicación ILM inalcanzable**.

Utilice la opción Equilibrado para lograr la mejor combinación de protección de datos, rendimiento de la red y éxito de ingesta. Equilibrado es la opción predeterminada en el asistente Crear regla ILM.

Estricto

Cuando selecciona la opción Estricto, StorageGRID utiliza la ubicación sincrónica en la ingesta y realiza inmediatamente todas las copias de objetos especificadas en las instrucciones de ubicación de la regla. La ingesta falla si StorageGRID no puede crear todas las copias, por ejemplo, porque una ubicación de almacenamiento requerida no está disponible temporalmente. El cliente debe volver a intentar la operación.

Utilice la opción Estricto si tiene un requisito operativo o reglamentario para almacenar inmediatamente objetos solo en las ubicaciones descritas en la regla ILM. Por ejemplo, para satisfacer un requisito reglamentario, es posible que necesite utilizar la opción Estricto y un filtro avanzado de Restricción de ubicación para garantizar que los objetos nunca se almacenen en determinados centros de datos.

Ver ["Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto"](#) .

Ventajas, desventajas y limitaciones de las opciones de ingesta

Comprender las ventajas y desventajas de cada una de las tres opciones para proteger datos en la ingesta (equilibrada, estricta o confirmación dual) puede ayudarlo a decidir cuál seleccionar para una regla ILM.

Para obtener una descripción general de las opciones de ingesta, consulte ["Opciones de ingesta"](#) .

Ventajas de las opciones Equilibrada y Estricta

En comparación con la confirmación dual, que crea copias provisionales durante la ingesta, las dos opciones de ubicación sincrónica pueden proporcionar las siguientes ventajas:

- **Mejor seguridad de los datos:** los datos de los objetos se protegen inmediatamente como se especifica en las instrucciones de ubicación de las reglas ILM, que se pueden configurar para proteger contra una amplia variedad de condiciones de falla, incluida la falla de más de una ubicación de almacenamiento. La confirmación dual solo puede proteger contra la pérdida de una única copia local.

- **Operación de red más eficiente:** cada objeto se procesa solo una vez, a medida que se ingiere. Debido a que el sistema StorageGRID no necesita rastrear ni eliminar copias provisionales, hay menos carga de procesamiento y se consume menos espacio de base de datos.
- **(Equilibrado) Recomendado:** La opción Equilibrada proporciona una eficiencia ILM óptima. Se recomienda usar la opción Equilibrada a menos que se requiera un comportamiento de ingesta estricto o la cuadrícula cumpla con todos los criterios para usar la confirmación dual.
- **(Estricta) Certeza sobre las ubicaciones de los objetos:** La opción Estricta garantiza que los objetos se almacenen inmediatamente de acuerdo con las instrucciones de ubicación de la regla ILM.

Desventajas de las opciones equilibrada y estricta

En comparación con la confirmación dual, las opciones equilibrada y estricta tienen algunas desventajas:

- **Ingestas de cliente más prolongadas:** las latencias de ingesta de cliente pueden ser más prolongadas. Cuando se utilizan las opciones Equilibrado o Estricto, no se devuelve un mensaje de "ingesta exitosa" al cliente hasta que se crean y almacenan todos los fragmentos codificados de borrado o copias replicadas. Sin embargo, lo más probable es que los datos de los objetos lleguen a su ubicación final mucho más rápido.
- **(Estricto) Mayores tasas de errores de ingesta:** con la opción Estricto, la ingesta falla siempre que StorageGRID no pueda realizar inmediatamente todas las copias especificadas en la regla ILM. Es posible que observe altas tasas de errores de ingesta si una ubicación de almacenamiento requerida está temporalmente fuera de línea o si los problemas de red causan demoras en la copia de objetos entre sitios.
- **(Estricto) Las ubicaciones de carga multiparte de S3 podrían no ser las esperadas en algunas circunstancias:** con Estricto, se espera que los objetos se coloquen como lo describe la regla ILM o que la ingesta falle. Sin embargo, con una carga multiparte de S3, ILM se evalúa para cada parte del objeto a medida que se ingiere y para el objeto como un todo cuando se completa la carga multiparte. En las siguientes circunstancias, esto podría dar lugar a ubicaciones diferentes a las esperadas:
 - **Si ILM cambia mientras una carga multiparte de S3 está en progreso:** debido a que cada parte se coloca de acuerdo con la regla que está activa cuando se ingiere la parte, es posible que algunas partes del objeto no cumplan con los requisitos actuales de ILM cuando se complete la carga multiparte. En estos casos la ingesta del objeto no falla. En cambio, cualquier pieza que no esté colocada correctamente se pone en cola para una reevaluación de ILM y se mueve a la ubicación correcta más tarde.
 - **Cuando las reglas ILM filtran por tamaño:** al evaluar ILM para una pieza, StorageGRID filtra por el tamaño de la pieza, no por el tamaño del objeto. Esto significa que partes de un objeto pueden almacenarse en ubicaciones que no cumplen los requisitos de ILM para el objeto en su totalidad. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan en DC1, mientras que todos los objetos más pequeños se almacenan en DC2, al momento de la ingesta cada parte de 1 GB de una carga multiparte de 10 partes se almacena en DC2. Cuando se evalúa ILM para el objeto, todas las partes del objeto se mueven a DC1.
- **(Estricto) La ingesta no falla cuando se actualizan las etiquetas o los metadatos de los objetos y no se pueden realizar las nuevas ubicaciones requeridas:** con Estricto, se espera que los objetos se coloquen como lo describe la regla ILM o que la ingesta falle. Sin embargo, cuando se actualizan los metadatos o las etiquetas de un objeto que ya está almacenado en la cuadrícula, el objeto no se vuelve a ingerir. Esto significa que cualquier cambio en la ubicación de los objetos que se active mediante la actualización no se realiza de inmediato. Los cambios de ubicación se realizan cuando el ILM se vuelve a evaluar mediante procesos ILM en segundo plano normales. Si no se pueden realizar los cambios de ubicación requeridos (por ejemplo, porque la nueva ubicación requerida no está disponible), el objeto actualizado conserva su ubicación actual hasta que sea posible realizar los cambios de ubicación.

Limitaciones en la ubicación de objetos con las opciones Equilibrado y Estricto

Las opciones Equilibrado o Estricto no se pueden usar para reglas ILM que tengan alguna de estas instrucciones de ubicación:

- Ubicación en un grupo de almacenamiento en la nube el día 0.
- Ubicaciones en un grupo de almacenamiento en la nube cuando la regla tiene un tiempo de creación definido por el usuario como su tiempo de referencia.

Estas restricciones existen porque StorageGRID no puede realizar copias de manera sincrónica a un grupo de almacenamiento en la nube, y un tiempo de creación definido por el usuario podría resolverse en el presente.

Cómo interactúan las reglas y la consistencia de ILM para afectar la protección de datos

Tanto su regla ILM como su elección de consistencia afectan cómo se protegen los objetos. Estas configuraciones pueden interactuar.

Por ejemplo, el comportamiento de ingesta seleccionado para una regla ILM afecta la ubicación inicial de las copias de objetos, mientras que la consistencia utilizada cuando se almacena un objeto afecta la ubicación inicial de los metadatos del objeto. Debido a que StorageGRID requiere acceso a los datos y metadatos de un objeto para cumplir con las solicitudes de los clientes, seleccionar niveles de protección coincidentes para la consistencia y el comportamiento de ingesta puede brindar una mejor protección de datos inicial y respuestas del sistema más predecibles.

A continuación se muestra un breve resumen de los valores de consistencia disponibles en StorageGRID:

- **Todos:** Todos los nodos reciben metadatos del objeto inmediatamente o la solicitud fallará.
- **Fuerte-global:** Los metadatos de los objetos se distribuyen inmediatamente a todos los sitios. Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.
- **Sitio fuerte:** los metadatos del objeto se distribuyen inmediatamente a otros nodos del sitio. Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes dentro de un sitio.
- **Lectura después de nueva escritura:** proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Recomendado para la mayoría de los casos.
- **Disponible:** Proporciona consistencia eventual tanto para objetos nuevos como para actualizaciones de objetos. Para los buckets S3, úselo solo cuando sea necesario (por ejemplo, para un bucket que contiene valores de registro que rara vez se leen, o para operaciones HEAD o GET en claves que no existen). No compatible con depósitos S3 FabricPool .



Antes de seleccionar un valor de consistencia, "[Lea la descripción completa de la consistencia](#)". Debe comprender los beneficios y las limitaciones antes de cambiar el valor predeterminado.

Ejemplo de cómo la consistencia y las reglas ILM pueden interactuar

Supongamos que tiene una cuadrícula de dos sitios con la siguiente regla ILM y la siguiente consistencia:

- **Regla ILM:** Crea dos copias de objetos, una en el sitio local y otra en un sitio remoto. Utilice el comportamiento de ingesta estricto.
- **Consistencia:** Fuerte-global (los metadatos del objeto se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en la red, StorageGRID realiza copias de los objetos y distribuye metadatos a ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra pérdida en el momento del mensaje de ingesta exitosa. Por ejemplo, si el sitio local se pierde poco después de la ingesta, aún existen copias de los datos del objeto y de los metadatos del objeto en el sitio remoto. El objeto es completamente recuperable.

Si, en cambio, utilizara la misma regla ILM y la consistencia del sitio fuerte, el cliente podría recibir un mensaje de éxito después de que los datos del objeto se repliquen en el sitio remoto pero antes de que los metadatos del objeto se distribuyan allí. En este caso, el nivel de protección de los metadatos del objeto no coincide con el nivel de protección de los datos del objeto. Si el sitio local se pierde poco después de la ingesta, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre la consistencia y las reglas ILM puede ser compleja. Comuníquese con NetApp si necesita ayuda.

Información relacionada

["Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto"](#)

Cómo se almacenan los objetos (codificación de replicación o borrado)

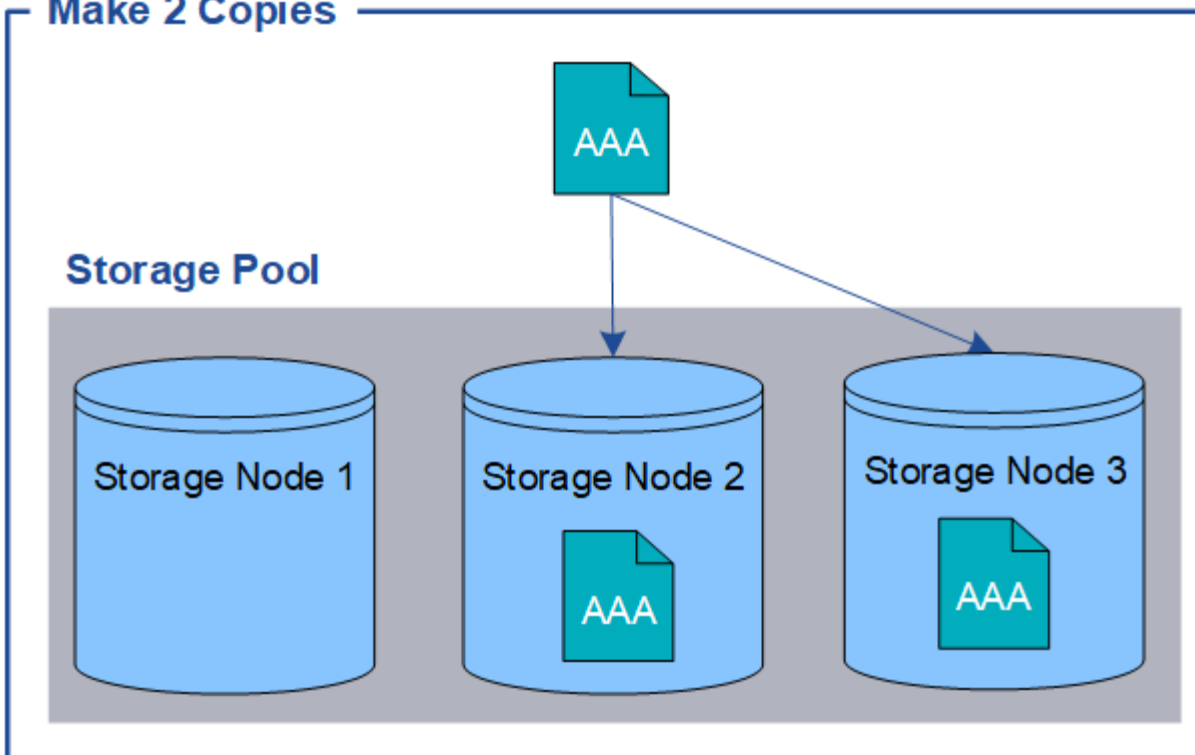
¿Qué es la replicación?

La replicación es uno de los dos métodos utilizados por StorageGRID para almacenar datos de objetos (la codificación de borrado es el otro método). Cuando los objetos coinciden con una regla ILM que utiliza replicación, el sistema crea copias exactas de los datos de los objetos y almacena las copias en los nodos de almacenamiento.

Cuando configura una regla ILM para crear copias replicadas, especifica cuántas copias se deben crear, dónde se deben colocar esas copias y durante cuánto tiempo se deben almacenar las copias en cada ubicación.

En el siguiente ejemplo, la regla ILM especifica que dos copias replicadas de cada objeto se coloquen en un grupo de almacenamiento que contiene tres nodos de almacenamiento.

Make 2 Copies



Cuando StorageGRID hace coincidir objetos con esta regla, crea dos copias del objeto y coloca cada copia en un nodo de almacenamiento diferente en el grupo de almacenamiento. Las dos copias se pueden colocar en cualquiera de los dos de los tres nodos de almacenamiento disponibles. En este caso, la regla colocó copias de objetos en los nodos de almacenamiento 2 y 3. Dado que hay dos copias, el objeto se puede recuperar si alguno de los nodos del grupo de almacenamiento falla.



StorageGRID solo puede almacenar una copia replicada de un objeto en cualquier nodo de almacenamiento determinado. Si su red incluye tres nodos de almacenamiento y crea una regla ILM de 4 copias, solo se realizarán tres copias: una copia para cada nodo de almacenamiento. La alerta **Colocación ILM inalcanzable** se activa para indicar que la regla ILM no se pudo aplicar por completo.

Información relacionada

- ["¿Qué es la codificación de borrado?"](#)
- ["¿Qué es un pool de almacenamiento?"](#)
- ["Habilite la protección contra pérdida de sitios mediante codificación de replicación y borrado"](#)

Por qué no debería utilizar la replicación de copia única

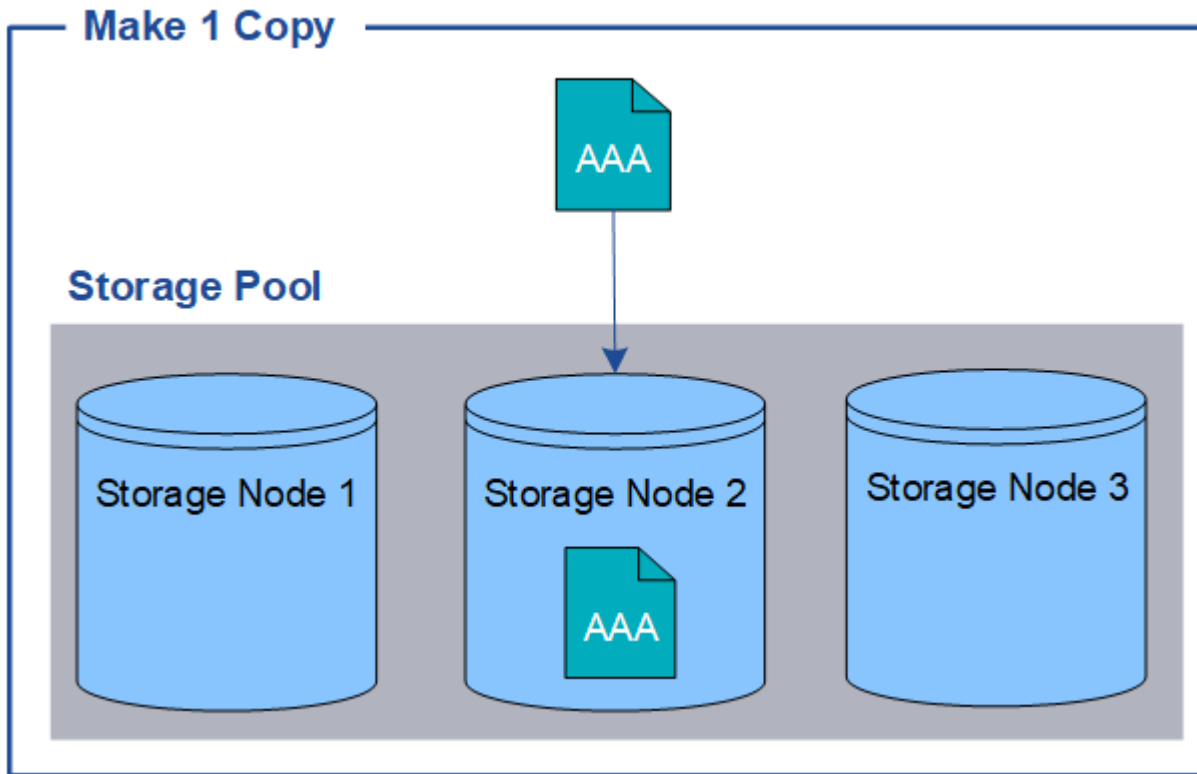
Al crear una regla ILM para crear copias replicadas, siempre debe especificar al menos dos copias para cualquier período de tiempo en las instrucciones de ubicación.



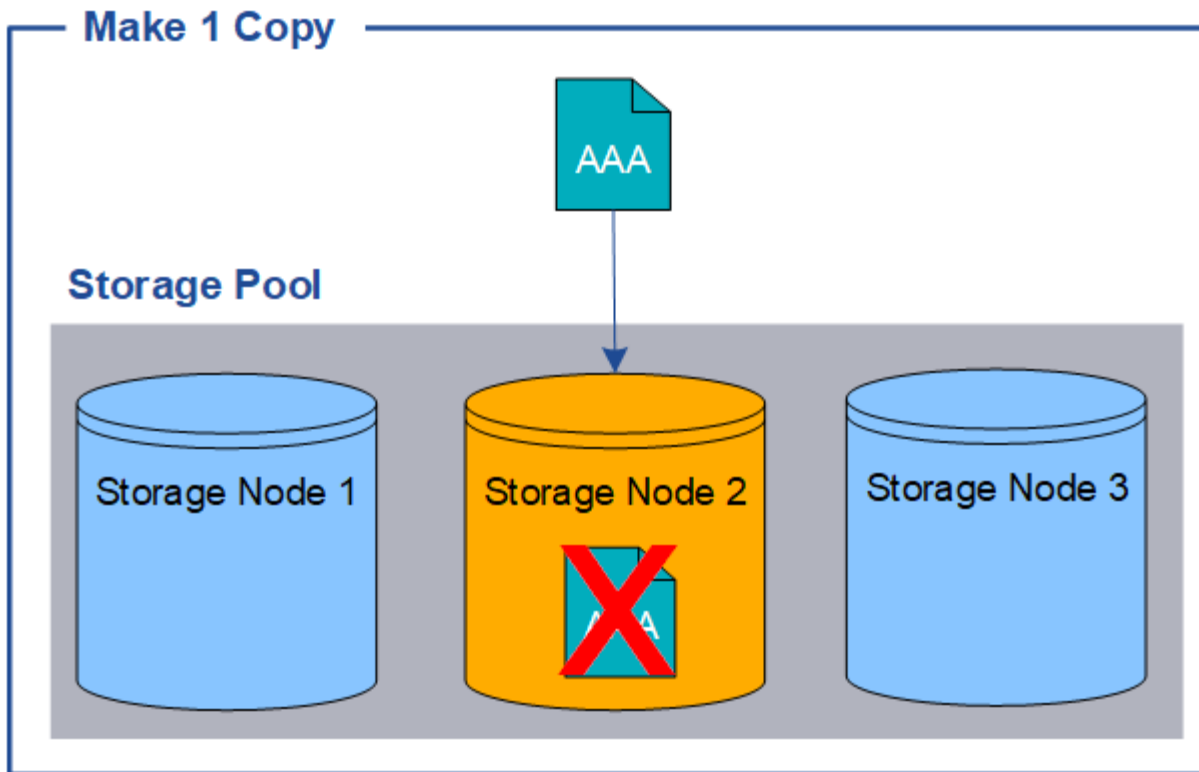
No utilice una regla ILM que cree solo una copia replicada por un período de tiempo determinado. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

En el siguiente ejemplo, la regla ILM Realizar 1 copia especifica que una copia replicada de un objeto se

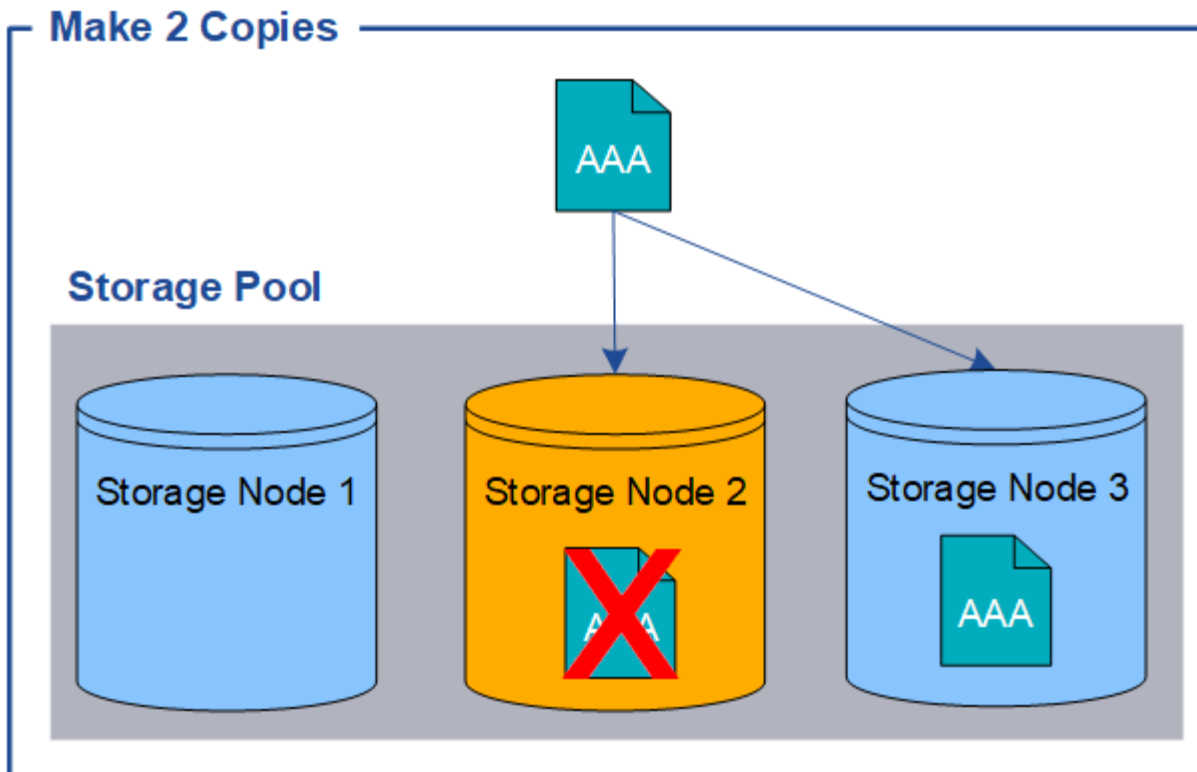
coloque en un grupo de almacenamiento que contenga tres nodos de almacenamiento. Cuando se ingiere un objeto que coincide con esta regla, StorageGRID coloca una única copia en un solo nodo de almacenamiento.



Cuando una regla ILM crea solo una copia replicada de un objeto, el objeto se vuelve inaccesible cuando el nodo de almacenamiento no está disponible. En este ejemplo, perderá temporalmente el acceso al objeto AAA siempre que el Nodo de almacenamiento 2 esté fuera de línea, como durante una actualización u otro procedimiento de mantenimiento. Perderá el objeto AAA por completo si falla el Nodo de almacenamiento 2.



Para evitar perder datos de objetos, siempre debe hacer al menos dos copias de todos los objetos que desee proteger con replicación. Si existen dos o más copias, aún podrá acceder al objeto si un nodo de almacenamiento falla o se desconecta.



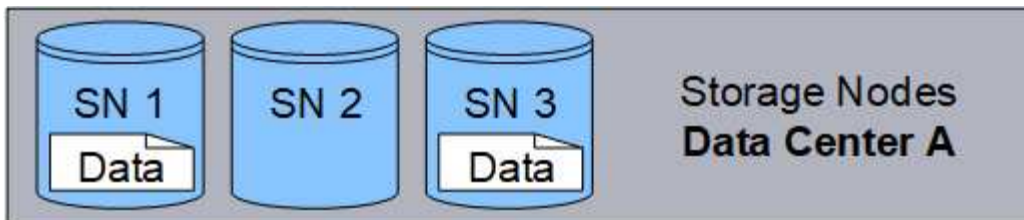
¿Qué es la codificación de borrado?

La codificación de borrado es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos (la replicación es el otro método). Cuando los objetos coinciden con una regla ILM que utiliza codificación de borrado, esos objetos se dividen en fragmentos de datos, se calculan fragmentos de paridad adicionales y cada fragmento se almacena en un nodo de almacenamiento diferente.

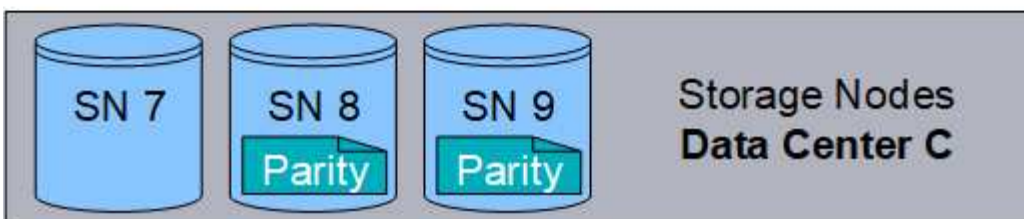
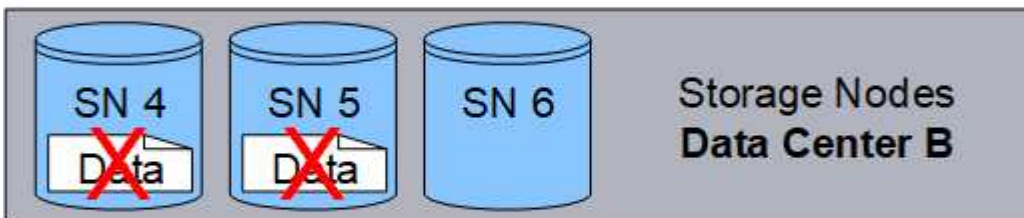
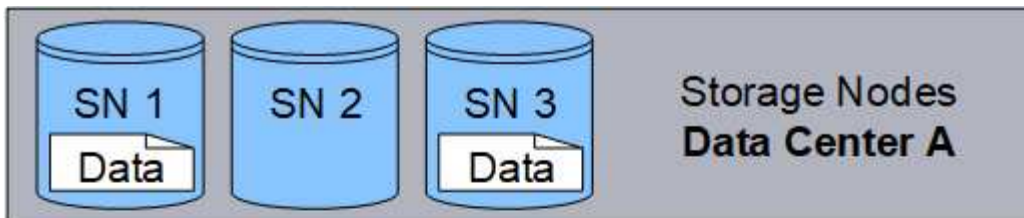
Cuando se accede a un objeto, se vuelve a ensamblar utilizando los fragmentos almacenados. Si un fragmento de datos o de paridad se corrompe o se pierde, el algoritmo de codificación de borrado puede recrear ese fragmento utilizando un subconjunto de los fragmentos de datos y de paridad restantes.

A medida que crea reglas ILM, StorageGRID crea perfiles de codificación de borrado que admiten esas reglas. Puede ver una lista de perfiles de codificación de borrado, ["cambiar el nombre de un perfil de codificación de borrado"](#), o ["Desactivar un perfil de codificación de borrado si no se utiliza actualmente en ninguna regla ILM"](#).

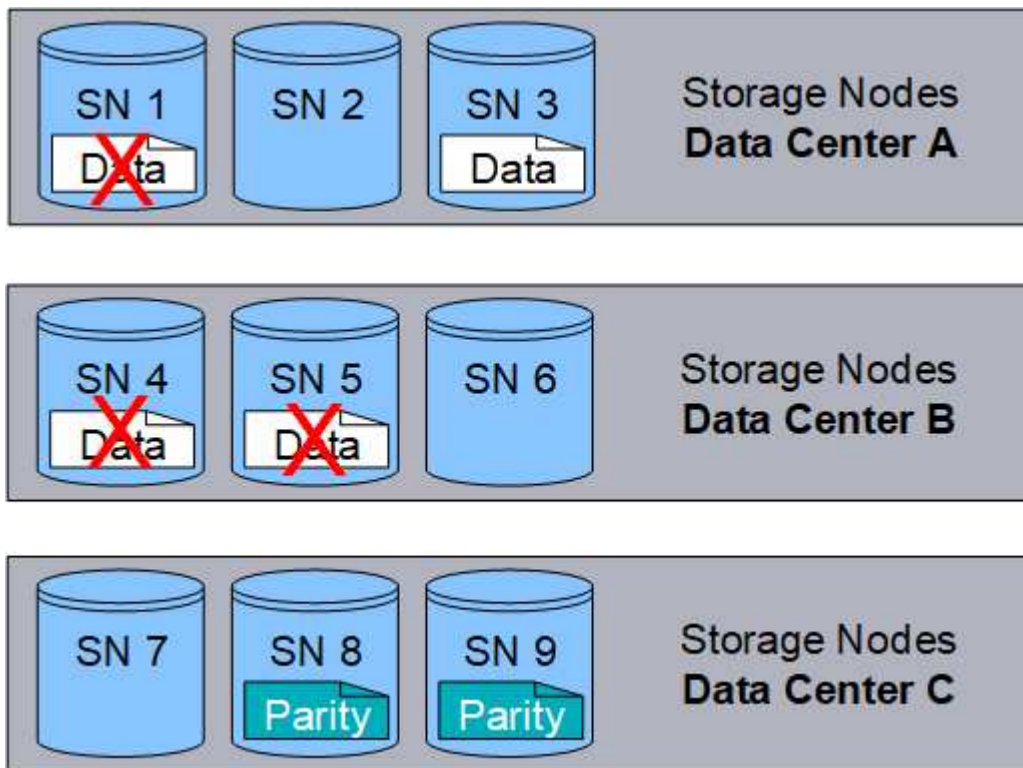
El siguiente ejemplo ilustra el uso de un algoritmo de codificación de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y se calculan dos fragmentos de paridad a partir de los datos del objeto. Cada uno de los seis fragmentos se almacena en un nodo diferente en tres sitios de centros de datos para brindar protección de datos ante fallas de nodos o pérdidas de sitios.



El esquema de codificación de borrado 4+2 se puede configurar de varias maneras. Por ejemplo, puede configurar un grupo de almacenamiento de un solo sitio que contenga seis nodos de almacenamiento. Para "protección contra pérdida de sitio", puede utilizar un grupo de almacenamiento que contenga tres sitios con tres nodos de almacenamiento en cada sitio. Se puede recuperar un objeto siempre que cuatro de los seis fragmentos (datos o paridad) permanezcan disponibles. Se pueden perder hasta dos fragmentos sin perder los datos del objeto. Si se pierde un sitio entero, el objeto aún puede recuperarse o repararse, siempre que todos los demás fragmentos permanezcan accesibles.



Si se pierden más de dos nodos de almacenamiento, el objeto no se podrá recuperar.



Información relacionada

- ["¿Qué es la replicación?"](#)
- ["¿Qué es un pool de almacenamiento?"](#)
- ["¿Qué son los esquemas de codificación de borrado?"](#)
- ["Cambiar el nombre de un perfil de codificación de borrado"](#)
- ["Desactivar un perfil de codificación de borrado"](#)

¿Qué son los esquemas de codificación de borrado?

Los esquemas de codificación de borrado controlan cuántos fragmentos de datos y cuántos fragmentos de paridad se crean para cada objeto.

Cuando crea o edita una regla ILM, selecciona un esquema de codificación de borrado disponible. StorageGRID crea automáticamente esquemas de codificación de borrado en función de la cantidad de nodos de almacenamiento y sitios que conforman el grupo de almacenamiento que planea utilizar.

Protección de datos

El sistema StorageGRID utiliza el algoritmo de codificación de borrado Reed-Solomon. El algoritmo divide un objeto en k fragmentos de datos y m fragmentos de paridad.

El $k + m = n$ Los fragmentos se encuentran dispersos en n Nodos de almacenamiento para proporcionar protección de datos de la siguiente manera:

- Para recuperar o reparar un objeto, k Se necesitan fragmentos.
- Un objeto puede soportar hasta m fragmentos perdidos o corruptos. Cuanto mayor sea el valor de m ,

mayor será la tolerancia al fallo.

La mejor protección de datos la proporciona el esquema de codificación de borrado con la mayor tolerancia a fallas de nodo o volumen dentro de un grupo de almacenamiento.

Gastos generales de almacenamiento

La sobrecarga de almacenamiento de un esquema de codificación de borrado se calcula dividiendo el número de fragmentos de paridad(m) por el número de fragmentos de datos(k). Puede utilizar la sobrecarga de almacenamiento para calcular cuánto espacio en disco requiere cada objeto con código de borrado:

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Por ejemplo, si almacena un objeto de 10 MB utilizando el esquema 4+2 (que tiene una sobrecarga de almacenamiento del 50 %), el objeto consume 15 MB de almacenamiento en la red. Si almacena el mismo objeto de 10 MB utilizando el esquema 6+2 (que tiene una sobrecarga de almacenamiento del 33 %), el objeto consume aproximadamente 13,3 MB.

Seleccione el esquema de codificación de borrado con el valor total más bajo de $k+m$ que se ajuste a sus necesidades. Los esquemas de codificación de borrado con un menor número de fragmentos son computacionalmente más eficientes porque:

- Se crean y distribuyen (o recuperan) menos fragmentos por objeto
- Muestran un mejor rendimiento porque el tamaño del fragmento es mayor
- Pueden requerir que se agreguen menos nodos en un ["expansión cuando se requiere más almacenamiento"](#)

Directrices para los pools de almacenamiento

Al seleccionar el grupo de almacenamiento que se utilizará para una regla que creará una copia con código de borrado, utilice las siguientes pautas para los grupos de almacenamiento:

- El grupo de almacenamiento debe incluir tres o más sitios, o exactamente un sitio.



No se puede utilizar la codificación de borrado si el grupo de almacenamiento incluye dos sitios.

- [Esquemas de codificación de borrado para grupos de almacenamiento que contienen tres o más sitios](#)
- [Esquemas de codificación de borrado para grupos de almacenamiento de un solo sitio](#)
- No utilice un grupo de almacenamiento que incluya el sitio Todos los sitios.
- El grupo de almacenamiento debe incluir al menos $k+m + 1$ Nodos de almacenamiento que pueden almacenar datos de objetos.



Los nodos de almacenamiento se pueden configurar durante la instalación para que contengan solo metadatos de objetos y no datos de objetos. Para obtener más información, consulte ["Tipos de nodos de almacenamiento"](#).

El número mínimo de nodos de almacenamiento requeridos es $k+m$. Sin embargo, tener al menos un nodo de almacenamiento adicional puede ayudar a prevenir fallas de ingesta o retrasos en ILM si un nodo de almacenamiento requerido no está disponible temporalmente.

Esquemas de codificación de borrado para grupos de almacenamiento que contienen tres o más sitios

La siguiente tabla describe los esquemas de codificación de borrado actualmente admitidos por StorageGRID para grupos de almacenamiento que incluyen tres o más sitios. Todos estos esquemas brindan protección contra pérdida de sitio. Se puede perder un sitio y el objeto seguirá siendo accesible.

Para los esquemas de codificación de borrado que brindan protección contra pérdida de sitio, la cantidad recomendada de nodos de almacenamiento en el grupo de almacenamiento excede $k+m + 1$ porque cada sitio requiere un mínimo de tres nodos de almacenamiento.

Esquema de codificación de borrado ($k+m$)	Número mínimo de sitios implementados	Número recomendado de nodos de almacenamiento en cada sitio	Número total recomendado de nodos de almacenamiento	¿Protección contra pérdida de sitio?	Gastos generales de almacenamiento
4+2	3	3	9	Sí	50%
6+2	4	3	12	Sí	33%
8+2	5	3	15	Sí	25%
6+3	3	4	12	Sí	50%
9+3	4	4	16	Sí	33%
2+1	3	3	9	Sí	50%
4+1	5	3	15	Sí	25%
6+1	7	3	21	Sí	17%
7+5	3	5	15	Sí	71%



StorageGRID requiere un mínimo de tres nodos de almacenamiento por sitio. Para utilizar el esquema 7+5, cada sitio requiere un mínimo de cuatro nodos de almacenamiento. Se recomienda utilizar cinco nodos de almacenamiento por sitio.

Al seleccionar un esquema de codificación de borrado que proporcione protección del sitio, equilibre la importancia relativa de los siguientes factores:

- **Número de fragmentos:** el rendimiento y la flexibilidad de expansión generalmente son mejores cuando el número total de fragmentos es menor.
- **Tolerancia a fallos:** La tolerancia a fallos aumenta al tener más segmentos de paridad (es decir, cuando m tiene un valor más alto.)
- **Tráfico de red:** Al recuperarse de fallas, se utiliza un esquema con más fragmentos (es decir, un total más alto para $k+m$) crea más tráfico de red.
- **Gastos generales de almacenamiento:** los esquemas con mayores gastos generales requieren más espacio de almacenamiento por objeto.

Por ejemplo, al decidir entre un esquema 4+2 y un esquema 6+3 (ambos tienen una sobrecarga de almacenamiento del 50 %), seleccione el esquema 6+3 si se requiere tolerancia a fallas adicional. Seleccione el esquema 4+2 si los recursos de red están limitados. Si todos los demás factores son iguales, seleccione 4+2 porque tiene un número total menor de fragmentos.



Si no está seguro de qué esquema utilizar, seleccione 4+2 o 6+3, o comuníquese con el soporte técnico.

Esquemas de codificación de borrado para grupos de almacenamiento de un solo sitio

Un grupo de almacenamiento de un solo sitio admite todos los esquemas de codificación de borrado definidos para tres o más sitios, siempre que el sitio tenga suficientes nodos de almacenamiento.

El número mínimo de nodos de almacenamiento requeridos es $k+m$, pero un grupo de almacenamiento con $k+m +1$ Se recomiendan nodos de almacenamiento. Por ejemplo, el esquema de codificación de borrado 2+1 requiere un grupo de almacenamiento con un mínimo de tres nodos de almacenamiento, pero se recomiendan cuatro nodos de almacenamiento.

Esquema de codificación de borrado ($k+m$)	Número mínimo de nodos de almacenamiento	Número recomendado de nodos de almacenamiento	Gastos generales de almacenamiento
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Ventajas, desventajas y requisitos de la codificación de borrado

Antes de decidir si utilizar la codificación de borrado o replicación para proteger los datos de los objetos contra pérdidas, debe comprender las ventajas, desventajas y los requisitos de la codificación de borrado.

Ventajas de la codificación de borrado

En comparación con la replicación, la codificación de borrado ofrece mayor confiabilidad, disponibilidad y

eficiencia de almacenamiento.

- **Confiabilidad:** La confiabilidad se mide en términos de tolerancia a fallas, es decir, la cantidad de fallas simultáneas que pueden mantenerse sin pérdida de datos. Con la replicación, se almacenan múltiples copias idénticas en diferentes nodos y en distintos sitios. Con la codificación de borrado, un objeto se codifica en fragmentos de datos y paridad y se distribuye entre muchos nodos y sitios. Esta dispersión proporciona protección contra fallas tanto del sitio como del nodo. En comparación con la replicación, la codificación de borrado proporciona una confiabilidad mejorada a costos de almacenamiento comparables.
- **Disponibilidad:** La disponibilidad se puede definir como la capacidad de recuperar objetos si los nodos de almacenamiento fallan o se vuelven inaccesibles. En comparación con la replicación, la codificación de borrado proporciona una mayor disponibilidad a costos de almacenamiento comparables.
- **Eficiencia de almacenamiento:** para niveles similares de disponibilidad y confiabilidad, los objetos protegidos mediante codificación de borrado consumen menos espacio en disco que los mismos objetos si estuvieran protegidos mediante replicación. Por ejemplo, un objeto de 10 MB que se replica en dos sitios consume 20 MB de espacio en disco (dos copias), mientras que un objeto que tiene un código de borrado en tres sitios con un esquema de codificación de borrado 6+3 solo consume 15 MB de espacio en disco.



El espacio en disco para objetos con código de borrado se calcula como el tamaño del objeto más la sobrecarga de almacenamiento. El porcentaje de sobrecarga de almacenamiento es la cantidad de fragmentos de paridad dividida por la cantidad de fragmentos de datos.

Desventajas de la codificación de borrado

En comparación con la replicación, la codificación de borrado tiene las siguientes desventajas:

- Se recomienda un mayor número de nodos y sitios de almacenamiento, según el esquema de codificación de borrado. Por el contrario, si replica datos de objetos, solo necesita un nodo de almacenamiento para cada copia. Ver ["Esquemas de codificación de borrado para grupos de almacenamiento que contienen tres o más sitios"](#) y ["Esquemas de codificación de borrado para grupos de almacenamiento de un solo sitio"](#).
- Aumento del coste y la complejidad de las ampliaciones de almacenamiento. Para expandir una implementación que utiliza replicación, agregue capacidad de almacenamiento en cada ubicación donde se realizan copias de objetos. Para expandir una implementación que utiliza codificación de borrado, debe considerar tanto el esquema de codificación de borrado en uso como qué tan llenos están los nodos de almacenamiento existentes. Por ejemplo, si espera hasta que los nodos existentes estén 100% llenos, debe agregar al menos $k+m$ Nodos de almacenamiento, pero si se expande cuando los nodos existentes están llenos al 70 %, puede agregar dos nodos por sitio y aún así maximizar la capacidad de almacenamiento utilizable. Para obtener más información, consulte ["Añadir capacidad de almacenamiento para objetos con código de borrado"](#).
- Hay mayores latencias de recuperación cuando se utiliza codificación de borrado en sitios distribuidos geográficamente. Los fragmentos de objeto de un objeto codificado para borrado y distribuido en sitios remotos tardan más en recuperarse a través de conexiones WAN que los de un objeto replicado y disponible localmente (el mismo sitio al que se conecta el cliente).
- Cuando se utiliza codificación de borrado en sitios distribuidos geográficamente, hay un mayor uso de tráfico de red WAN para recuperaciones y reparaciones, especialmente para objetos recuperados con frecuencia o para reparaciones de objetos a través de conexiones de red WAN.
- Cuando se utiliza codificación de borrado en varios sitios, el rendimiento máximo de objetos disminuye drásticamente a medida que aumenta la latencia de la red entre los sitios. Esta disminución se debe a la disminución correspondiente en el rendimiento de la red TCP, lo que afecta la rapidez con la que el sistema StorageGRID puede almacenar y recuperar fragmentos de objetos.

- Mayor uso de recursos computacionales.

Cuándo utilizar la codificación de borrado

La codificación de borrado es la más adecuada para los siguientes requisitos:

- Objetos de tamaño superior a 1 MB.



La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

- Almacenamiento a largo plazo o en frío para contenido que se recupera con poca frecuencia.
- Alta disponibilidad y confiabilidad de los datos.
- Protección contra fallas completas del sitio y del nodo.
- Eficiencia de almacenamiento.
- Implementaciones de un solo sitio que requieren una protección de datos eficiente con una única copia con código de borrado en lugar de múltiples copias replicadas.
- Implementaciones de múltiples sitios donde la latencia entre sitios es inferior a 100 ms.

Cómo se determina la retención de objetos

StorageGRID ofrece opciones para que los administradores de la red y los usuarios individuales especifiquen durante cuánto tiempo almacenar los objetos. En general, cualquier instrucción de retención proporcionada por un usuario inquilino tiene prioridad sobre las instrucciones de retención proporcionadas por el administrador de la red.

Cómo los usuarios inquilinos controlan la retención de objetos

Los usuarios inquilinos pueden usar estos métodos para controlar cuánto tiempo se almacenan sus objetos en StorageGRID:

- Si la configuración global de Bloqueo de objetos S3 está habilitada para la red, los usuarios inquilinos de S3 pueden crear depósitos con el Bloqueo de objetos S3 habilitado y luego seleccionar un **Período de retención predeterminado** para cada depósito.
- Si la configuración global de Bloqueo de objetos S3 está habilitada para la red, los usuarios inquilinos de S3 pueden crear depósitos con Bloqueo de objetos S3 habilitado y luego usar la API REST de S3 para especificar configuraciones de retención hasta la fecha y retención legal para cada versión de objeto agregada a ese depósito.
 - Una versión de un objeto que se encuentra bajo retención legal no se puede eliminar mediante ningún método.
 - Antes de que se alcance la fecha de conservación de una versión de un objeto, esa versión no se puede eliminar mediante ningún método.
 - Los objetos en depósitos con el bloqueo de objetos S3 habilitado son retenidos por ILM "para siempre". Sin embargo, una vez alcanzada su fecha de retención, una versión de un objeto puede eliminarse mediante una solicitud del cliente o mediante la expiración del ciclo de vida del depósito. Ver ["Administrar objetos con S3 Object Lock"](#).
- Los usuarios inquilinos de S3 pueden agregar una configuración de ciclo de vida a sus depósitos que

especifique una acción de vencimiento. Si existe un ciclo de vida de depósito, StorageGRID almacena un objeto hasta que se cumpla la fecha o la cantidad de días especificados en la acción Vencimiento, a menos que el cliente elimine el objeto primero. Ver ["Crear la configuración del ciclo de vida de S3"](#).

- Un cliente S3 puede emitir una solicitud de eliminación de objeto. StorageGRID siempre prioriza las solicitudes de eliminación del cliente sobre el ciclo de vida del bucket S3 o ILM al determinar si eliminar o conservar un objeto.

Cómo los administradores de red controlan la retención de objetos

Los administradores de la red pueden utilizar estos métodos para controlar la retención de objetos:

- Establezca un período máximo de retención de bloqueo de objetos S3 para cada inquilino. Luego, los usuarios inquilinos pueden establecer un período de retención predeterminado para cada uno de sus depósitos. El período máximo de retención también se aplica a cualquier objeto recién ingerido para ese depósito (fecha de retención del objeto).
- Cree instrucciones de ubicación de ILM para controlar durante cuánto tiempo se almacenan los objetos. Cuando los objetos coinciden con una regla ILM, StorageGRID almacena esos objetos hasta que transcurra el último período de tiempo de la regla ILM. Los objetos se conservan indefinidamente si se especifica "para siempre" en las instrucciones de ubicación.
- Independientemente de quién controla cuánto tiempo se conservan los objetos, las configuraciones de ILM controlan qué tipos de copias de objetos (replicadas o codificadas por borrado) se almacenan y dónde se ubican las copias (nodos de almacenamiento o grupos de almacenamiento en la nube).

Cómo interactúan el ciclo de vida del bucket S3 y ILM

Cuando se configura un ciclo de vida de un bucket S3, las acciones de vencimiento del ciclo de vida anulan la política ILM para los objetos que coinciden con el filtro del ciclo de vida. Como resultado, un objeto podría permanecer en la cuadrícula incluso después de que hayan transcurrido las instrucciones ILM para colocar el objeto.

Ejemplos de retención de objetos

Para comprender mejor las interacciones entre S3 Object Lock, las configuraciones del ciclo de vida del bucket, las solicitudes de eliminación de clientes e ILM, considere los siguientes ejemplos.

Ejemplo 1: El ciclo de vida del depósito S3 conserva los objetos durante más tiempo que ILM

ILM

Almacenar dos copias durante 1 año (365 días)

Ciclo de vida del bucket

Los objetos expiran en 2 años (730 días)

Resultado

StorageGRID almacena el objeto durante 730 días. StorageGRID utiliza la configuración del ciclo de vida del depósito para determinar si se debe eliminar o conservar un objeto.



Si el ciclo de vida del depósito especifica que los objetos deben conservarse durante más tiempo del especificado por ILM, StorageGRID continúa usando las instrucciones de ubicación de ILM al determinar la cantidad y el tipo de copias a almacenar. En este ejemplo, se continuarán almacenando dos copias del objeto en StorageGRID desde el día 366 al 730.

Ejemplo 2: El ciclo de vida del depósito S3 hace que los objetos caduquen antes que ILM

ILM

Conservar dos copias durante 2 años (730 días)

Ciclo de vida del bucket

Los objetos expiran en 1 año (365 días)

Resultado

StorageGRID elimina ambas copias del objeto después del día 365.

Ejemplo 3: La eliminación del cliente anula el ciclo de vida del depósito y el ILM

ILM

Almacenar dos copias en nodos de almacenamiento "para siempre"

Ciclo de vida del bucket

Los objetos expiran en 2 años (730 días)

Solicitud de eliminación de cliente

Emitido el día 400

Resultado

StorageGRID elimina ambas copias del objeto el día 400 en respuesta a la solicitud de eliminación del cliente.

Ejemplo 4: El bloqueo de objetos S3 anula la solicitud de eliminación del cliente

Bloqueo de objetos S3

La fecha de conservación hasta para una versión de objeto es 2026-03-31. No está en vigor ninguna retención legal.

Regla ILM compatible

Almacenar dos copias en nodos de almacenamiento "para siempre"

Solicitud de eliminación de cliente

Emitido el 31/03/2024

Resultado

StorageGRID no eliminará la versión del objeto porque la fecha de conservación aún está a 2 años de distancia.

Cómo se eliminan los objetos

StorageGRID puede eliminar objetos ya sea en respuesta directa a una solicitud del cliente o automáticamente como resultado de la expiración del ciclo de vida de un bucket S3 o los requisitos de la política ILM. Comprender las diferentes formas en que se pueden eliminar objetos y cómo StorageGRID maneja las solicitudes de eliminación puede ayudarlo a administrar objetos de manera más efectiva.

StorageGRID puede utilizar uno de dos métodos para eliminar objetos:

- Eliminación sincrónica: cuando StorageGRID recibe una solicitud de eliminación de cliente, todas las copias de objetos se eliminan inmediatamente. Después de eliminar las copias se informa al cliente que la eliminación se realizó correctamente.
- Los objetos se ponen en cola para su eliminación: cuando StorageGRID recibe una solicitud de eliminación, el objeto se pone en cola para su eliminación y se informa inmediatamente al cliente que la eliminación se realizó correctamente. Las copias de objetos se eliminan más tarde mediante el procesamiento ILM en segundo plano.

Al eliminar objetos, StorageGRID utiliza el método que optimiza el rendimiento de la eliminación, minimiza los posibles retrasos en la eliminación y libera espacio más rápidamente.

La tabla resume cuándo StorageGRID utiliza cada método.

Método para realizar la eliminación	Cuando se utiliza
Los objetos se ponen en cola para su eliminación	Cuando cualquiera de las siguientes condiciones sea verdadera: • La eliminación automática de objetos se ha activado por uno de los siguientes eventos: ◦ Se alcanza la fecha de vencimiento o el número de días en la configuración del ciclo de vida de un bucket S3. ◦ Transcurre el último período de tiempo especificado en una regla ILM. Nota: Los objetos en un bucket que tiene habilitado el Bloqueo de objetos S3 no se pueden eliminar si están bajo una retención legal o si se ha especificado una fecha de retención pero aún no se cumple. • Un cliente S3 solicita la eliminación y una o más de estas condiciones son verdaderas: ◦ Las copias no se pueden eliminar en 30 segundos porque, por ejemplo, la ubicación de un objeto no está disponible temporalmente. ◦ Las colas de eliminación en segundo plano están inactivas.
Los objetos se eliminan inmediatamente (eliminación sincrónica)	Cuando un cliente S3 realiza una solicitud de eliminación y se cumplen todas las siguientes condiciones: • Todas las copias se pueden eliminar en 30 segundos. • Las colas de eliminación en segundo plano contienen objetos para procesar.

Cuando los clientes S3 realizan solicitudes de eliminación, StorageGRID comienza agregando objetos a la cola de eliminación. Luego pasa a realizar la eliminación sincrónica. Asegurarse de que la cola de eliminación en segundo plano tenga objetos para procesar permite que StorageGRID procese las eliminaciones de manera más eficiente, especialmente para clientes de baja concurrencia, al mismo tiempo que ayuda a prevenir retrasos en la eliminación de clientes.

Tiempo necesario para eliminar objetos

La forma en que StorageGRID elimina objetos puede afectar el funcionamiento aparente del sistema:

- Cuando StorageGRID realiza una eliminación sincrónica, puede tardar hasta 30 segundos en devolver un

resultado al cliente. Esto significa que puede parecer que la eliminación ocurre más lentamente, aunque en realidad las copias se eliminan más rápido que cuando StorageGRID pone en cola los objetos para su eliminación.

- Si supervisa de cerca el rendimiento de eliminación durante una eliminación masiva, es posible que observe que la tasa de eliminación parece ser lenta después de que se haya eliminado una cierta cantidad de objetos. Este cambio se produce cuando StorageGRID pasa de poner en cola objetos para su eliminación a realizar una eliminación sincrónica. La aparente reducción en la tasa de eliminación no significa que las copias de objetos se estén eliminando más lentamente. Por el contrario, indica que, en promedio, ahora se está liberando espacio más rápidamente.

Si está eliminando una gran cantidad de objetos y su prioridad es liberar espacio rápidamente, considere usar una solicitud de cliente para eliminar objetos en lugar de eliminarlos mediante ILM u otros métodos. En general, el espacio se libera más rápidamente cuando la eliminación la realizan los clientes porque StorageGRID puede usar la eliminación sincrónica.

La cantidad de tiempo necesaria para liberar espacio después de eliminar un objeto depende de varios factores:

- Si las copias de objetos se eliminan de forma sincrónica o se ponen en cola para su eliminación más tarde (para solicitudes de eliminación del cliente).
- Otros factores, como la cantidad de objetos en la red o la disponibilidad de recursos de la red cuando las copias de objetos se ponen en cola para su eliminación (tanto para eliminaciones de cliente como para otros métodos).

Cómo se eliminan los objetos versionados de S3

Cuando el control de versiones está habilitado para un bucket S3, StorageGRID sigue el comportamiento de Amazon S3 al responder a solicitudes de eliminación, ya sea que dichas solicitudes provengan de un cliente S3, la expiración del ciclo de vida de un bucket S3 o los requisitos de la política ILM.

Cuando los objetos están versionados, las solicitudes de eliminación de objetos no eliminan la versión actual del objeto y no liberan espacio. En cambio, una solicitud de eliminación de objeto crea un marcador de eliminación de cero bytes como la versión actual del objeto, lo que hace que la versión anterior del objeto sea "no actual". Un marcador de eliminación de objeto se convierte en un marcador de eliminación de objeto vencido cuando es la versión actual y no hay versiones no actuales.

Incluso aunque el objeto no se haya eliminado, StorageGRID se comporta como si la versión actual del objeto ya no estuviera disponible. Las solicitudes a ese objeto devuelven 404 Not Found. Sin embargo, debido a que no se han eliminado los datos del objeto no actual, las solicitudes que especifican una versión no actual del objeto pueden tener éxito.

Para liberar espacio al eliminar objetos versionados o para quitar marcadores de eliminación, utilice una de las siguientes opciones:

- **Solicitud de cliente S3:** especifique el ID de la versión del objeto en la solicitud S3 DELETE `Object(DELETE /object?versionId=ID )`. Tenga en cuenta que esta solicitud solo elimina copias de objetos de la versión especificada (las otras versiones aún ocupan espacio).
- **Ciclo de vida del bucket:** utilice el `NoncurrentVersionExpiration` acción en la configuración del ciclo de vida del bucket. Cuando se alcanza la cantidad de `NoncurrentDays` especificada, StorageGRID elimina de forma permanente todas las copias de versiones de objetos no actuales. Estas versiones de objetos no se pueden recuperar.

El `NewerNoncurrentVersions` La acción en la configuración del ciclo de vida del bucket especifica la cantidad de versiones no actuales que se conservan en un bucket S3 versionado. Si hay más versiones

no actuales que `NewerNoncurrentVersions` especifica que StorageGRID elimina las versiones anteriores cuando ha transcurrido el valor `NoncurrentDays`. El `NewerNoncurrentVersions` El umbral anula las reglas del ciclo de vida proporcionadas por ILM, lo que significa que un objeto no actual con una versión dentro del `NewerNoncurrentVersions` El umbral se mantiene si ILM solicita su eliminación.

Para eliminar los marcadores de eliminación de objetos caducados, utilice el `Expiration` acción con una de las siguientes etiquetas: `ExpiredObjectDeleteMarker`, `Days`, o `Date`.

- **ILM:** "Clonar una política activa" y agregue dos reglas ILM a la nueva política:
 - Primera regla: utilice "Tiempo no actual" como tiempo de referencia para que coincida con las versiones no actuales del objeto. En "Paso 1 (Ingresar detalles) del asistente para crear una regla de ILM", seleccione **Sí** para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?"
 - Segunda regla: utiliza **Tiempo de ingesta** para que coincida con la versión actual. La regla "Hora no actual" debe aparecer en la política encima de la regla **Hora de ingestión**.

Para eliminar marcadores de eliminación de objetos vencidos, utilice una regla de **Tiempo de ingesta** para que coincida con los marcadores de eliminación actuales. Los marcadores de eliminación solo se eliminan cuando ha transcurrido un **Periodo de tiempo de Días** y el creador de eliminación actual ha expirado (no hay versiones no actuales).

- **Eliminar objetos en el depósito:** utilice el administrador de inquilinos para "eliminar todas las versiones de los objetos", incluidos los marcadores de eliminación, de un depósito.

Cuando se elimina un objeto versionado, StorageGRID crea un marcador de eliminación de cero bytes como la versión actual del objeto. Todos los objetos y marcadores de eliminación deben eliminarse antes de poder eliminar un depósito versionado.

- Los marcadores de eliminación creados en StorageGRID 11.7 o versiones anteriores solo se pueden eliminar mediante solicitudes de cliente S3, no se eliminan mediante ILM, reglas de ciclo de vida del bucket ni mediante la eliminación de objetos en operaciones de bucket.
- Los marcadores de eliminación de un depósito creado en StorageGRID 11.8 o posterior se pueden quitar mediante ILM, reglas de ciclo de vida del depósito, operaciones de eliminación de objetos en el depósito o una eliminación explícita del cliente S3.

Información relacionada

- "Utilice la API REST de S3"
- "Ejemplo 4: Reglas y políticas de ILM para objetos versionados de S3"

Crear y asignar grados de almacenamiento

Los grados de almacenamiento identifican el tipo de almacenamiento utilizado por un nodo de almacenamiento. Puede crear grados de almacenamiento si desea que las reglas ILM coloquen determinados objetos en determinados nodos de almacenamiento.

Antes de empezar

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

Acerca de esta tarea

Cuando instala StorageGRID por primera vez, el grado de almacenamiento **Predeterminado** se asigna

automáticamente a cada nodo de almacenamiento en su sistema. Según sea necesario, puede definir opcionalmente grados de almacenamiento personalizados y asignarlos a diferentes nodos de almacenamiento.

El uso de grados de almacenamiento personalizados le permite crear grupos de almacenamiento ILM que contienen solo un tipo específico de nodo de almacenamiento. Por ejemplo, es posible que desee que determinados objetos se almacenen en sus nodos de almacenamiento más rápidos, como los dispositivos de almacenamiento totalmente flash StorageGRID .



Los nodos de almacenamiento se pueden configurar durante la instalación para que contengan solo metadatos de objetos y no datos de objetos. A los nodos de almacenamiento de solo metadatos no se les puede asignar un grado de almacenamiento. Para obtener más información, consulte ["Tipos de nodos de almacenamiento"](#) .

Si el grado de almacenamiento no es una preocupación (por ejemplo, todos los nodos de almacenamiento son idénticos), puede omitir este procedimiento y usar la selección **incluye todos los grados de almacenamiento** para el grado de almacenamiento cuando ["crear grupos de almacenamiento"](#) . El uso de esta selección garantiza que el grupo de almacenamiento incluirá todos los nodos de almacenamiento del sitio, independientemente de su grado de almacenamiento.



No cree más niveles de almacenamiento de los necesarios. Por ejemplo, no cree un grado de almacenamiento para cada nodo de almacenamiento. En su lugar, asigne cada grado de almacenamiento a dos o más nodos. Los grados de almacenamiento asignados a un solo nodo pueden provocar retrasos en ILM si ese nodo deja de estar disponible.

Pasos

1. Seleccione **ILM > Grados de almacenamiento**.
2. Definir grados de almacenamiento personalizados:
 - a. Para cada grado de almacenamiento personalizado que desee agregar, seleccione ***Insertar***  para agregar una fila.
 - b. Introduzca una etiqueta descriptiva.



Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

c. Seleccione **Aplicar cambios**.

d. Opcionalmente, si necesita modificar una etiqueta guardada, seleccione **Editar*** y seleccione ***Aplicar cambios**.



No se pueden eliminar los niveles de almacenamiento.

3. Asignar nuevos grados de almacenamiento a los nodos de almacenamiento:

a. Localice el nodo de almacenamiento en la lista LDR y seleccione su ícono ***Editar*** .

b. Seleccione el grado de almacenamiento apropiado de la lista.



LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default disk	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes



Asignar un grado de almacenamiento a un nodo de almacenamiento determinado solo una vez. Un nodo de almacenamiento recuperado de una falla mantiene el grado de almacenamiento asignado previamente. No cambie esta asignación después de que se active la política ILM. Si se cambia la asignación, los datos se almacenan según el nuevo grado de almacenamiento.

- a. Seleccione **Aplicar cambios**.

Utilice grupos de almacenamiento

¿Qué es un pool de almacenamiento?

Un grupo de almacenamiento es una agrupación lógica de nodos de almacenamiento.

Cuando instala StorageGRID, se crea automáticamente un grupo de almacenamiento por sitio. Puede configurar grupos de almacenamiento adicionales según sea necesario para sus requisitos de almacenamiento.



Los nodos de almacenamiento se pueden configurar durante la instalación para contener datos de objetos y metadatos de objetos, o solo metadatos de objetos. Los nodos de almacenamiento de solo metadatos no se pueden usar en grupos de almacenamiento. Para obtener más información, consulte "[Tipos de nodos de almacenamiento](#)".

Los grupos de almacenamiento tienen dos atributos:

- **Grado de almacenamiento:** para los nodos de almacenamiento, el rendimiento relativo del almacenamiento de respaldo.
- **Sitio:** El centro de datos donde se almacenarán los objetos.

Los grupos de almacenamiento se utilizan en las reglas ILM para determinar dónde se almacenan los datos de los objetos y el tipo de almacenamiento utilizado. Cuando configura las reglas de ILM para la replicación, selecciona uno o más grupos de almacenamiento.

Pautas para la creación de grupos de almacenamiento

Configure y utilice grupos de almacenamiento para protegerse contra la pérdida de datos mediante la distribución de datos en varios sitios. Las copias replicadas y las copias con código de borrado requieren diferentes configuraciones de grupo de almacenamiento.

Ver ["Ejemplos de habilitación de la protección contra pérdida de sitios mediante codificación de replicación y borrado"](#).

Directrices para todos los grupos de almacenamiento

- Mantenga las configuraciones del grupo de almacenamiento lo más simples posible. No cree más grupos de almacenamiento de los necesarios.
- Cree grupos de almacenamiento con tantos nodos como sea posible. Cada grupo de almacenamiento debe contener dos o más nodos. Un grupo de almacenamiento con nodos insuficientes puede provocar retrasos en ILM si un nodo deja de estar disponible.
- Evite crear o utilizar grupos de almacenamiento que se superpongan (que contengan uno o más de los mismos nodos). Si los grupos de almacenamiento se superponen, es posible que se guarden más de una copia de datos de objetos en el mismo nodo.
- En general, no utilice el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) ni el sitio Todos los sitios. Estos elementos se actualizan automáticamente para incluir cualquier sitio nuevo que agregue en una expansión, lo que podría no ser el comportamiento deseado.

Directrices para los grupos de almacenamiento utilizados para copias replicadas

- Para la protección contra pérdida de sitios utilizando ["replicación"](#), especifique uno o más grupos de almacenamiento específicos del sitio en el ["Instrucciones de colocación para cada regla ILM"](#).

Durante la instalación de StorageGRID se crea automáticamente un grupo de almacenamiento para cada sitio.

El uso de un grupo de almacenamiento para cada sitio garantiza que las copias de objetos replicados se coloquen exactamente donde usted espera (por ejemplo, una copia de cada objeto en cada sitio para protección contra pérdida del sitio).

- Si agrega un sitio en una expansión, cree un nuevo grupo de almacenamiento que contenga solo el nuevo sitio. Entonces, ["actualizar las reglas de ILM"](#) para controlar qué objetos se almacenan en el nuevo sitio.
- Si la cantidad de copias es menor que la cantidad de grupos de almacenamiento, el sistema distribuye las copias para equilibrar el uso del disco entre los grupos.
- Si los grupos de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), todas las copias del objeto podrían guardarse en un solo sitio. Debe asegurarse de que los grupos de almacenamiento seleccionados no contengan los mismos nodos de almacenamiento.

Directrices para los grupos de almacenamiento utilizados para copias con código de borrado

- Para la protección contra pérdida de sitios utilizando ["codificación de borrado"](#), cree grupos de almacenamiento que consten de al menos tres sitios. Si un grupo de almacenamiento incluye solo dos sitios, no podrá utilizar ese grupo de almacenamiento para la codificación de borrado. No hay esquemas de codificación de borrado disponibles para un grupo de almacenamiento que tiene dos sitios.
- La cantidad de nodos de almacenamiento y sitios contenidos en el grupo de almacenamiento determinan qué ["esquemas de codificación de borrado"](#) están disponibles.

- Si es posible, un grupo de almacenamiento debe incluir más que la cantidad mínima de nodos de almacenamiento necesarios para el esquema de codificación de borrado que seleccione. Por ejemplo, si utiliza un esquema de codificación de borrado 6+3, debe tener al menos nueve nodos de almacenamiento. Sin embargo, se recomienda tener al menos un nodo de almacenamiento adicional por sitio.
- Distribuya los nodos de almacenamiento en los sitios de la manera más uniforme posible. Por ejemplo, para admitir un esquema de codificación de borrado 6+3, configure un grupo de almacenamiento que incluya al menos tres nodos de almacenamiento en tres sitios.
- Si tiene requisitos de alto rendimiento, no se recomienda utilizar un grupo de almacenamiento que incluya varios sitios si la latencia de red entre sitios es superior a 100 ms. A medida que aumenta la latencia, la velocidad a la que StorageGRID puede crear, colocar y recuperar fragmentos de objetos disminuye drásticamente debido a la disminución del rendimiento de la red TCP.

La disminución del rendimiento afecta las tasas máximas alcanzables de ingesta y recuperación de objetos (cuando se selecciona Equilibrado o Estricto como comportamiento de ingesta) o podría generar retrasos en la cola de ILM (cuando se selecciona Confirmación dual como comportamiento de ingesta). Ver "[Comportamiento de ingesta de reglas ILM](#)".



Si su red incluye solo un sitio, no podrá utilizar el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) ni el sitio Todos los sitios en un perfil de codificación de borrado. Este comportamiento evita que el perfil se vuelva inválido si se agrega un segundo sitio.

Habilitar la protección contra pérdida de sitios

Si su implementación de StorageGRID incluye más de un sitio, puede usar codificación de replicación y borrado con grupos de almacenamiento configurados adecuadamente para habilitar la protección contra pérdida de sitios.

La codificación de replicación y borrado requiere diferentes configuraciones de grupo de almacenamiento:

- Para utilizar la replicación para la protección contra pérdida del sitio, utilice los grupos de almacenamiento específicos del sitio que se crean automáticamente durante la instalación de StorageGRID. Luego crea reglas ILM con "[instrucciones de colocación](#)" que especifican múltiples grupos de almacenamiento para que se coloque una copia de cada objeto en cada sitio.
- Para utilizar la codificación de borrado para la protección contra pérdida del sitio, "[crear grupos de almacenamiento que consten de varios sitios](#)". Luego, cree reglas ILM que utilicen un grupo de almacenamiento compuesto por varios sitios y cualquier esquema de codificación de borrado disponible.



Al configurar su implementación de StorageGRID para la protección contra pérdida de sitios, también debe tener en cuenta los efectos de "[opciones de ingesta](#)" y "[consistencia](#)".

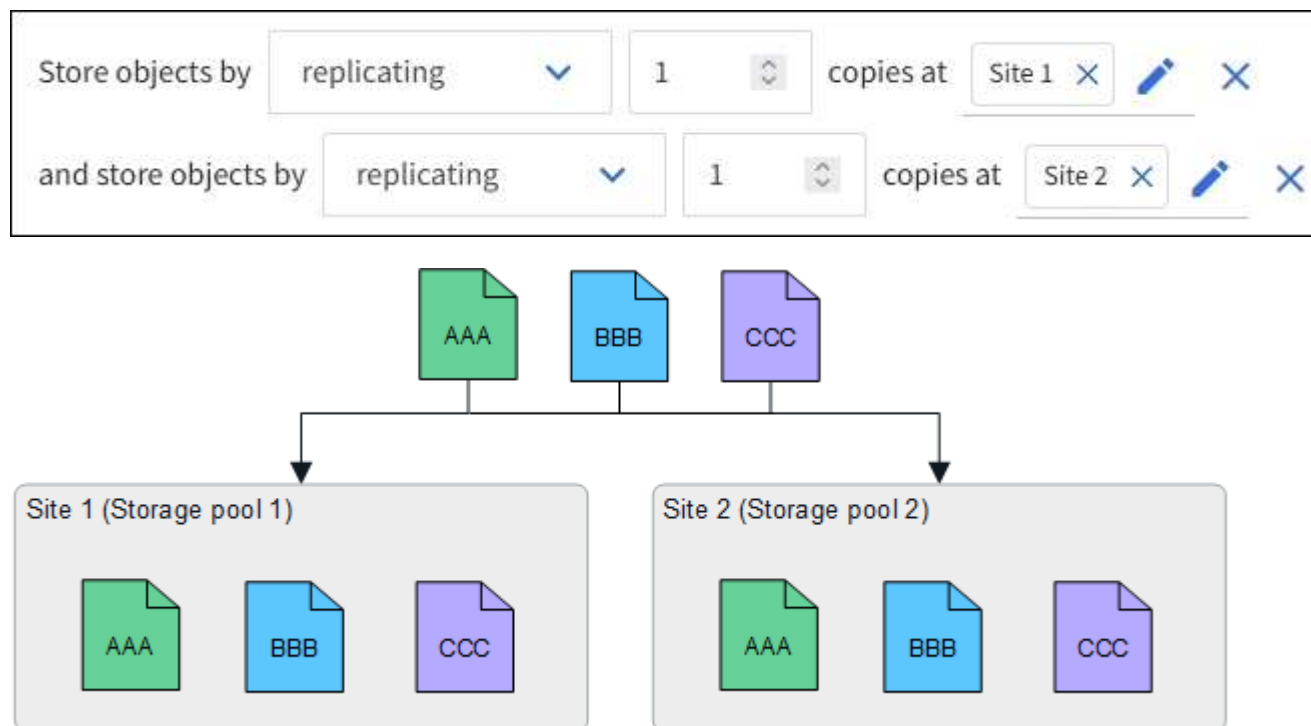
Ejemplo de replicación

De forma predeterminada, se crea un grupo de almacenamiento para cada sitio durante la instalación de StorageGRID. Tener grupos de almacenamiento que constan de un solo sitio le permite configurar reglas ILM que utilizan la replicación para la protección contra pérdida del sitio. En este ejemplo:

- El grupo de almacenamiento 1 contiene el Sitio 1
- El grupo de almacenamiento 2 contiene el Sitio 2
- La regla ILM contiene dos colocaciones:

- Almacenar objetos replicando 1 copia en el Sitio 1
- Almacenar objetos replicando 1 copia en el Sitio 2

Ubicación de las reglas de ILM:



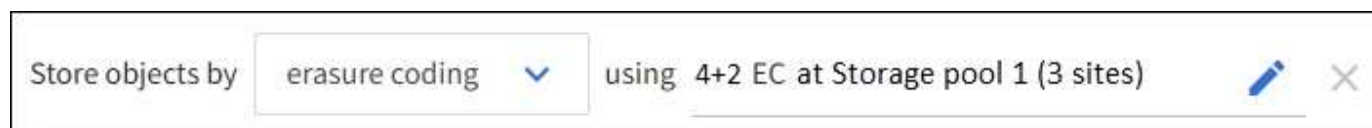
Si se pierde un sitio, hay copias de los objetos disponibles en el otro sitio.

Ejemplo de codificación de borrado

Tener grupos de almacenamiento que constan de más de un sitio por grupo de almacenamiento le permite configurar reglas ILM que utilizan codificación de borrado para la protección contra pérdida de sitios. En este ejemplo:

- El grupo de almacenamiento 1 contiene los sitios 1 a 3
- La regla ILM contiene una ubicación: almacenar objetos mediante codificación de borrado utilizando un esquema EC 4+2 en el grupo de almacenamiento 1, que contiene tres sitios

Ubicación de las reglas de ILM:



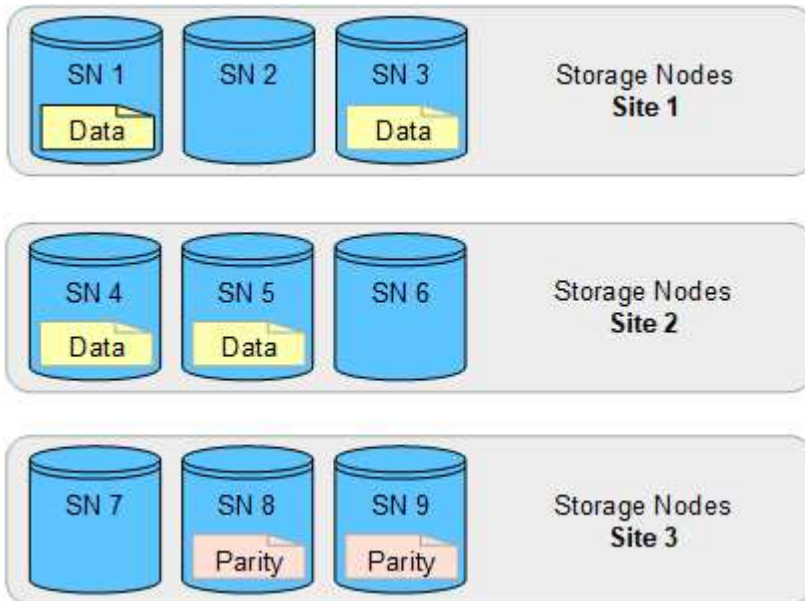
En este ejemplo:

- La regla ILM utiliza un esquema de codificación de borrado 4+2.
- Cada objeto se divide en cuatro fragmentos de datos iguales y se calculan dos fragmentos de paridad a partir de los datos del objeto.
- Cada uno de los seis fragmentos se almacena en un nodo diferente en tres sitios de centros de datos para brindar protección de datos ante fallas de nodos o pérdidas de sitios.

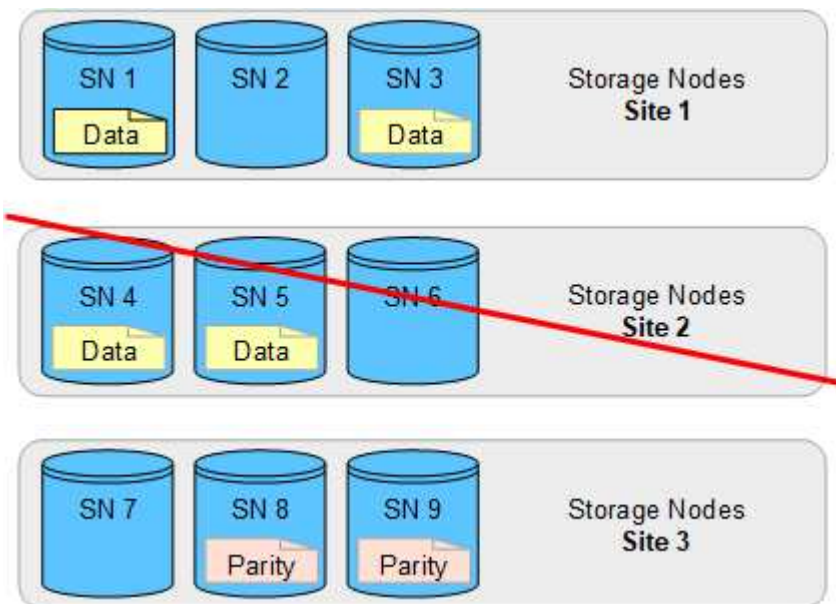


Se permite la codificación de borrado en grupos de almacenamiento que contengan cualquier cantidad de sitios *excepto* dos sitios.

Regla ILM que utiliza el esquema de codificación de borrado 4+2:



Si se pierde un sitio, aún se pueden recuperar los datos:



Crear un grupo de almacenamiento

Crea grupos de almacenamiento para determinar dónde el sistema StorageGRID almacena los datos de los objetos y el tipo de almacenamiento utilizado. Cada grupo de almacenamiento incluye uno o más sitios y uno o más grados de almacenamiento.



Cuando instala StorageGRID 11.9 en una nueva red, se crean automáticamente grupos de almacenamiento para cada sitio. Sin embargo, si instaló inicialmente StorageGRID 11.6 o una versión anterior, los grupos de almacenamiento no se crean automáticamente para cada sitio.

Si desea crear grupos de almacenamiento en la nube para almacenar datos de objetos fuera de su sistema StorageGRID , consulte la ["Información sobre el uso de grupos de almacenamiento en la nube"](#) .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Ha revisado las pautas para crear grupos de almacenamiento.

Acerca de esta tarea

Los grupos de almacenamiento determinan dónde se almacenan los datos de los objetos. La cantidad de grupos de almacenamiento que necesita depende de la cantidad de sitios en su red y de los tipos de copias que desea: replicadas o con código de borrado.

- Para la replicación y la codificación de borrado de un solo sitio, cree un grupo de almacenamiento para cada sitio. Por ejemplo, si desea almacenar copias de objetos replicados en tres sitios, cree tres grupos de almacenamiento.
- Para la codificación de borrado en tres o más sitios, cree un grupo de almacenamiento que incluya una entrada para cada sitio. Por ejemplo, si desea borrar objetos de código en tres sitios, cree un grupo de almacenamiento.



No incluya el sitio Todos los sitios en un grupo de almacenamiento que se utilizará en un perfil de codificación de borrado. En su lugar, agregue una entrada separada al grupo de almacenamiento para cada sitio que almacenará datos codificados con borrado. Ver [este paso](#) por ejemplo.

- Si tiene más de un grado de almacenamiento, no cree un grupo de almacenamiento que incluya diferentes grados de almacenamiento en un solo sitio. Ver el ["Pautas para la creación de grupos de almacenamiento"](#) .

Pasos

1. Seleccione **ILM > Grupos de almacenamiento**.

La pestaña Grupos de almacenamiento enumera todos los grupos de almacenamiento definidos.



Para las nuevas instalaciones de StorageGRID 11.6 o anteriores, el grupo de almacenamiento Todos los nodos de almacenamiento se actualiza automáticamente cada vez que agrega nuevos sitios de centros de datos. No utilice este grupo en las reglas de ILM.

2. Para crear un nuevo grupo de almacenamiento, seleccione **Crear**.
3. Introduzca un nombre único para el grupo de almacenamiento. Utilice un nombre que sea fácil de identificar cuando configure perfiles de codificación de borrado y reglas ILM.
4. En la lista desplegable **Sitio**, seleccione un sitio para este grupo de almacenamiento.

Cuando selecciona un sitio, la cantidad de nodos de almacenamiento en la tabla se actualiza automáticamente.

En general, no utilice el sitio Todos los sitios en ningún grupo de almacenamiento. Las reglas ILM que utilizan un grupo de almacenamiento de todos los sitios colocan los objetos en cualquier sitio disponible, lo que le brinda menos control sobre la ubicación de los objetos. Además, un grupo de almacenamiento de todos los sitios utiliza los nodos de almacenamiento en un nuevo sitio de inmediato, lo que podría no ser el

comportamiento esperado.

5. En la lista desplegable **Grado de almacenamiento**, seleccione el tipo de almacenamiento que se utilizará si una regla ILM usa este grupo de almacenamiento.

El grado de almacenamiento, *incluye todos los grados de almacenamiento*, incluye todos los nodos de almacenamiento en el sitio seleccionado. Si creó grados de almacenamiento adicionales para los nodos de almacenamiento en su cuadrícula, aparecerán en el menú desplegable.

6. Si desea utilizar el grupo de almacenamiento en un perfil de codificación de borrado de varios sitios, seleccione **Agregar más nodos** para agregar una entrada para cada sitio al grupo de almacenamiento.



Se le advertirá si agrega más de una entrada con diferentes grados de almacenamiento para un sitio.

Para eliminar una entrada, seleccione el icono de eliminar

7. Cuando esté satisfecho con sus selecciones, seleccione **Guardar**.

El nuevo grupo de almacenamiento se agrega a la lista.

Ver detalles del grupo de almacenamiento

Puede ver los detalles de un grupo de almacenamiento para determinar dónde se utiliza y ver qué nodos y grados de almacenamiento están incluidos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).

Pasos

1. Seleccione **ILM > Grupos de almacenamiento**.

La tabla de grupos de almacenamiento incluye la siguiente información para cada grupo de almacenamiento que incluye nodos de almacenamiento:

- **Nombre:** el nombre para mostrar único del grupo de almacenamiento.
- **Recuento de nodos:** la cantidad de nodos en el grupo de almacenamiento.
- **Uso de almacenamiento:** el porcentaje del espacio utilizable total que se ha utilizado para datos de objetos en este nodo. Este valor no incluye metadatos del objeto.
- **Capacidad total:** el tamaño del grupo de almacenamiento, que equivale a la cantidad total de espacio utilizable para datos de objetos para todos los nodos del grupo de almacenamiento.
- **Uso de ILM:** cómo se utiliza actualmente el grupo de almacenamiento. Es posible que un grupo de almacenamiento no se utilice o que se utilice en una o más reglas ILM, perfiles de codificación de borrado o ambos.

2. Para ver los detalles de un grupo de almacenamiento específico, seleccione su nombre.

Aparece la página de detalles del grupo de almacenamiento.

3. Consulte la pestaña **Nodos** para obtener información sobre los nodos de almacenamiento incluidos en el grupo de almacenamiento.

La tabla incluye la siguiente información para cada nodo:

- Nombre del nodo
- Nombre del sitio
- Grado de almacenamiento
- Uso de almacenamiento: el porcentaje del espacio total utilizable para los datos de objetos que se ha utilizado para el nodo de almacenamiento.



El mismo valor de uso de almacenamiento (%) también se muestra en el gráfico Almacenamiento utilizado - Datos de objeto para cada nodo de almacenamiento (seleccione **NODOS** > **Nodo de almacenamiento** > **Almacenamiento**).

4. Vea la pestaña **Uso de ILM** para determinar si el grupo de almacenamiento se está utilizando actualmente en alguna regla de ILM o perfil de codificación de borrado.
5. Opcionalmente, vaya a la **página de reglas de ILM** para conocer y administrar las reglas que utilizan el grupo de almacenamiento.

Ver el "[Instrucciones para trabajar con reglas ILM](#)".

Editar grupo de almacenamiento

Puede editar un grupo de almacenamiento para cambiar su nombre o actualizar sitios y grados de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes "[permisos de acceso específicos](#)".
- Usted ha revisado el "[Pautas para la creación de grupos de almacenamiento](#)".
- Si planea editar un grupo de almacenamiento que se utiliza en una regla de la política ILM activa, debe considerar cómo sus cambios afectarán la ubicación de los datos de los objetos.

Acerca de esta tarea

Si está agregando un nuevo sitio o grado de almacenamiento a un grupo de almacenamiento que se utiliza en la política ILM activa, tenga en cuenta que los nodos de almacenamiento en el nuevo sitio o grado de almacenamiento no se utilizarán automáticamente. Para forzar a StorageGRID a usar un nuevo sitio o grado de almacenamiento, debe activar una nueva política ILM después de guardar el grupo de almacenamiento editado.

Pasos

1. Seleccione **ILM** > **Grupos de almacenamiento**.
2. Seleccione la casilla de verificación del grupo de almacenamiento que desea editar.

No se puede editar el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores).

3. Seleccione **Editar**.
4. Según sea necesario, cambie el nombre del grupo de almacenamiento.
5. Según sea necesario, seleccione otros sitios y grados de almacenamiento.

No se le permite cambiar el sitio o el grado de almacenamiento si el grupo de almacenamiento se utiliza en un perfil de codificación de borrado y el cambio provocaría que el esquema de codificación de borrado se vuelva inválido. Por ejemplo, si un grupo de almacenamiento utilizado en un perfil de codificación de borrado actualmente incluye un grado de almacenamiento con un solo sitio, no podrá utilizar un grado de almacenamiento con dos sitios porque el cambio haría que el esquema de codificación de borrado no sea válido.



Agregar o eliminar sitios de un grupo de almacenamiento existente no moverá ningún dato codificado de borrado existente. Si desea mover los datos existentes del sitio, debe crear un nuevo grupo de almacenamiento y un perfil EC para volver a codificar los datos.

6. Seleccione **Guardar**.

Después de terminar

Si agregó un nuevo sitio o grado de almacenamiento a un grupo de almacenamiento utilizado en la política ILM activa, active una nueva política ILM para forzar a StorageGRID a usar el nuevo sitio o grado de almacenamiento. Por ejemplo, clone su política ILM existente y luego active el clon. Ver ["Trabajar con las reglas y políticas de ILM"](#).

Eliminar un grupo de almacenamiento

Puedes eliminar un grupo de almacenamiento que no esté en uso.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["permisos de acceso necesarios"](#).

Pasos

1. Seleccione **ILM > Grupos de almacenamiento**.
2. Mire la columna de uso de ILM en la tabla para determinar si puede eliminar el grupo de almacenamiento.

No se puede eliminar un grupo de almacenamiento si se está utilizando en una regla ILM o en un perfil de codificación de borrado. Según sea necesario, seleccione **nombre del grupo de almacenamiento > uso de ILM** para determinar dónde se utiliza el grupo de almacenamiento.

3. Si el grupo de almacenamiento que desea eliminar no está en uso, seleccione la casilla de verificación.
4. Seleccione **Eliminar**.
5. Seleccione **Aceptar**.

Utilice grupos de almacenamiento en la nube

¿Qué es un pool de almacenamiento en la nube?

Un grupo de almacenamiento en la nube le permite usar ILM para mover datos de objetos fuera de su sistema StorageGRID. Por ejemplo, es posible que desee mover objetos a los que se accede con poca frecuencia a un almacenamiento en la nube de menor costo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso de archivo en el almacenamiento de blobs de Microsoft Azure. O bien, es posible que desee mantener una copia de seguridad en la nube de los objetos

StorageGRID para mejorar la recuperación ante desastres.

Desde una perspectiva ILM, un grupo de almacenamiento en la nube es similar a un grupo de almacenamiento. Para almacenar objetos en cualquiera de las ubicaciones, seleccione el grupo al crear las instrucciones de ubicación para una regla ILM. Sin embargo, mientras que los grupos de almacenamiento constan de nodos de almacenamiento dentro del sistema StorageGRID, un grupo de almacenamiento en la nube consta de un depósito externo (S3) o contenedor (almacenamiento de blobs de Azure).

La tabla compara los grupos de almacenamiento con los grupos de almacenamiento en la nube y muestra las similitudes y diferencias de alto nivel.

	Pool de almacenamiento	Grupo de almacenamiento en la nube
¿Cómo se crea?	Usando la opción ILM > Grupos de almacenamiento en el Administrador de Grid.	Usando la opción ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube en Grid Manager. Debe configurar el contenedor o depósito externo antes de poder crear el grupo de almacenamiento en la nube.
¿Cuántos pools puedes crear?	Ilimitado.	Hasta 10.
¿Dónde se almacenan los objetos?	En uno o más nodos de almacenamiento dentro de StorageGRID.	En un bucket de Amazon S3, un contenedor de almacenamiento de blobs de Azure o un Google Cloud externo al sistema StorageGRID. Si el grupo de almacenamiento en la nube es un bucket de Amazon S3: • Opcionalmente, puede configurar un ciclo de vida de depósito para trasladar objetos a un almacenamiento a largo plazo y de bajo costo, como Amazon S3 Glacier o S3 Glacier Deep Archive. El sistema de almacenamiento externo debe ser compatible con la clase de almacenamiento Glacier y la API S3 RestoreObject. • Puede crear grupos de almacenamiento en la nube para usar con AWS Commercial Cloud Services (C2S), que admite la región secreta de AWS. Si el grupo de almacenamiento en la nube es un contenedor de almacenamiento de blobs de Azure, StorageGRID traslada el objeto al nivel de archivo. Nota: En general, no configure la administración del ciclo de vida del almacenamiento de blobs de Azure para el contenedor utilizado para un grupo de almacenamiento en la nube. Las operaciones de restauración de objetos en el grupo de almacenamiento en la nube pueden verse afectadas por el ciclo de vida configurado.

	Pool de almacenamiento	Grupo de almacenamiento en la nube
¿Qué controla la ubicación de los objetos?	Una regla ILM en las políticas ILM activas.	Una regla ILM en las políticas ILM activas.
¿Qué método de protección de datos se utiliza?	Codificación de replicación o borrado.	Replicación.
¿Cuántas copias de cada objeto están permitidas?	Múltiple.	Una copia en el grupo de almacenamiento en la nube y, opcionalmente, una o más copias en StorageGRID. Nota: No es posible almacenar un objeto en más de un grupo de almacenamiento en la nube al mismo tiempo.
¿Cuales son las ventajas?	Los objetos son accesibles rápidamente en cualquier momento.	Almacenamiento de bajo coste. Nota: Los datos de FabricPool no se pueden agrupar en grupos de almacenamiento en la nube.

Ciclo de vida de un objeto de grupo de almacenamiento en la nube

Antes de implementar grupos de almacenamiento en la nube, revise el ciclo de vida de los objetos que se almacenan en cada tipo de grupo de almacenamiento en la nube.

S3: Ciclo de vida de un objeto de grupo de almacenamiento en la nube

Los pasos describen las etapas del ciclo de vida de un objeto almacenado en un grupo de almacenamiento en la nube S3.



"Glacier" se refiere tanto a la clase de almacenamiento Glacier como a la clase de almacenamiento Glacier Deep Archive, con una excepción: la clase de almacenamiento Glacier Deep Archive no admite el nivel de restauración acelerada. Solo se admite la recuperación masiva o estándar.



Google Cloud Platform (GCP) admite la recuperación de objetos del almacenamiento a largo plazo sin necesidad de una operación de restauración POST.

1. Objeto almacenado en StorageGRID

Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. Objeto movido al pool de almacenamiento en la nube S3

- Cuando el objeto coincide con una regla ILM que utiliza un grupo de almacenamiento en la nube S3 como su ubicación, StorageGRID mueve el objeto al depósito S3 externo especificado por el grupo de almacenamiento en la nube.

- Cuando el objeto se ha movido al grupo de almacenamiento en la nube S3, la aplicación cliente puede recuperarlo mediante una solicitud GetObject de S3 desde StorageGRID, a menos que el objeto se haya transferido al almacenamiento Glacier.

3. Objeto en transición a Glacier (estado no recuperable)

- Opcionalmente, el objeto puede trasladarse al almacenamiento de Glacier. Por ejemplo, el depósito S3 externo podría usar la configuración del ciclo de vida para trasladar un objeto al almacenamiento de Glacier inmediatamente o después de una cierta cantidad de días.



Si desea realizar la transición de objetos, debe crear una configuración de ciclo de vida para el depósito S3 externo y debe utilizar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y admita la API S3 RestoreObject.

- Durante la transición, la aplicación cliente puede utilizar una solicitud S3 HeadObject para monitorear el estado del objeto.

4. Objeto restaurado del almacenamiento del glaciar

Si un objeto se ha transferido al almacenamiento de Glacier, la aplicación cliente puede emitir una solicitud S3 RestoreObject para restaurar una copia recuperable al grupo de almacenamiento en la nube S3. La solicitud especifica cuántos días debe estar disponible la copia en el grupo de almacenamiento en la nube y el nivel de acceso a datos que se utilizará para la operación de restauración (acelerada, estándar o masiva). Cuando se alcanza la fecha de vencimiento de la copia recuperable, la copia vuelve automáticamente a un estado no recuperable.



Si también existen una o más copias del objeto en los nodos de almacenamiento dentro de StorageGRID, no es necesario restaurar el objeto desde Glacier emitiendo una solicitud RestoreObject. En cambio, la copia local se puede recuperar directamente, mediante una solicitud GetObject.

5. Objeto recuperado

Una vez que se ha restaurado un objeto, la aplicación cliente puede emitir una solicitud GetObject para recuperar el objeto restaurado.

Azure: ciclo de vida de un objeto de grupo de almacenamiento en la nube

Los pasos describen las etapas del ciclo de vida de un objeto almacenado en un grupo de almacenamiento en la nube de Azure.

1. Objeto almacenado en StorageGRID

Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. Objeto movido al grupo de almacenamiento en la nube de Azure

Cuando el objeto coincide con una regla ILM que usa un grupo de almacenamiento en la nube de Azure como su ubicación, StorageGRID mueve el objeto al contenedor de almacenamiento de blobs de Azure externo especificado por el grupo de almacenamiento en la nube.

3. Objeto en transición al nivel de archivo (estado no recuperable)

Inmediatamente después de mover el objeto al grupo de almacenamiento en la nube de Azure, StorageGRID transfiere automáticamente el objeto al nivel de archivo de almacenamiento de blobs de

Azure.

4. Objeto restaurado desde el nivel de archivo

Si un objeto se ha trasladado al nivel de archivo, la aplicación cliente puede emitir una solicitud S3 RestoreObject para restaurar una copia recuperable en el grupo de almacenamiento en la nube de Azure.

Cuando StorageGRID recibe RestoreObject, transfiere temporalmente el objeto al nivel Esporádico de almacenamiento de blobs de Azure. Tan pronto como se alcanza la fecha de vencimiento en la solicitud RestoreObject, StorageGRID transfiere el objeto nuevamente al nivel de archivo.



Si una o más copias del objeto también existen en los nodos de almacenamiento dentro de StorageGRID, no es necesario restaurar el objeto desde el nivel de acceso de archivo emitiendo una solicitud RestoreObject. En cambio, la copia local se puede recuperar directamente, mediante una solicitud GetObject.

5. Objeto recuperado

Una vez que se ha restaurado un objeto en el grupo de almacenamiento en la nube de Azure, la aplicación cliente puede emitir una solicitud GetObject para recuperar el objeto restaurado.

Información relacionada

["Utilice la API REST de S3"](#)

Cuándo utilizar grupos de almacenamiento en la nube

Al utilizar grupos de almacenamiento en la nube, puede realizar copias de seguridad o agrupar datos en niveles en una ubicación externa. Además, puedes realizar copias de seguridad o agrupar datos en más de una nube.

Realizar una copia de seguridad de los datos de StorageGRID en una ubicación externa

Puede utilizar un grupo de almacenamiento en la nube para realizar copias de seguridad de objetos StorageGRID en una ubicación externa.

Si las copias en StorageGRID son inaccesibles, los datos de los objetos en el grupo de almacenamiento en la nube se pueden usar para atender las solicitudes de los clientes. Sin embargo, es posible que necesite emitir una solicitud S3 RestoreObject para acceder a la copia del objeto de respaldo en el grupo de almacenamiento en la nube.

Los datos de objetos en un grupo de almacenamiento en la nube también se pueden usar para recuperar datos perdidos de StorageGRID debido a una falla del volumen de almacenamiento o del nodo de almacenamiento. Si la única copia restante de un objeto está en un grupo de almacenamiento en la nube, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

Para implementar una solución de respaldo:

1. Crear un único grupo de almacenamiento en la nube.
2. Configure una regla ILM que almacene simultáneamente copias de objetos en nodos de almacenamiento (como copias replicadas o codificadas por borrado) y una única copia de objeto en el grupo de almacenamiento en la nube.

3. Añade la regla a tu política ILM. Luego, simule y active la política.

Datos de niveles desde StorageGRID a una ubicación externa

Puede utilizar un grupo de almacenamiento en la nube para almacenar objetos fuera del sistema StorageGRID . Por ejemplo, supongamos que tiene una gran cantidad de objetos que necesita conservar, pero espera acceder a ellos en raras ocasiones, o nunca. Puede utilizar un grupo de almacenamiento en la nube para organizar los objetos en un almacenamiento de menor costo y liberar espacio en StorageGRID.

Para implementar una solución de niveles:

1. Crear un único grupo de almacenamiento en la nube.
2. Configure una regla ILM que mueva objetos rara vez utilizados desde los nodos de almacenamiento al grupo de almacenamiento en la nube.
3. Añade la regla a tu política ILM. Luego, simule y active la política.

Mantener múltiples puntos finales en la nube

Puede configurar varios puntos finales de Cloud Storage Pool si desea organizar en niveles o realizar copias de seguridad de datos de objetos en más de una nube. Los filtros en sus reglas ILM le permiten especificar qué objetos se almacenan en cada grupo de almacenamiento en la nube. Por ejemplo, es posible que desee almacenar objetos de algunos inquilinos o buckets en Amazon S3 Glacier y objetos de otros inquilinos o buckets en Azure Blob Storage. O bien, es posible que desee mover datos entre Amazon S3 Glacier y Azure Blob Storage.



Al utilizar varios puntos finales de un grupo de almacenamiento en la nube, tenga en cuenta que un objeto solo se puede almacenar en un grupo de almacenamiento en la nube a la vez.

Para implementar múltiples puntos finales en la nube:

1. Crea hasta 10 grupos de almacenamiento en la nube.
2. Configure las reglas de ILM para almacenar los datos de objetos adecuados en el momento adecuado en cada grupo de almacenamiento en la nube. Por ejemplo, almacene objetos del depósito A en el grupo de almacenamiento en la nube A y almacene objetos del depósito B en el grupo de almacenamiento en la nube B. O bien, almacene objetos en el grupo de almacenamiento en la nube A durante un período de tiempo y luego muévalos al grupo de almacenamiento en la nube B.
3. Añade las reglas a tu política de ILM. Luego, simule y active la política.

Consideraciones para los grupos de almacenamiento en la nube

Si planea utilizar un grupo de almacenamiento en la nube para mover objetos fuera del sistema StorageGRID , debe revisar las consideraciones para configurar y usar grupos de almacenamiento en la nube.

Consideraciones generales

- En general, el almacenamiento de archivo en la nube, como Amazon S3 Glacier o Azure Blob Storage, es un lugar económico para almacenar datos de objetos. Sin embargo, los costos de recuperar datos del almacenamiento de archivos en la nube son relativamente altos. Para lograr el costo general más bajo, debe considerar cuándo y con qué frecuencia accederá a los objetos en el grupo de almacenamiento en la nube. Se recomienda utilizar un grupo de almacenamiento en la nube solo para contenido al que se espera acceder con poca frecuencia.

- No se admite el uso de grupos de almacenamiento en la nube con FabricPool debido a la latencia adicional para recuperar un objeto del destino del grupo de almacenamiento en la nube.
- Los objetos que tienen habilitado el bloqueo de objetos S3 no se pueden colocar en grupos de almacenamiento en la nube.
- Si el depósito S3 de destino de un grupo de almacenamiento en la nube tiene habilitado el bloqueo de objetos S3, el intento de configurar la replicación del depósito (PutBucketReplication) fallará con un error AccessDenied.
- Las siguientes combinaciones de plataforma, autenticación y protocolo con bloqueo de objetos S3 no son compatibles con los grupos de almacenamiento en la nube:
 - **Plataformas:** Google Cloud Platform y Azure
 - **Tipos de autenticación:** Roles de IAM en cualquier lugar y acceso anónimo
 - **Protocolo:** HTTP

Consideraciones sobre los puertos utilizados para los grupos de almacenamiento en la nube

Para garantizar que las reglas ILM puedan mover objetos hacia y desde el grupo de almacenamiento en la nube especificado, debe configurar la red o las redes que contienen los nodos de almacenamiento de su sistema. Debe asegurarse de que los siguientes puertos puedan comunicarse con el grupo de almacenamiento en la nube.

De forma predeterminada, los grupos de almacenamiento en la nube utilizan los siguientes puertos:

- **80:** Para URI de punto final que comienzan con http
- **443:** Para URI de puntos finales que comienzan con https

Puede especificar un puerto diferente al crear o editar un grupo de almacenamiento en la nube.

Si utiliza un servidor proxy no transparente, también debe ["configurar un proxy de almacenamiento"](#) para permitir que se envíen mensajes a puntos finales externos, como un punto final en Internet.

Consideraciones sobre los costos

El acceso al almacenamiento en la nube mediante un Cloud Storage Pool requiere conectividad de red a la nube. Debe considerar el costo de la infraestructura de red que utilizará para acceder a la nube y aprovisionarla adecuadamente, en función de la cantidad de datos que espera mover entre StorageGRID y la nube mediante el grupo de almacenamiento en la nube.

Cuando StorageGRID se conecta al punto final del grupo de almacenamiento en la nube externo, emite varias solicitudes para monitorear la conectividad y garantizar que pueda realizar las operaciones necesarias. Si bien estas solicitudes implicarán algunos costos adicionales, el costo de monitorear un grupo de almacenamiento en la nube debería ser solo una pequeña fracción del costo total de almacenar objetos en S3 o Azure.

Es posible que se produzcan costos más significativos si necesita mover objetos desde un punto final de un grupo de almacenamiento en la nube externo a StorageGRID. Los objetos se pueden mover nuevamente a StorageGRID en cualquiera de estos casos:

- La única copia del objeto está en un grupo de almacenamiento en la nube y usted decide almacenar el objeto en StorageGRID. En este caso, reconfigura tus reglas y políticas de ILM. Cuando se produce la evaluación de ILM, StorageGRID emite varias solicitudes para recuperar el objeto del grupo de almacenamiento en la nube. Luego, StorageGRID crea localmente la cantidad especificada de copias replicadas o codificadas por borrado. Una vez que el objeto se mueve nuevamente a StorageGRID, se elimina la copia en el grupo de almacenamiento en la nube.

- Los objetos se pierden debido a una falla del nodo de almacenamiento. Si la única copia restante de un objeto está en un grupo de almacenamiento en la nube, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.



Cuando los objetos se mueven nuevamente a StorageGRID desde un grupo de almacenamiento en la nube, StorageGRID emite múltiples solicitudes al punto final del grupo de almacenamiento en la nube para cada objeto. Antes de mover grandes cantidades de objetos, comuníquese con el soporte técnico para obtener ayuda para estimar el tiempo y los costos asociados.

S3: Permisos necesarios para el depósito del grupo de almacenamiento en la nube

Las políticas para el depósito S3 externo utilizado para un grupo de almacenamiento en la nube deben otorgarle a StorageGRID permiso para mover un objeto al depósito, obtener el estado de un objeto, restaurar un objeto desde el almacenamiento de Glacier cuando sea necesario, etc. Idealmente, StorageGRID debería tener acceso de control total al depósito.(s3: *); sin embargo, si esto no es posible, la política del bucket debe otorgar los siguientes permisos S3 a StorageGRID:

- s3:AbortMultipartUpload
- s3:DeleteObject
- s3:GetObject
- s3:ListBucket
- s3:ListBucketMultipartUploads
- s3:ListMultipartUploadParts
- s3:PutObject
- s3:RestoreObject

S3: Consideraciones para el ciclo de vida del depósito externo

El movimiento de objetos entre StorageGRID y el depósito S3 externo especificado en el grupo de almacenamiento en la nube está controlado por las reglas de ILM y las políticas de ILM activas en StorageGRID. Por el contrario, la transición de objetos del depósito S3 externo especificado en el grupo de almacenamiento en la nube a Amazon S3 Glacier o S3 Glacier Deep Archive (o a una solución de almacenamiento que implementa la clase de almacenamiento Glacier) está controlada por la configuración del ciclo de vida de ese depósito.

Si desea realizar la transición de objetos desde el grupo de almacenamiento en la nube, debe crear la configuración de ciclo de vida adecuada en el depósito S3 externo y debe utilizar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y admita la API S3 RestoreObject.

Por ejemplo, supongamos que desea que todos los objetos que se mueven desde StorageGRID al grupo de almacenamiento en la nube se transfieran al almacenamiento de Amazon S3 Glacier de inmediato. Debe crear una configuración de ciclo de vida en el depósito S3 externo que especifique una única acción (**Transición**) de la siguiente manera:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Esta regla trasladaría todos los objetos de bucket a Amazon S3 Glacier el día en que se crearon (es decir, el día en que se trasladaron de StorageGRID al Cloud Storage Pool).



Al configurar el ciclo de vida del depósito externo, nunca utilice acciones **Expiración** para definir cuándo expiran los objetos. Las acciones de expiración hacen que el sistema de almacenamiento externo elimine los objetos expirados. Si posteriormente intenta acceder a un objeto caducado desde StorageGRID, no se encontrará el objeto eliminado.

Si desea transferir objetos del grupo de almacenamiento en la nube a S3 Glacier Deep Archive (en lugar de a Amazon S3 Glacier), especifique `<StorageClass>DEEP_ARCHIVE</StorageClass>` en el ciclo de vida del bucket. Sin embargo, tenga en cuenta que no puede utilizar el Expedited Nivel para restaurar objetos del Archivo S3 Glacier Deep.

Azure: Consideraciones para el nivel de acceso

Al configurar una cuenta de almacenamiento de Azure, puede establecer el nivel de acceso predeterminado en Activo o Esporádico. Al crear una cuenta de almacenamiento para usarla con un grupo de almacenamiento en la nube, debe utilizar el nivel Activo como nivel predeterminado. Si bien StorageGRID establece inmediatamente el nivel en Archivo cuando mueve objetos al grupo de almacenamiento en la nube, el uso de una configuración predeterminada de Activo garantiza que no se le cobrará una tarifa de eliminación anticipada por los objetos eliminados del nivel Fresco antes del mínimo de 30 días.

Azure: No se admite la gestión del ciclo de vida

No utilice la administración del ciclo de vida del almacenamiento de blobs de Azure para el contenedor utilizado con un grupo de almacenamiento en la nube. Las operaciones del ciclo de vida podrían interferir con las operaciones del grupo de almacenamiento en la nube.

Información relacionada

["Crear un grupo de almacenamiento en la nube"](#)

Comparar los grupos de almacenamiento en la nube y la replicación de CloudMirror

A medida que comience a utilizar los grupos de almacenamiento en la nube, puede resultar útil comprender las similitudes y diferencias entre los grupos de almacenamiento

en la nube y el servicio de replicación StorageGRID CloudMirror.

	Grupo de almacenamiento en la nube	Servicio de replicación CloudMirror
¿Cuál es el propósito principal?	Actúa como un objetivo de archivo. La copia del objeto en el grupo de almacenamiento en la nube puede ser la única copia del objeto o puede ser una copia adicional. Es decir, en lugar de mantener dos copias en el sitio, puede mantener una copia dentro de StorageGRID y enviar una copia al grupo de almacenamiento en la nube.	Permite que un inquilino replique automáticamente objetos desde un depósito en StorageGRID (origen) a un depósito S3 externo (destino). Crea una copia independiente de un objeto en una infraestructura S3 independiente.
¿Cómo está configurado?	Se define de la misma manera que los grupos de almacenamiento, utilizando Grid Manager o la API de administración de Grid. Se puede seleccionar como ubicación de colocación en una regla ILM. Mientras que un grupo de almacenamiento consta de un grupo de nodos de almacenamiento, un grupo de almacenamiento en la nube se define mediante un punto final remoto de S3 o Azure (dirección IP, credenciales, etc.).	Un usuario inquilino "configura la replicación de CloudMirror" definiendo un punto final de CloudMirror (dirección IP, credenciales, etc.) mediante el Administrador de inquilinos o la API S3. Una vez configurado el punto final de CloudMirror, cualquier depósito propiedad de esa cuenta de inquilino se puede configurar para apuntar al punto final de CloudMirror.
¿Quién es responsable de configurarlo?	Por lo general, un administrador de red	Normalmente, un usuario inquilino
¿Cual es el destino?	• Cualquier infraestructura S3 compatible (incluido Amazon S3) • Nivel de archivo de blobs de Azure • Plataforma de Google Cloud (GCP)	• Cualquier infraestructura S3 compatible (incluido Amazon S3) • Plataforma de Google Cloud (GCP)
¿Qué hace que los objetos se muevan al destino?	Una o más reglas ILM en las políticas ILM activas. Las reglas de ILM definen qué objetos StorageGRID mueve al grupo de almacenamiento en la nube y cuándo se mueven los objetos.	El acto de ingerir un nuevo objeto en un depósito de origen que se ha configurado con un punto final de CloudMirror. Los objetos que existían en el depósito de origen antes de que este se configurara con el punto final de CloudMirror no se replican, a menos que se modifiquen.

	Grupo de almacenamiento en la nube	Servicio de replicación CloudMirror
¿Cómo se recuperan los objetos?	Las aplicaciones deben realizar solicitudes a StorageGRID para recuperar objetos que se han movido a un grupo de almacenamiento en la nube. Si la única copia de un objeto se ha transferido al almacenamiento de archivo, StorageGRID administra el proceso de restauración del objeto para que pueda recuperarse.	Dado que la copia reflejada en el depósito de destino es una copia independiente, las aplicaciones pueden recuperar el objeto realizando solicitudes a StorageGRID o al destino S3. Por ejemplo, supongamos que utiliza la replicación de CloudMirror para reflejar objetos en una organización asociada. El socio puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario utilizar StorageGRID .
¿Puedes leer desde el destino directamente?	No. Los objetos trasladados a un grupo de almacenamiento en la nube son administrados por StorageGRID. Las solicitudes de lectura deben dirigirse a StorageGRID (y StorageGRID será responsable de la recuperación del grupo de almacenamiento en la nube).	Sí, porque la copia reflejada es una copia independiente.
¿Qué sucede si se elimina un objeto de la fuente?	El objeto también se elimina del grupo de almacenamiento en la nube.	La acción de eliminar no se replica. Un objeto eliminado ya no existe en el depósito StorageGRID , pero continúa existiendo en el depósito de destino. De manera similar, los objetos en el depósito de destino se pueden eliminar sin afectar el origen.
¿Cómo acceder a los objetos después de un desastre (el sistema StorageGRID no está operativo)?	Los nodos StorageGRID fallidos deben recuperarse. Durante este proceso, se pueden restaurar copias de objetos replicados utilizando las copias en el grupo de almacenamiento en la nube.	Las copias de objetos en el destino CloudMirror son independientes de StorageGRID, por lo que se puede acceder a ellas directamente antes de que se recuperen los nodos de StorageGRID .

Crear un grupo de almacenamiento en la nube

Un grupo de almacenamiento en la nube especifica un único depósito externo de Amazon S3 u otro proveedor compatible con S3 o un contenedor de almacenamiento de blobs de Azure.

Cuando se crea un grupo de almacenamiento en la nube, se especifica el nombre y la ubicación del contenedor o depósito externo que StorageGRID usará para almacenar objetos, el tipo de proveedor de nube (Amazon S3/GCP o Azure Blob Storage) y la información que StorageGRID necesita para acceder al contenedor o depósito externo.

StorageGRID valida el grupo de almacenamiento en la nube tan pronto como lo guarda, por lo que debe asegurarse de que el depósito o contenedor especificado en el grupo de almacenamiento en la nube exista y

sea accesible.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["permisos de acceso necesarios"](#) .
- Usted ha revisado el ["Consideraciones para los grupos de almacenamiento en la nube"](#) .
- El contenedor o depósito externo al que hace referencia el grupo de almacenamiento en la nube ya existe y usted tiene la [información del punto final del servicio](#) .
- Para acceder al cubo o contenedor, tienes el [Información de la cuenta para el tipo de autenticación](#) Tú elegirás.

Pasos

1. Seleccione **ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube**.
2. Seleccione **Crear**, luego ingrese la siguiente información:

Campo	Descripción
Nombre del grupo de almacenamiento en la nube	Un nombre que describe brevemente el grupo de almacenamiento en la nube y su propósito. Utilice un nombre que sea fácil de identificar cuando configure las reglas de ILM.
Tipo de proveedor	¿Qué proveedor de nube utilizará para este grupo de almacenamiento en la nube? • Amazon S3/GCP: seleccione esta opción para un proveedor de Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) u otro proveedor compatible con S3. • Almacenamiento de blobs de Azure
Cubo o contenedor	El nombre del depósito S3 externo o del contenedor de Azure. No es posible cambiar este valor una vez guardado el grupo de almacenamiento en la nube.

3. Según su selección del tipo de proveedor, ingrese la información del punto final del servicio.

Amazon S3/GCP

- a. Para el protocolo, seleccione HTTPS o HTTP.



No utilice conexiones HTTP para datos confidenciales.

- b. Introduzca el nombre del host. Ejemplo:

`s3-aws-region.amazonaws.com`

- c. Seleccione el estilo de URL:

Opción	Descripción
Detección automática	Intente detectar automáticamente qué estilo de URL utilizar, según la información proporcionada. Por ejemplo, si especifica una dirección IP, StorageGRID utilizará una URL de estilo ruta. Seleccione esta opción solo si no sabe qué estilo específico usar.
Estilo alojado virtualmente	Utilice una URL de estilo alojado virtualmente para acceder al depósito. Las URL de estilo alojado virtualmente incluyen el nombre del depósito como parte del nombre de dominio. Ejemplo: <code>https://bucket-name.s3.company.com/key-name</code>
Estilo de ruta	Utilice una URL de estilo de ruta para acceder al depósito. Las URL de estilo de ruta incluyen el nombre del depósito al final. Ejemplo: <code>https://s3.company.com/bucket-name/key-name</code> Nota: La opción de URL de estilo de ruta no se recomienda y quedará obsoleta en una versión futura de StorageGRID.

- d. Opcionalmente, ingrese el número de puerto o utilice el puerto predeterminado: 443 para HTTPS o 80 para HTTP.

Almacenamiento de blobs de Azure

- a. Utilice uno de los siguientes formatos para ingresar el URI del punto final del servicio.

- `https://host:port`
- `http://host:port`

Ejemplo: `https://myaccount.blob.core.windows.net:443`

Si no especifica un puerto, de manera predeterminada se utiliza el puerto 443 para HTTPS y el puerto 80 para HTTP.

4. Seleccione **Continuar**. Luego, seleccione el tipo de autenticación e ingrese la información requerida para el punto final del grupo de almacenamiento en la nube:

Tecla de acceso

Para Amazon S3/GCP u otro proveedor compatible con S3

- a. **ID de clave de acceso:** Ingrese el ID de clave de acceso para la cuenta que posee el depósito externo.
- b. **Clave de acceso secreta:** Ingrese la clave de acceso secreta.

Roles de IAM en cualquier lugar

Para el servicio AWS IAM Roles Anywhere

StorageGRID utiliza el Servicio de token de seguridad de AWS (STS) para generar dinámicamente un token de corta duración para acceder a los recursos de AWS.

- a. **Región de AWS IAM Roles Anywhere:** seleccione la región para el grupo de almacenamiento en la nube. Por ejemplo, `us-east-1`.
- b. **URN de ancla de confianza:** ingrese la URN del ancla de confianza que valida las solicitudes de credenciales STS de corta duración. Puede ser una CA raíz o intermedia.
- c. **URN de perfil:** ingrese la URN del perfil de IAM Roles Anywhere que enumera los roles que pueden asumirse para cualquier persona de confianza.
- d. **URN de rol:** Ingrese el URN del rol de IAM que puede asumir cualquier persona de confianza.
- e. **Duración de la sesión:** Ingrese la duración de las credenciales de seguridad temporales y la sesión del rol. Ingrese al menos 15 minutos y no más de 12 horas.
- f. **Certificado de CA del servidor** (opcional): Uno o más certificados de CA confiables, en formato PEM, para verificar el servidor de IAM Roles Anywhere. Si se omite, el servidor no se verificará.
- g. **Certificado de entidad final:** La clave pública, en formato PEM, del certificado X509 firmado por el ancla de confianza. AWS IAM Roles Anywhere utiliza esta clave para emitir un token STS.
- h. **Clave privada de entidad final:** la clave privada para el certificado de entidad final.

CAP (portal de acceso C2S)

Para el servicio S3 de Servicios de Nube Comercial (C2S)

- a. **URL de credenciales temporales:** ingrese la URL completa que StorageGRID utilizará para obtener las credenciales temporales del servidor CAP, incluidos todos los parámetros de API obligatorios y opcionales asignados a su cuenta C2S.
- b. **Certificado CA del servidor:** seleccione **Explorar** y cargue el certificado CA que StorageGRID utilizará para verificar el servidor CAP. El certificado debe estar codificado en PEM y ser emitido por una autoridad de certificación gubernamental (CA) apropiada.
- c. **Certificado de cliente:** seleccione **Explorar** y cargue el certificado que StorageGRID utilizará para identificarse en el servidor CAP. El certificado del cliente debe estar codificado en PEM, emitido por una autoridad de certificación gubernamental (CA) apropiada y tener acceso a su cuenta C2S.
- d. **Clave privada del cliente:** seleccione **Explorar** y cargue la clave privada codificada en PEM para el certificado del cliente.
- e. Si la clave privada del cliente está cifrada, ingrese la contraseña para descifrarla. De lo contrario, deje el campo **Frase de contraseña de clave privada del cliente** en blanco.



Si se va a cifrar el certificado del cliente, utilice el formato tradicional para el cifrado. El formato cifrado PKCS #8 no es compatible.

Almacenamiento de blobs de Azure

Para Azure Blob Storage, solo clave compartida

- Nombre de la cuenta:** Ingrese el nombre de la cuenta de almacenamiento que posee el contenedor externo
- Clave de cuenta:** Ingrese la clave secreta para la cuenta de almacenamiento

Puede utilizar el portal de Azure para encontrar estos valores.

Anónimo

No se requiere información adicional

5. Seleccione **Continuar**. A continuación, elija el tipo de verificación de servidor que desea utilizar:

Opción	Descripción
Usar certificados de CA raíz en el sistema operativo del nodo de almacenamiento	Utilice los certificados CA de Grid instalados en el sistema operativo para proteger las conexiones.
Utilice un certificado CA personalizado	Utilice un certificado CA personalizado. Seleccione Explorar y cargue el certificado codificado en PEM.
No verificar el certificado	Seleccionar esta opción significa que las conexiones TLS al grupo de almacenamiento en la nube no son seguras.

6. Seleccione **Guardar**.

Cuando guarda un grupo de almacenamiento en la nube, StorageGRID hace lo siguiente:

- Valida que el depósito o contenedor y el punto final del servicio existan y que se pueda acceder a ellos utilizando las credenciales que usted especificó.
- Escribe un archivo de marcador en el depósito o contenedor para identificarlo como un grupo de almacenamiento en la nube. Nunca elimine este archivo, que se llama `x-ntap-sgws-cloud-pool-uuid`.

Si falla la validación del grupo de almacenamiento en la nube, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, se podría informar un error si hay un error de certificado o si el depósito o contenedor especificado aún no existe.

7. Si se produce un error, consulte la "[Instrucciones para solucionar problemas de grupos de almacenamiento en la nube](#)", resuelva cualquier problema y luego intente guardar el grupo de almacenamiento en la nube nuevamente.

Ver detalles del grupo de almacenamiento en la nube

Puede ver los detalles de un grupo de almacenamiento en la nube para determinar

dónde se utiliza y ver qué nodos y grados de almacenamiento están incluidos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .

Pasos

1. Seleccione **ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube**.

La tabla de grupos de almacenamiento en la nube incluye la siguiente información para cada grupo de almacenamiento en la nube que incluye nodos de almacenamiento:

- **Nombre:** el nombre para mostrar único del grupo.
- **URI:** El identificador uniforme de recursos del grupo de almacenamiento en la nube.
- **Tipo de proveedor:** ¿Qué proveedor de nube se utiliza para este grupo de almacenamiento en la nube?
- **Contenedor:** el nombre del depósito utilizado para el grupo de almacenamiento en la nube.
- **Uso de ILM:** cómo se utiliza actualmente el pool. Es posible que un grupo de almacenamiento en la nube no se utilice o que se utilice en una o más reglas ILM, perfiles de codificación de borrado o ambos.
- **Último error:** el último error detectado durante una verificación del estado de este grupo de almacenamiento en la nube.

2. Para ver los detalles de un grupo de almacenamiento en la nube específico, seleccione su nombre.

Aparece la página de detalles del grupo.

3. Consulte la pestaña **Autenticación** para obtener información sobre el tipo de autenticación para este grupo de almacenamiento en la nube y para editar los detalles de autenticación.
4. Vea la pestaña **Verificación del servidor** para obtener información sobre los detalles de verificación, editar la verificación, descargar un nuevo certificado o copiar el certificado PEM.
5. Vea la pestaña **Uso de ILM** para determinar si el grupo de almacenamiento en la nube se está utilizando actualmente en alguna regla de ILM o perfil de codificación de borrado.
6. Opcionalmente, vaya a la **página de reglas de ILM** para ["Conozca y administre cualquier regla"](#) que utilizan el grupo de almacenamiento en la nube.

Editar un grupo de almacenamiento en la nube

Puede editar un grupo de almacenamiento en la nube para cambiar su nombre, punto final de servicio u otros detalles; sin embargo, no puede cambiar el depósito S3 ni el contenedor de Azure de un grupo de almacenamiento en la nube.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Usted ha revisado el ["Consideraciones para los grupos de almacenamiento en la nube"](#) .

Pasos

1. Seleccione **ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube**.

La tabla Grupos de almacenamiento en la nube enumera los grupos de almacenamiento en la nube existentes.

2. Seleccione la casilla de verificación del grupo de almacenamiento en la nube que desea editar y luego seleccione **Acciones > Editar**.

Alternativamente, seleccione el nombre del grupo de almacenamiento en la nube y luego seleccione **Editar**.

3. Según sea necesario, cambie el nombre del grupo de almacenamiento en la nube, el punto final del servicio, las credenciales de autenticación o el método de verificación del certificado.



No se puede cambiar el tipo de proveedor ni el bucket S3 ni el contenedor de Azure para un grupo de almacenamiento en la nube.

Si anteriormente cargó un certificado de servidor o cliente, puede expandir el acordeón **Detalles del certificado** para revisar el certificado que está actualmente en uso.

4. Seleccione **Guardar**.

Cuando guarda un grupo de almacenamiento en la nube, StorageGRID valida que el depósito o contenedor y el punto final del servicio existan y que se pueda acceder a ellos mediante las credenciales que usted especificó.

Si falla la validación del grupo de almacenamiento en la nube, se muestra un mensaje de error. Por ejemplo, se podría informar un error si hay un error de certificado.

Vea las instrucciones para "[Solución de problemas de grupos de almacenamiento en la nube](#)", resuelva el problema y luego intente guardar el grupo de almacenamiento en la nube nuevamente.

Eliminar un grupo de almacenamiento en la nube

Puede eliminar un grupo de almacenamiento en la nube si no se utiliza en una regla ILM y no contiene datos de objetos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tú tienes el "[permisos de acceso necesarios](#)".

Si es necesario, utilice ILM para mover datos de objetos

Si el grupo de almacenamiento en la nube que desea eliminar contiene datos de objetos, debe usar ILM para mover los datos a una ubicación diferente. Por ejemplo, puede mover los datos a nodos de almacenamiento en su red o a un grupo de almacenamiento en la nube diferente.

Pasos

1. Seleccione **ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube**.

2. Mire la columna de uso de ILM en la tabla para determinar si puede eliminar el grupo de almacenamiento en la nube.

No se puede eliminar un grupo de almacenamiento en la nube si se está utilizando en una regla ILM o en un perfil de codificación de borrado.

3. Si se está utilizando el grupo de almacenamiento en la nube, seleccione **nombre del grupo de almacenamiento en la nube > uso de ILM**.
4. ["Clonar cada regla ILM"](#) que actualmente coloca objetos en el grupo de almacenamiento en la nube que desea eliminar.
5. Determina dónde quieres mover los objetos existentes administrados por cada regla que clonaste.

Puede utilizar uno o más grupos de almacenamiento o un grupo de almacenamiento en la nube diferente.

6. Edite cada una de las reglas que clonó.

Para el paso 2 del asistente para crear reglas de ILM, seleccione la nueva ubicación en el campo **copias en**.

7. ["Crear una nueva política de ILM"](#) y reemplazar cada una de las reglas antiguas con una regla clonada.
8. Activar la nueva política.
9. Espere a que ILM elimine objetos del grupo de almacenamiento en la nube y los coloque en la nueva ubicación.

Eliminar grupo de almacenamiento en la nube

Cuando el grupo de almacenamiento en la nube esté vacío y no se utilice en ninguna regla de ILM, puedes eliminarlo.

Antes de empezar

- Ha eliminado todas las reglas ILM que podrían haber utilizado el grupo.
- Ha confirmado que el bucket S3 o el contenedor de Azure no contiene ningún objeto.

Se produce un error si intenta eliminar un grupo de almacenamiento en la nube si contiene objetos. Ver ["Solucionar problemas de grupos de almacenamiento en la nube"](#).



Cuando se crea un grupo de almacenamiento en la nube, StorageGRID escribe un archivo marcador en el depósito o contenedor para identificarlo como un grupo de almacenamiento en la nube. No elimine este archivo, que se llama `x-ntap-sgws-cloud-pool-uuid`.

Pasos

1. Seleccione **ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube**.
2. Si la columna de uso de ILM indica que no se está utilizando el grupo de almacenamiento en la nube, seleccione la casilla de verificación.
3. Seleccione **Acciones > Eliminar**.
4. Seleccione **Aceptar**.

Solucionar problemas de grupos de almacenamiento en la nube

Utilice estos pasos de solución de problemas para ayudar a resolver errores que pueda encontrar al crear, editar o eliminar un grupo de almacenamiento en la nube.

Determinar si se ha producido un error

StorageGRID realiza una comprobación de estado simple en cada grupo de almacenamiento en la nube leyendo el objeto conocido `x-ntap-sgws-cloud-pool-uuid` para garantizar que se pueda acceder al grupo de almacenamiento en la nube y que funcione correctamente. Cuando StorageGRID detecta un error en el punto final, realiza una comprobación del estado cada minuto desde cada nodo de almacenamiento. Cuando se resuelve el error, las comprobaciones de estado se detienen. Si una verificación de estado detecta un problema, se muestra un mensaje en la columna **Último error** de la tabla Grupos de almacenamiento en la nube en la página Grupos de almacenamiento.

La tabla muestra el error más reciente detectado para cada grupo de almacenamiento en la nube e indica cuánto tiempo hace que ocurrió el error.

Además, se activa una alerta de **Error de conectividad del Cloud Storage Pool** si la comprobación de estado detecta que se han producido uno o más errores nuevos del Cloud Storage Pool en los últimos 5 minutos. Si recibe una notificación por correo electrónico para esta alerta, vaya a la página Grupos de almacenamiento (seleccione **ILM > Grupos de almacenamiento**), revise los mensajes de error en la columna **Último error** y consulte las pautas de solución de problemas a continuación.

Comprobar si se ha resuelto un error

Después de resolver cualquier problema subyacente, puede determinar si se ha resuelto el error. Desde la página Grupo de almacenamiento en la nube, seleccione el punto final y seleccione **Borrar error**. Un mensaje de confirmación indica que StorageGRID ha solucionado el error del grupo de almacenamiento en la nube.

Si se ha resuelto el problema subyacente, el mensaje de error ya no se muestra. Sin embargo, si el problema subyacente no se ha solucionado (o si se encuentra un error diferente), el mensaje de error se mostrará en la columna **Último error** dentro de unos minutos.

Error: Error en la comprobación de salud. Error del punto final

Es posible que encuentre este error cuando habilite el bloqueo de objetos S3 con retención predeterminada para su depósito de Amazon S3 después de comenzar a usar este depósito para un grupo de almacenamiento en la nube. Este error ocurre cuando la operación PUT no tiene un encabezado HTTP con un valor de suma de comprobación de carga útil como `Content-MD5`. AWS requiere este valor de encabezado para operaciones PUT en buckets con el bloqueo de objetos S3 habilitado.

Para corregir este problema, siga los pasos que se indican en ["Editar un grupo de almacenamiento en la nube"](#) sin realizar ningún cambio. Esta acción activa la validación de la configuración del grupo de almacenamiento en la nube que detecta y actualiza automáticamente el indicador de bloqueo de objetos S3 en una configuración de punto final del grupo de almacenamiento en la nube.

Error: Este grupo de almacenamiento en la nube contiene contenido inesperado

Es posible que encuentre este error cuando intente crear, editar o eliminar un grupo de almacenamiento en la nube. Este error se produce si el depósito o contenedor incluye el `x-ntap-sgws-cloud-pool-uuid` archivo marcador, pero ese archivo no tiene el campo de metadatos con el UUID esperado.

Por lo general, solo verá este error si está creando un nuevo grupo de almacenamiento en la nube y otra instancia de StorageGRID ya está usando el mismo grupo de almacenamiento en la nube.

Pruebe uno de estos pasos para corregir el problema:

- Si está configurando un nuevo grupo de almacenamiento en la nube y el depósito contiene el `x-ntap-sgws-cloud-pool-uuid` archivo y claves de objeto adicionales similares al siguiente ejemplo, cree un

nuevo depósito y use este nuevo depósito en su lugar.

Ejemplo de una clave de objeto adicional: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Si el `x-ntap-sgws-cloud-pool-uuid` el archivo es el único objeto en el depósito, elimine este archivo.

Si estos pasos no se aplican a su situación, comuníquese con el soporte técnico.

Error: No se pudo crear o actualizar el grupo de almacenamiento en la nube. Error del punto final

Es posible que encuentre este error en las siguientes circunstancias:

- Cuando intenta crear o editar un grupo de almacenamiento en la nube.
- Cuando selecciona una plataforma, autenticación o combinación de protocolo no compatible con S3 Object Lock durante la configuración de un nuevo grupo de almacenamiento en la nube. Ver ["Consideraciones para los grupos de almacenamiento en la nube"](#).

Este error indica que un problema de conectividad o configuración impide que StorageGRID escriba en el grupo de almacenamiento en la nube.

Para corregir el problema, revise el mensaje de error del punto final.

- Si el mensaje de error contiene `Get url: EOF` Verifique que el punto final del servicio utilizado para el grupo de almacenamiento en la nube no utilice HTTP para un contenedor o depósito que requiera HTTPS.
- Si el mensaje de error contiene `Get url: net/http: request canceled while waiting for connection`, verifique que la configuración de la red permita que los nodos de almacenamiento accedan al punto final de servicio utilizado para el grupo de almacenamiento en la nube.
- Si el error se debe a una plataforma, autenticación o protocolo no compatible, cambie a una configuración compatible con S3 Object Lock e intente guardar nuevamente el nuevo grupo de almacenamiento en la nube.
- Para todos los demás mensajes de error de punto final, pruebe una o más de las siguientes opciones:
 - Cree un contenedor o depósito externo con el mismo nombre que ingresó para el grupo de almacenamiento en la nube e intente guardar el nuevo grupo de almacenamiento en la nube nuevamente.
 - Corrija el nombre del contenedor o depósito que especificó para el grupo de almacenamiento en la nube e intente guardar el nuevo grupo de almacenamiento en la nube nuevamente.

Error: No se pudo analizar el certificado de CA

Es posible que encuentre este error cuando intente crear o editar un grupo de almacenamiento en la nube. El error ocurre si StorageGRID no pudo analizar el certificado ingresado al configurar el grupo de almacenamiento en la nube.

Para corregir el problema, verifique el certificado CA que proporcionó para ver si hay problemas.

Error: No se encontró un grupo de almacenamiento en la nube con este ID

Es posible que encuentre este error cuando intente editar o eliminar un grupo de almacenamiento en la nube. Este error ocurre si el punto final devuelve una respuesta 404, que puede significar cualquiera de las siguientes cosas:

- Las credenciales utilizadas para el grupo de almacenamiento en la nube no tienen permiso de lectura para el depósito.
- El depósito utilizado para el grupo de almacenamiento en la nube no incluye el `x-ntap-sgws-cloud-pool-uuid` archivo de marcador.

Pruebe uno o más de estos pasos para corregir el problema:

- Verifique que el usuario asociado a la clave de acceso configurada tenga los permisos necesarios.
- Edite el grupo de almacenamiento en la nube con credenciales que tengan los permisos necesarios.
- Si los permisos son correctos, comuníquese con el soporte.

Error: No se pudo comprobar el contenido del grupo de almacenamiento en la nube. Error del punto final

Es posible que encuentre este error cuando intente eliminar un grupo de almacenamiento en la nube. Este error indica que algún tipo de problema de conectividad o configuración impide que StorageGRID lea el contenido del depósito de Cloud Storage Pool.

Para corregir el problema, revise el mensaje de error del punto final.

Error: Ya se han colocado objetos en este depósito

Es posible que encuentre este error cuando intente eliminar un grupo de almacenamiento en la nube. No puedes eliminar un grupo de almacenamiento en la nube si contiene datos que ILM movió allí, datos que estaban en el depósito antes de configurar el grupo de almacenamiento en la nube o datos que alguna otra fuente colocó en el depósito después de que se creó el grupo de almacenamiento en la nube.

Pruebe uno o más de estos pasos para corregir el problema:

- Siga las instrucciones para mover objetos nuevamente a StorageGRID en "Ciclo de vida de un objeto de grupo de almacenamiento en la nube".
- Si está seguro de que ILM no colocó los objetos restantes en el grupo de almacenamiento en la nube, elimine manualmente los objetos del depósito.



Nunca elimine manualmente objetos de un grupo de almacenamiento en la nube que ILM pueda haber colocado allí. Si posteriormente intenta acceder a un objeto eliminado manualmente desde StorageGRID, no se encontrará el objeto eliminado.

Error: el proxy encontró un error externo al intentar acceder al grupo de almacenamiento en la nube

Es posible que encuentre este error si ha configurado un proxy de almacenamiento no transparente entre los nodos de almacenamiento y el punto final S3 externo utilizado para el grupo de almacenamiento en la nube. Este error se produce si el servidor proxy externo no puede acceder al punto final del grupo de almacenamiento en la nube. Por ejemplo, es posible que el servidor DNS no pueda resolver el nombre de host o que haya un problema de red externa.

Pruebe uno o más de estos pasos para corregir el problema:

- Verifique la configuración del grupo de almacenamiento en la nube (**ILM > Grupos de almacenamiento**).
- Verifique la configuración de red del servidor proxy de almacenamiento.

Error: el certificado X.509 está fuera del período de validez

Es posible que encuentre este error cuando intente eliminar un grupo de almacenamiento en la nube. Este error ocurre cuando la autenticación requiere un certificado X.509 para garantizar que se valide el grupo de almacenamiento en la nube externo correcto y el grupo externo está vacío antes de que se elimine la configuración del grupo de almacenamiento en la nube.

Pruebe estos pasos para corregir el problema:

- Actualice el certificado configurado para la autenticación en el grupo de almacenamiento en la nube.
- Asegúrese de que se haya resuelto cualquier alerta de vencimiento de certificado en este grupo de almacenamiento en la nube.

Información relacionada

["Ciclo de vida de un objeto de grupo de almacenamiento en la nube"](#)

Administrar perfiles de codificación de borrado

Puede ver los detalles de un perfil de codificación de borrado y cambiar el nombre de un perfil si es necesario. Puede desactivar un perfil de codificación de borrado si no se utiliza actualmente en ninguna regla ILM.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["permisos de acceso necesarios"](#).

Ver detalles del perfil de codificación de borrado

Puede ver los detalles de un perfil de codificación de borrado para determinar su estado, el esquema de codificación de borrado utilizado y otra información.

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Codificación de borrado**.
2. Seleccione el perfil. Aparece la página de detalles del perfil.
3. Opcionalmente, consulte la pestaña de reglas de ILM para obtener una lista de las reglas de ILM que usan el perfil y las políticas de ILM que usan esas reglas.
4. Opcionalmente, consulte la pestaña Nodos de almacenamiento para obtener detalles sobre cada nodo de almacenamiento en el grupo de almacenamiento del perfil, como el sitio donde está ubicado y el uso del almacenamiento.

Cambiar el nombre de un perfil de codificación de borrado

Es posible que desees cambiar el nombre de un perfil de codificación de borrado para que sea más obvio lo que hace el perfil.

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Codificación de borrado**.
2. Seleccione el perfil que desea renombrar.
3. Seleccione **Cambiar nombre**.

4. Introduzca un nombre único para el perfil de codificación de borrado.

El nombre del perfil de codificación de borrado se agrega al nombre del grupo de almacenamiento en la instrucción de ubicación de una regla ILM.



Los nombres de los perfiles de codificación de borrado deben ser únicos. Se produce un error de validación si utiliza el nombre de un perfil existente, incluso si dicho perfil se ha desactivado.

5. Seleccione **Guardar**.

Desactivar un perfil de codificación de borrado

Puede desactivar un perfil de codificación de borrado si ya no planea usarlo y si el perfil no se utiliza actualmente en ninguna regla de ILM.



Confirme que no haya operaciones de reparación de datos con código de borrado ni procedimientos de desmantelamiento en proceso. Se devuelve un mensaje de error si intenta desactivar un perfil de codificación de borrado mientras alguna de estas operaciones está en progreso.

Acerca de esta tarea

StorageGRID le impide desactivar un perfil de codificación de borrado si se cumple alguna de las siguientes condiciones:

- Actualmente, el perfil de codificación de borrado se utiliza en una regla ILM.
- El perfil de codificación de borrado ya no se utiliza en ninguna regla ILM, pero los datos de objetos y los fragmentos de paridad para el perfil aún existen.

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Codificación de borrado**.
2. En la pestaña Activo, revise la columna **Estado** para confirmar que el perfil de codificación de borrado que desea desactivar no se utiliza en ninguna regla de ILM.

No se puede desactivar un perfil de codificación de borrado si se utiliza en alguna regla ILM. En el ejemplo, el perfil 2+1 del centro de datos 1 se utiliza en al menos una regla ILM.

☐	Profile name ? ⇅	Status ? ⇅	Storage pool ? ⇅	Erasure-coding scheme ? ⇅
☐	2+1 Data Center 1	Used in <u>5 rules</u>	Data Center 1	2+1
☐	New profile	Deactivated	Data Center 1	2+1

3. Si el perfil se utiliza en una regla ILM, siga estos pasos:
 - a. Seleccione **ILM > Reglas**.
 - b. Seleccione cada regla y revise el diagrama de retención para determinar si la regla utiliza el perfil de codificación de borrado que desea desactivar.
 - c. Si la regla ILM utiliza el perfil de codificación de borrado que desea desactivar, determine si la regla se

utiliza en alguna política ILM.

d. Complete los pasos adicionales de la tabla, según dónde se utilice el perfil de codificación de borrado.

¿Dónde se ha utilizado el perfil?	Pasos adicionales a realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
Nunca se utiliza en ninguna regla ILM	No se requieren pasos adicionales. Continúe con este procedimiento.	<i>Ninguno</i>
En una regla ILM que nunca se ha utilizado en ninguna política ILM	i. Editar o eliminar todas las reglas ILM afectadas. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de codificación de borrado. ii. Continúe con este procedimiento.	"Trabajar con las reglas y políticas de ILM"
En una regla ILM que actualmente se encuentra en una política ILM activa	i. Clonar la política. ii. Eliminar la regla ILM que utiliza el perfil de codificación de borrado. iii. Agregue una o más reglas ILM nuevas para garantizar que los objetos estén protegidos. iv. Guarde, simule y active la nueva política. v. Espere a que se aplique la nueva política y a que los objetos existentes se muevan a nuevas ubicaciones según las nuevas reglas que agregó. Nota: Dependiendo de la cantidad de objetos y el tamaño de su sistema StorageGRID , las operaciones de ILM podrían tardar semanas o incluso meses en mover los objetos a nuevas ubicaciones, según las nuevas reglas de ILM. Si bien puede intentar desactivar de forma segura un perfil de codificación de borrado mientras aún esté asociado con datos, la operación de desactivación fallará. Un mensaje de error le informará si el perfil aún no está listo para ser desactivado. vi. Edite o elimine la regla que quitó de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de codificación de borrado. vii. Continúe con este procedimiento.	"Crear una política ILM" "Trabajar con las reglas y políticas de ILM"

¿Dónde se ha utilizado el perfil?	Pasos adicionales a realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
En una regla ILM que actualmente se encuentra en una política ILM	i. Editar la política. ii. Eliminar la regla ILM que utiliza el perfil de codificación de borrado. iii. Agregue una o más reglas ILM nuevas para garantizar que todos los objetos estén protegidos. iv. Guardar la política. v. Edite o elimine la regla que quitó de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de codificación de borrado. vi. Continúe con este procedimiento.	"Crear una política ILM" "Trabajar con las reglas y políticas de ILM"

e. Actualice la página Perfiles de codificación de borrado para asegurarse de que el perfil no se utilice en una regla ILM.

4. Si el perfil no se utiliza en una regla ILM, seleccione el botón de opción y seleccione **Desactivar**. Aparece el cuadro de diálogo Desactivar perfil de codificación de borrado.



Puede seleccionar varios perfiles para desactivarlos al mismo tiempo, siempre que cada perfil no se utilice en ninguna regla.

5. Si está seguro de que desea desactivar el perfil, seleccione **Desactivar**.

Resultados

- Si StorageGRID puede desactivar el perfil de codificación de borrado, su estado es Desactivado. Ya no puedes seleccionar este perfil para ninguna regla ILM. No es posible reactivar un perfil desactivado.
- Si StorageGRID no puede desactivar el perfil, aparecerá un mensaje de error. Por ejemplo, aparece un mensaje de error si los datos del objeto aún están asociados con este perfil. Es posible que tengas que esperar varias semanas antes de intentar nuevamente el proceso de desactivación.

Configurar regiones (opcional y solo S3)

Las reglas ILM pueden filtrar objetos según las regiones donde se crean los buckets S3, lo que le permite almacenar objetos de diferentes regiones en diferentes ubicaciones de almacenamiento.

Si desea utilizar una región de bucket S3 como filtro en una regla, primero debe crear las regiones que los buckets pueden usar en su sistema.



No es posible cambiar la región de un depósito una vez creado el mismo.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).

- Tienes "permisos de acceso específicos" .

Acerca de esta tarea

Al crear un depósito S3, puede especificar que el depósito se cree en una región específica. Al especificar una región, el bucket puede estar geográficamente cerca de sus usuarios, lo que puede ayudar a optimizar la latencia, minimizar los costos y abordar los requisitos regulatorios.

Al crear una regla ILM, es posible que desee utilizar la región asociada con un depósito S3 como filtro avanzado. Por ejemplo, puede diseñar una regla que se aplique únicamente a los objetos en los depósitos S3 creados en el `us-west-2` región. Luego, puede especificar que se coloquen copias de esos objetos en nodos de almacenamiento en un sitio del centro de datos dentro de esa región para optimizar la latencia.

Al configurar regiones, siga estas pautas:

- De forma predeterminada, se considera que todos los depósitos pertenecen a la `us-east-1` región.
- Debe crear las regiones usando Grid Manager antes de poder especificar una región no predeterminada al crear depósitos usando Tenant Manager o Tenant Management API o con el elemento de solicitud `LocationConstraint` para solicitudes de API de depósito PUT de S3. Se produce un error si una solicitud PUT Bucket utiliza una región que no se ha definido en StorageGRID.
- Debes utilizar el nombre exacto de la región al crear el bucket S3. Los nombres de las regiones distinguen entre mayúsculas y minúsculas. Los caracteres válidos son números, letras y guiones.



EU no se considera un alias de eu-west-1. Si desea utilizar la región UE o eu-west-1, debe utilizar el nombre exacto.

- No se puede eliminar ni modificar una región si se utiliza en una regla asignada a cualquier política (activa o inactiva).
- Si utiliza una región no válida como filtro avanzado en una regla ILM, no podrá agregar esa regla a una política.

Puede obtenerse una región no válida si utiliza una región como filtro avanzado en una regla ILM pero luego elimina esa región, o si utiliza la API de administración de cuadrícula para crear una regla y especificar una región que no ha definido.

- Si elimina una región después de usarla para crear un depósito S3, deberá volver a agregar la región si alguna vez desea utilizar el filtro avanzado de Restricción de ubicación para buscar objetos en ese depósito.

Pasos

1. Seleccione **ILM > Regiones**.

Aparece la página Regiones, con una lista de las regiones definidas actualmente. **Región 1** muestra la región predeterminada, `us-east-1` , que no se puede modificar ni eliminar.

2. Para agregar una región:

- a. Seleccione **Agregar otra región**.
- b. Ingrese el nombre de la región que desea utilizar al crear depósitos S3.

Debe utilizar este nombre de región exacto como elemento de solicitud `LocationConstraint` cuando cree el bucket S3 correspondiente.

3. Para eliminar una región no utilizada, seleccione el icono de eliminar  .

Aparece un mensaje de error si intenta eliminar una región que se utiliza actualmente en cualquier política (activa o inactiva).

4. Cuando haya terminado de realizar cambios, seleccione **Guardar**.

Ahora puede seleccionar estas regiones desde la sección Filtros avanzados en el paso 1 del asistente Crear regla ILM. Ver "[Utilice filtros avanzados en las reglas de ILM](#)".

Crear regla ILM

Utilice reglas ILM para administrar objetos

Para administrar objetos, debe crear un conjunto de reglas de administración del ciclo de vida de la información (ILM) y organizarlas en una política ILM.

Cada objeto ingerido en el sistema se evalúa en función de la política activa. Cuando una regla en la política coincide con los metadatos de un objeto, las instrucciones en la regla determinan qué acciones realiza StorageGRID para copiar y almacenar ese objeto.



Los metadatos de los objetos no son administrados por las reglas ILM. En cambio, los metadatos de los objetos se almacenan en una base de datos de Cassandra en lo que se conoce como un almacén de metadatos. Se mantienen automáticamente tres copias de los metadatos de los objetos en cada sitio para proteger los datos contra pérdidas.

Elementos de una regla ILM

Una regla ILM tiene tres elementos:

- **Criterios de filtrado:** Los filtros básicos y avanzados de una regla definen a qué objetos se aplica la regla. Si un objeto coincide con todos los filtros, StorageGRID aplica la regla y crea las copias de objetos especificadas en las instrucciones de ubicación de la regla.
- **Instrucciones de ubicación:** Las instrucciones de ubicación de una regla definen el número, tipo y ubicación de las copias de objetos. Cada regla puede incluir una secuencia de instrucciones de ubicación para cambiar la cantidad, el tipo y la ubicación de las copias de objetos a lo largo del tiempo. Cuando expira el plazo para una colocación, las instrucciones de la siguiente colocación se aplican automáticamente en la siguiente evaluación de ILM.
- **Comportamiento de ingesta:** el comportamiento de ingesta de una regla le permite elegir cómo se protegen los objetos filtrados por la regla a medida que se ingieren (cuando un cliente S3 guarda un objeto en la cuadrícula).

Filtrado de reglas ILM

Cuando se crea una regla ILM, se especifican filtros para identificar a qué objetos se aplica la regla.

En el caso más simple, es posible que una regla no utilice ningún filtro. Cualquier regla que no utilice filtros se aplica a todos los objetos, por lo que debe ser la última regla (predeterminada) en una política ILM. La regla predeterminada proporciona instrucciones de almacenamiento para los objetos que no coinciden con los filtros de otra regla.

- Los filtros básicos le permiten aplicar diferentes reglas a grupos grandes y distintos de objetos. Estos

filtros le permiten aplicar una regla a cuentas de inquilinos específicos, depósitos S3 específicos o ambos.

Los filtros básicos le brindan una forma sencilla de aplicar diferentes reglas a un gran número de objetos. Por ejemplo, es posible que sea necesario almacenar los registros financieros de su empresa para cumplir con los requisitos reglamentarios, mientras que es posible que sea necesario almacenar los datos del departamento de marketing para facilitar las operaciones diarias. Después de crear cuentas de inquilinos independientes para cada departamento o después de segregar datos de los diferentes departamentos en grupos S3 separados, puede crear fácilmente una regla que se aplique a todos los registros financieros y una segunda regla que se aplique a todos los datos de marketing.

- Los filtros avanzados le brindan un control granular. Puede crear filtros para seleccionar objetos según las siguientes propiedades del objeto:
 - Tiempo de ingesta
 - Hora del último acceso
 - Todo o parte del nombre del objeto (Clave)
 - Restricción de ubicación (solo S3)
 - Tamaño del objeto
 - Metadatos del usuario
 - Etiqueta de objeto (solo S3)

Puede filtrar objetos según criterios muy específicos. Por ejemplo, los objetos almacenados por el departamento de imágenes de un hospital pueden usarse con frecuencia cuando tienen menos de 30 días y con poca frecuencia después, mientras que los objetos que contienen información de visitas de pacientes pueden necesitar copiarse al departamento de facturación en la sede central de la red de salud. Puede crear filtros que identifiquen cada tipo de objeto según el nombre del objeto, el tamaño, las etiquetas de objeto S3 o cualquier otro criterio relevante y luego crear reglas independientes para almacenar cada conjunto de objetos de forma adecuada.

Puede combinar filtros según sea necesario en una sola regla. Por ejemplo, el departamento de marketing podría querer almacenar archivos de imágenes grandes de forma diferente a sus registros de proveedores, mientras que el departamento de Recursos Humanos podría necesitar almacenar registros de personal en una geografía específica e información de políticas de forma centralizada. En este caso, puede crear reglas que filtren por cuenta de inquilino para segregar los registros de cada departamento, mientras utiliza filtros en cada regla para identificar el tipo específico de objetos a los que se aplica la regla.

Instrucciones de colocación de reglas ILM

Las instrucciones de ubicación determinan dónde, cuándo y cómo se almacenan los datos de los objetos. Una regla ILM puede incluir una o más instrucciones de ubicación. Cada instrucción de colocación se aplica a un único período de tiempo.

Al crear instrucciones de ubicación:

- Comienza especificando el tiempo de referencia, que determina cuándo comienzan las instrucciones de colocación. El tiempo de referencia puede ser cuando se ingiere un objeto, cuando se accede a un objeto, cuando un objeto versionado deja de ser actual o un tiempo definido por el usuario.
- A continuación, especifica cuándo se aplicará la ubicación, en relación con el tiempo de referencia. Por ejemplo, una ubicación podría comenzar el día 0 y continuar durante 365 días, en relación con el momento en que se ingirió el objeto.
- Por último, se especifica el tipo de copias (codificación de replicación o borrado) y la ubicación donde se almacenan las copias. Por ejemplo, es posible que desee almacenar dos copias replicadas en dos sitios

diferentes.

Cada regla puede definir múltiples ubicaciones para un solo período de tiempo y diferentes ubicaciones para diferentes períodos de tiempo.

- Para colocar objetos en varias ubicaciones durante un solo período de tiempo, seleccione **Agregar otro tipo o ubicación** para agregar más de una línea para ese período de tiempo.
- Para colocar objetos en diferentes ubicaciones en diferentes períodos de tiempo, seleccione **Agregar otro período de tiempo** para agregar el siguiente período de tiempo. Luego, especifique una o más líneas dentro del período de tiempo.

El ejemplo muestra dos instrucciones de ubicación en la página Definir ubicaciones del asistente Crear regla de ILM.

Time period and placements [Sort by start date](#)

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1 From Day 0 store for 365 days

Store objects by replicating 2 copies at Data Center 1, Data Center 2

and store objects by erasure coding using 6+3 EC scheme at all sites

[Add other type or location](#)

Time period 2 From Day 365 store forever

Store objects by replicating 2 copies at Data Center 3

[Add other type or location](#)

La primera instrucción de colocación ¹ tiene dos líneas para el primer año:

- La primera línea crea dos copias de objetos replicados en dos sitios de centros de datos.
- La segunda línea crea una copia con código de borrado 6+3 utilizando todos los sitios del centro de datos.

La segunda instrucción de colocación ² crea dos copias después de un año y conserva esas copias para siempre.

Al definir el conjunto de instrucciones de ubicación para una regla, debe asegurarse de que al menos una instrucción de ubicación comience en el día 0, que no haya espacios entre los períodos de tiempo que haya definido y que la instrucción de ubicación final continúe para siempre o hasta que ya no necesite copias de objetos.

A medida que expira cada período de tiempo de la regla, se aplican las instrucciones de ubicación de contenido para el siguiente período de tiempo. Se crean nuevas copias de objetos y se eliminan las copias innecesarias.

Comportamiento de ingesta de reglas ILM

El comportamiento de ingesta controla si las copias de objetos se colocan inmediatamente de acuerdo con las instrucciones de la regla, o si se realizan copias provisionales y las instrucciones de ubicación se aplican más tarde. Los siguientes comportamientos de ingesta están disponibles para las reglas ILM:

- **Equilibrado:** StorageGRID intenta realizar todas las copias especificadas en la regla ILM en la ingesta; si esto no es posible, se realizan copias provisionales y se devuelve el resultado exitoso al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.
- **Estricto:** Se deben realizar todas las copias especificadas en la regla ILM antes de devolver el resultado exitoso al cliente.
- **Confirmación dual:** StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve el éxito al cliente. Cuando sea posible se realizarán las copias especificadas en la regla ILM.

Información relacionada

- ["Opciones de ingesta"](#)
- ["Ventajas, desventajas y limitaciones de las opciones de ingesta"](#)
- ["Cómo interactúan la consistencia y las reglas ILM para afectar la protección de datos"](#)

Ejemplo de regla ILM

A modo de ejemplo, una regla ILM podría especificar lo siguiente:

- Aplicar únicamente a los objetos pertenecientes al Inquilino A.
- Haga dos copias replicadas de esos objetos y almacene cada copia en un sitio diferente.
- Conserve las dos copias "para siempre", lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que sean eliminados por una solicitud de eliminación del cliente o hasta que expire el ciclo de vida de un depósito.
- Utilice la opción Equilibrado para el comportamiento de ingesta: la instrucción de ubicación de dos sitios se aplica tan pronto como el Inquilino A guarda un objeto en StorageGRID, a menos que no sea posible realizar inmediatamente ambas copias requeridas.

Por ejemplo, si no se puede acceder al Sitio 2 cuando el Inquilino A guarda un objeto, StorageGRID hará dos copias provisionales en los Nodos de almacenamiento del Sitio 1. Tan pronto como el Sitio 2 esté disponible, StorageGRID hará la copia requerida en ese sitio.

Información relacionada

- ["¿Qué es un pool de almacenamiento?"](#)
- ["¿Qué es un pool de almacenamiento en la nube?"](#)

Acceda al asistente para crear una regla ILM

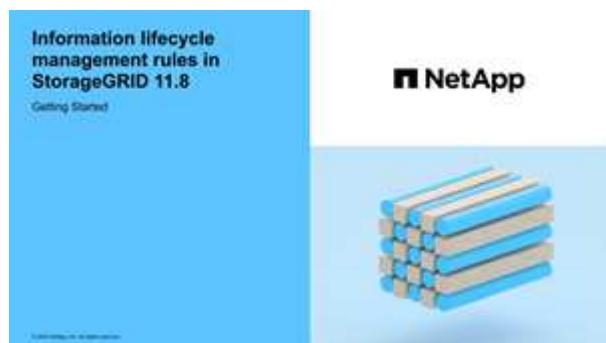
Las reglas ILM le permiten administrar la ubicación de los datos de los objetos a lo largo del tiempo. Para crear una regla ILM, utilice el asistente Crear una regla ILM.



Si desea crear la regla ILM predeterminada para una política, siga las ["Instrucciones para crear una regla ILM predeterminada"](#) en cambio.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Si desea especificar a qué cuentas de inquilino se aplica esta regla, tiene la ["Permiso de cuentas de inquilinos"](#) o conoce el ID de cuenta para cada cuenta.
- Si desea que la regla filtre objetos según los metadatos de la hora del último acceso, las actualizaciones de la hora del último acceso deben estar habilitadas por el bucket S3.
- Ha configurado todos los grupos de almacenamiento en la nube que planea utilizar. Ver ["Crear un grupo de almacenamiento en la nube"](#) .
- Estás familiarizado con el ["opciones de ingesta"](#) .
- Si necesita crear una regla compatible para usarla con S3 Object Lock, está familiarizado con el ["Requisitos para el bloqueo de objetos S3"](#) .
- Opcionalmente has visto el vídeo: ["Vídeo: Resumen de las reglas de ILM"](#) .



Acerca de esta tarea

Al crear reglas ILM:

- Tenga en cuenta la topología y las configuraciones de almacenamiento del sistema StorageGRID .
- Considere qué tipos de copias de objetos desea realizar (replicadas o codificadas por borrado) y la cantidad de copias de cada objeto que se requieren.
- Determinar qué tipos de metadatos de objetos se utilizan en las aplicaciones que se conectan al sistema StorageGRID . Las reglas ILM filtran objetos según sus metadatos.
- Considere dónde desea que se coloquen las copias de objetos a lo largo del tiempo.
- Decide qué opción de ingesta utilizar (equilibrada, estricta o confirmación dual).

Pasos

1. Seleccione **ILM** > **Reglas**.
2. Seleccione **Crear**. ["Paso 1 \(Ingresar detalles\)"](#) Aparece el asistente Crear una regla ILM.

Paso 1 de 3: Ingrese los detalles

El paso **Ingresar detalles** del asistente Crear una regla ILM le permite ingresar un nombre y una descripción para la regla y definir filtros para la regla.

Ingresar una descripción y definir filtros para la regla son opcionales.

Acerca de esta tarea

Al evaluar un objeto frente a un ["Regla ILM"](#) StorageGRID compara los metadatos del objeto con los filtros de

la regla. Si los metadatos del objeto coinciden con todos los filtros, StorageGRID utiliza la regla para colocar el objeto. Puede diseñar una regla para aplicarla a todos los objetos, o puede especificar filtros básicos, como una o más cuentas de inquilino o nombres de depósito, o filtros avanzados, como el tamaño del objeto o los metadatos del usuario.

Pasos

1. Introduzca un nombre único para la regla en el campo **Nombre**.
2. Opcionalmente, ingrese una breve descripción de la regla en el campo **Descripción**.

Debes describir el propósito o función de la regla para poder reconocerla más adelante.

3. Opcionalmente, seleccione una o más cuentas de inquilino S3 a las que se aplica esta regla. Si esta regla se aplica a todos los inquilinos, deje este campo en blanco.

Si no tiene el permiso de acceso de raíz o el permiso de cuentas de inquilino, no podrá seleccionar inquilinos de la lista. En su lugar, ingrese el ID del inquilino o ingrese varios ID como una cadena delimitada por comas.

4. De manera opcional, especifique los buckets S3 a los que se aplica esta regla.

Si se selecciona **se aplica a todos los buckets** (predeterminado), la regla se aplica a todos los buckets S3.

5. Para los inquilinos de S3, seleccione opcionalmente **Sí** para aplicar la regla solo a versiones de objetos más antiguas en depósitos de S3 que tengan habilitada la función de control de versiones.

Si selecciona **Sí**, se seleccionará automáticamente "Hora no actual" para la hora de referencia en ["Paso 2 del asistente para crear una regla ILM"](#).



El tiempo no actual se aplica únicamente a objetos S3 en depósitos con control de versiones habilitado. Ver ["Operaciones en buckets, PutBucketVersioning"](#) y ["Administrar objetos con S3 Object Lock"](#).

Puede utilizar esta opción para reducir el impacto de almacenamiento de los objetos versionados filtrando las versiones de objetos no actuales. Ver ["Ejemplo 4: Reglas y políticas de ILM para objetos versionados de S3"](#).

6. Opcionalmente, seleccione **Agregar un filtro avanzado** para especificar filtros adicionales.

Si no configura el filtrado avanzado, la regla se aplica a todos los objetos que coincidan con los filtros básicos. Para obtener más información sobre el filtrado avanzado, consulte [Utilice filtros avanzados en las reglas de ILM](#) y [Especificar múltiples tipos y valores de metadatos](#).

7. Seleccione **Continuar**. ["Paso 2 \(Definir ubicaciones\)"](#) Aparece el asistente Crear una regla ILM.

Utilice filtros avanzados en las reglas de ILM

El filtrado avanzado le permite crear reglas ILM que se aplican solo a objetos específicos en función de sus metadatos. Cuando configura el filtrado avanzado para una regla, selecciona el tipo de metadatos que desea que coincidan, selecciona un operador y especifica un valor de metadatos. Cuando se evalúan objetos, la regla ILM se aplica solo a aquellos objetos que tienen metadatos que coinciden con el filtro avanzado.

La tabla muestra los tipos de metadatos que puede especificar en los filtros avanzados, los operadores que puede utilizar para cada tipo de metadatos y los valores de metadatos esperados.

Tipo de metadatos	Operadores compatibles	Valor de metadatos
Tiempo de ingesta	• es • no es • es antes • está en o antes • es despues • está en o después	Hora y fecha en que se ingirió el objeto. Nota: Para evitar problemas de recursos al activar una nueva política ILM, puede usar el filtro avanzado Tiempo de ingesta en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de ingesta para que sea mayor o igual al tiempo aproximado en que entrará en vigencia la nueva política para garantizar que los objetos existentes no se muevan innecesariamente.
Llave	• es igual • no es igual • contiene • no contiene • comienza con • no empieza con • termina con • no termina con	Toda o parte de una clave de objeto S3 única. Por ejemplo, es posible que desees hacer coincidir objetos que terminen con <code>.txt</code> o empezar con <code>test-object/</code>.
Hora del último acceso	• es • no es • es antes • está en o antes • es despues • está en o después	Hora y fecha en que se recuperó (leyó o vio) el objeto por última vez. Nota: Si planeas "utilizar la hora del último acceso" Como filtro avanzado, se deben habilitar las actualizaciones de la última hora de acceso para el bucket S3.
Restricción de ubicación (solo S3)	• es igual • no es igual	La región donde se creó un depósito S3. Utilice ILM > Regiones para definir las regiones que se muestran. Nota: Un valor de <code>us-east-1</code> coincidirá con objetos en depósitos creados en la región <code>us-east-1</code>, así como con objetos en depósitos que no tienen ninguna región especificada. Ver "Configurar regiones (opcional y solo S3)".

Tipo de metadatos	Operadores compatibles	Valor de metadatos
Tamaño del objeto	• es igual • no es igual • menos que • menor o igual a • más que • mayor o igual a	El tamaño del objeto. La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.
Metadatos del usuario	• contiene • termina con • es igual • existe • comienza con • no contiene • no termina con • no es igual • no existe • no empieza con	Par clave-valor, donde Nombre de metadatos del usuario es la clave y Valor de metadatos es el valor. Por ejemplo, para filtrar objetos que tienen metadatos de usuario de <code>color=blue</code>, especificar <code>color</code> para Nombre de metadatos de usuario, <code>equals</code> para el operador, y <code>blue</code> para Valor de metadatos. Nota: Los nombres de metadatos del usuario no distinguen entre mayúsculas y minúsculas; los valores de metadatos del usuario sí distinguen entre mayúsculas y minúsculas.
Etiqueta de objeto (solo S3)	• contiene • termina con • es igual • existe • comienza con • no contiene • no termina con • no es igual • no existe • no empieza con	Par clave-valor, donde Nombre de etiqueta de objeto es la clave y Valor de etiqueta de objeto es el valor. Por ejemplo, para filtrar objetos que tienen una etiqueta de objeto de <code>Image=True</code>, especificar <code>Image</code> para Nombre de etiqueta de objeto, <code>equals</code> para el operador, y <code>True</code> para Valor de etiqueta de objeto. Nota: Los nombres de las etiquetas de objeto y los valores de las etiquetas de objeto distinguen entre mayúsculas y minúsculas. Debes ingresar estos elementos exactamente como fueron definidos para el objeto.

Especificar múltiples tipos y valores de metadatos

Al definir el filtrado avanzado, puede especificar múltiples tipos de metadatos y múltiples valores de metadatos. Por ejemplo, si desea que una regla coincida con objetos entre 10 MB y 100 MB de tamaño, deberá seleccionar el tipo de metadatos **Tamaño del objeto** y especificar dos valores de metadatos.

- El primer valor de metadatos especifica objetos mayores o iguales a 10 MB.
- El segundo valor de metadatos especifica objetos menores o iguales a 100 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size	greater than or equal to	10	MB	✕
and				
Object size	less than or equal to	100	MB	✕

El uso de múltiples entradas le permite tener un control preciso sobre qué objetos coinciden. En el siguiente ejemplo, la regla se aplica a los objetos que tienen Marca A o Marca B como valor de los metadatos de usuario `camera_type`. Sin embargo, la regla sólo se aplica a aquellos objetos de la marca B que tengan un tamaño inferior a 10 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

User metadata	camera_type	equals	Brand A	✕

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule: ✕

User metadata	camera_type	equals	Brand B	✕
and				
Object size	less than or equal to	10	MB	✕

[Add another advanced filter](#)

Paso 2 de 3: Definir ubicaciones

El paso **Definir ubicaciones** del asistente Crear regla ILM le permite definir las instrucciones de ubicación que determinan durante cuánto tiempo se almacenan los objetos, el tipo de copias (replicadas o con código de borrado), la ubicación de almacenamiento y la cantidad de copias.



Las capturas de pantalla que se muestran son ejemplos. Los resultados pueden variar según la versión de StorageGRID .

Acerca de esta tarea

Una regla ILM puede incluir una o más instrucciones de ubicación. Cada instrucción de colocación se aplica a un único período de tiempo. Cuando se utiliza más de una instrucción, los períodos de tiempo deben ser contiguos y al menos una instrucción debe comenzar el día 0. Las instrucciones pueden continuar indefinidamente o hasta que ya no necesite ninguna copia de objeto.

Cada instrucción de ubicación puede tener varias líneas si desea crear diferentes tipos de copias o utilizar diferentes ubicaciones durante ese período de tiempo.

En este ejemplo, la regla ILM almacena una copia replicada en el Sitio 1 y una copia replicada en el Sitio 2 durante el primer año. Después de un año, se realiza una copia con código de borrado 2+1 y se guarda en un solo sitio.

Pasos

1. Para **Hora de referencia**, seleccione el tipo de hora que se utilizará al calcular la hora de inicio de una instrucción de ubicación.

Opción	Descripción
Tiempo de ingesta	El momento en que se ingirió el objeto.
Hora del último acceso	La hora en que se recuperó el objeto por última vez (se leyó o se vio). Para utilizar esta opción, las actualizaciones de la hora del último acceso deben estar habilitadas para el bucket S3. Consulte "Utilice la hora del último acceso en las reglas de ILM" .
Hora de creación definida por el usuario	Un tiempo especificado en metadatos definidos por el usuario.
Tiempo no actual	"Hora no actual" se selecciona automáticamente si seleccionó Sí para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en buckets S3 con control de versiones habilitado)?" en "Paso 1 del asistente para crear una regla de ILM" .

Si desea crear una regla *compatible*, debe seleccionar **Tiempo de ingesta**. Consulte ["Administrar objetos con S3 Object Lock"](#) .

2. En la sección **Período de tiempo y ubicaciones**, ingrese una hora de inicio y una duración para el primer período de tiempo.

Por ejemplo, es posible que desee especificar dónde almacenar los objetos durante el primer año (*Desde el día 0 almacenar durante 365 días*). Al menos una instrucción debe comenzar en el día 0.

3. Si desea crear copias replicadas:
 - a. En la lista desplegable **Almacenar objetos por**, seleccione **replicando**.
 - b. Seleccione el número de copias que desea realizar.

Aparece una advertencia si cambia el número de copias a 1. Una regla ILM que crea solo una copia replicada por cada período de tiempo pone los datos en riesgo de pérdida permanente. Consulte ["Por qué no debería utilizar la replicación de copia única"](#) .

Para evitar el riesgo, realice una o más de las siguientes acciones:

- Aumentar el número de copias para el período de tiempo.
- Agregue copias a otros grupos de almacenamiento o a un grupo de almacenamiento en la nube.
- Seleccione **codificación de borrado** en lugar de **replicación**.

Puede ignorar esta advertencia de forma segura si esta regla ya crea múltiples copias para todos los períodos de tiempo.

- c. En el campo **copias en**, seleccione los grupos de almacenamiento que desea agregar.

Si especifica solo un grupo de almacenamiento, tenga en cuenta que StorageGRID solo puede

almacenar una copia replicada de un objeto en cualquier nodo de almacenamiento determinado. Si su red incluye tres nodos de almacenamiento y selecciona 4 como número de copias, solo se realizarán tres copias: una copia para cada nodo de almacenamiento.

La alerta **Colocación ILM inalcanzable** se activa para indicar que la regla ILM no se pudo aplicar por completo.

Si especifica más de un grupo de almacenamiento, tenga en cuenta estas reglas:

- La cantidad de copias no puede ser mayor que la cantidad de grupos de almacenamiento.
- Si la cantidad de copias es igual a la cantidad de grupos de almacenamiento, se almacena una copia del objeto en cada grupo de almacenamiento.
- Si la cantidad de copias es menor que la cantidad de grupos de almacenamiento, se almacena una copia en el sitio de ingesta y luego el sistema distribuye las copias restantes para mantener equilibrado el uso del disco entre los grupos y, al mismo tiempo, garantizar que ningún sitio obtenga más de una copia de un objeto.
- Si los grupos de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), todas las copias del objeto podrían guardarse en un solo sitio. Por este motivo, no especifique el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) y otro grupo de almacenamiento.

4. Si desea crear una copia con código de borrado:

a. En la lista desplegable **Almacenar objetos por**, seleccione **codificación de borrado**.



La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

b. Si no agregó un filtro de tamaño de objeto para un valor mayor a 200 KB, seleccione **Anterior** para regresar al Paso 1. Luego, seleccione **Agregar un filtro avanzado** y configure un filtro de **Tamaño de objeto** en cualquier valor mayor a 200 KB.

c. Seleccione el grupo de almacenamiento que desea agregar y el esquema de codificación de borrado que desea utilizar.

La ubicación de almacenamiento de una copia con código de borrado incluye el nombre del esquema de codificación de borrado, seguido del nombre del grupo de almacenamiento.

Los esquemas de codificación de borrado disponibles están limitados por la cantidad de nodos de almacenamiento en el grupo de almacenamiento que seleccione. A Recommended La insignia aparece junto a los esquemas que proporcionan el "[La mejor protección o la menor sobrecarga de almacenamiento](#)".

5. Opcionalmente:

- a. Seleccione **Agregar otro tipo o ubicación** para crear copias adicionales en diferentes ubicaciones.
- b. Seleccione **Agregar otro período de tiempo** para agregar diferentes períodos de tiempo.

Las eliminaciones de objetos se producen según las siguientes configuraciones:



- Los objetos se eliminan automáticamente al final del período de tiempo final, a menos que otro período de tiempo finalice **para siempre**.
- Dependiendo de "[Configuración del período de retención de depósitos e inquilinos](#)" Es posible que los objetos no se eliminen incluso si finaliza el período de retención de ILM.

6. Si desea almacenar objetos en un grupo de almacenamiento en la nube:

- a. En la lista desplegable **Almacenar objetos por**, seleccione **replicando**.
- b. Seleccione el campo **copias en** y luego seleccione un grupo de almacenamiento en la nube.

Al utilizar grupos de almacenamiento en la nube, tenga en cuenta estas reglas:

- No puede seleccionar más de un grupo de almacenamiento en la nube en una sola instrucción de ubicación. De manera similar, no es posible seleccionar un grupo de almacenamiento en la nube y un grupo de almacenamiento en la misma instrucción de ubicación.
- Solo puedes almacenar una copia de un objeto en un grupo de almacenamiento en la nube determinado. Aparece un mensaje de error si configura **Copias** en 2 o más.
- No es posible almacenar más de una copia de objeto en ningún grupo de almacenamiento en la nube al mismo tiempo. Aparece un mensaje de error si varias ubicaciones que utilizan un grupo de almacenamiento en la nube tienen fechas superpuestas o si varias líneas en la misma ubicación utilizan un grupo de almacenamiento en la nube.
- Puede almacenar un objeto en un grupo de almacenamiento en la nube al mismo tiempo que ese objeto se almacena como copias replicadas o con código de borrado en StorageGRID. Sin embargo, debe incluir más de una línea en la instrucción de ubicación para el período de tiempo, de modo que pueda especificar la cantidad y los tipos de copias para cada ubicación.

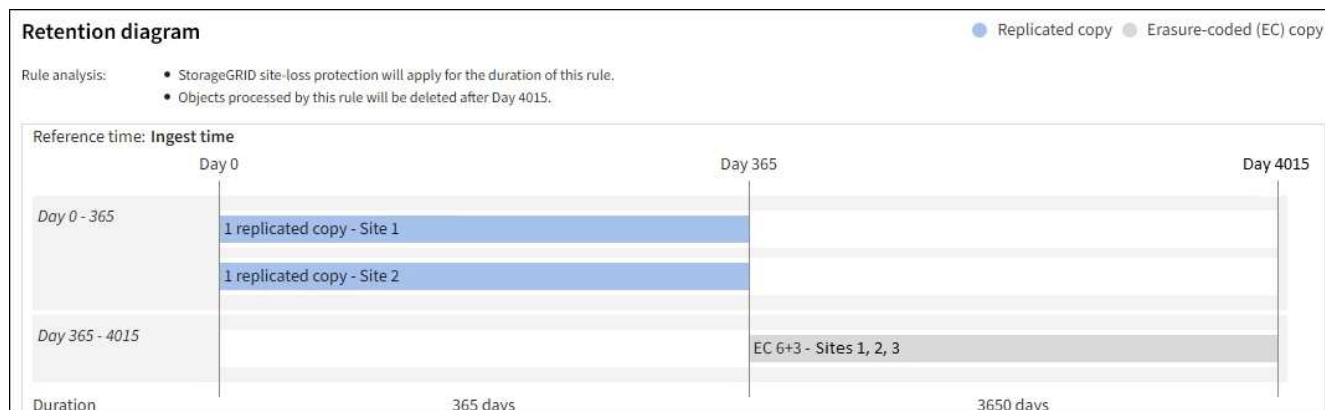
7. En el diagrama de retención, confirme sus instrucciones de ubicación.

En este ejemplo, la regla ILM almacena una copia replicada en el Sitio 1 y una copia replicada en el Sitio 2 durante el primer año. Después de un año y durante 10 años más, se guardará una copia con código de borrado 6+3 en tres sitios. Después de 11 años en total, los objetos se eliminarán de StorageGRID.

La sección de análisis de reglas del diagrama de retención establece:

- La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
- Los objetos procesados por esta regla se eliminarán después del día 4015.

Consulte "[Habilitar la protección contra pérdida del sitio.](#)"



8. Seleccione **Continuar**. "[Paso 3 \(Seleccionar el comportamiento de ingesta\)](#)" Aparece el asistente Crear una regla ILM.

Utilice la hora del último acceso en las reglas de ILM

Puede utilizar la hora del último acceso como hora de referencia en una regla ILM. Por ejemplo, es posible que desee dejar objetos que se hayan visto en los últimos tres meses en nodos de almacenamiento locales, mientras que mueve objetos que no se hayan visto recientemente a una ubicación externa. También puede utilizar Hora del último acceso como filtro avanzado si desea que una regla ILM se aplique solo a los objetos a los que se accedió por última vez en una fecha específica.

Acerca de esta tarea

Antes de utilizar la hora del último acceso en una regla ILM, revise las siguientes consideraciones:

- Al utilizar la hora del último acceso como tiempo de referencia, tenga en cuenta que cambiar la hora del último acceso de un objeto no activa una evaluación ILM inmediata. En su lugar, se evalúan las ubicaciones del objeto y el objeto se mueve según sea necesario cuando ILM en segundo plano evalúa el objeto. Esto podría tomar dos semanas o más después de acceder al objeto.

Tenga en cuenta esta latencia al crear reglas ILM basadas en el último tiempo de acceso y evite ubicaciones que utilicen períodos de tiempo cortos (menos de un mes).

- Al utilizar la Hora del último acceso como filtro avanzado o como hora de referencia, debe habilitar las actualizaciones de la Hora del último acceso para los buckets S3. Puedes utilizar el "[Administrador de inquilinos](#)" o el "[API de gestión de inquilinos](#)".



Las actualizaciones del último tiempo de acceso están deshabilitadas de manera predeterminada para los buckets S3.



Tenga en cuenta que habilitar actualizaciones de la última hora de acceso puede reducir el rendimiento, especialmente en sistemas con objetos pequeños. El impacto en el rendimiento se produce porque StorageGRID debe actualizar los objetos con nuevas marcas de tiempo cada vez que se recuperan los objetos.

La siguiente tabla resume si la hora del último acceso se actualiza para todos los objetos en el depósito para diferentes tipos de solicitudes.

Tipo de solicitud	Si la hora del último acceso se actualiza cuando las actualizaciones de la hora del último acceso están deshabilitadas	Si la hora del último acceso se actualiza cuando se habilitan las actualizaciones de la hora del último acceso
Solicitud para recuperar un objeto, su lista de control de acceso o sus metadatos	No	Sí
Solicitud para actualizar los metadatos de un objeto	Sí	Sí
Solicitud para copiar un objeto de un depósito a otro	• No, para la copia fuente • Sí, para la copia de destino	• Sí, para la copia fuente • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Paso 3 de 3: Seleccionar el comportamiento de ingesta

El paso **Seleccionar comportamiento de ingesta** del asistente Crear regla de ILM le permite elegir cómo se protegen los objetos filtrados por esta regla a medida que se ingieren.

Acerca de esta tarea

StorageGRID puede hacer copias provisionales y poner en cola los objetos para una evaluación ILM posterior, o puede hacer copias para cumplir con las instrucciones de ubicación de la regla de inmediato.

Pasos

1. Seleccione el ["comportamiento de ingestión"](#) Para utilizar.

Para obtener más información, consulte ["Ventajas, desventajas y limitaciones de las opciones de ingesta"](#).



No puedes usar la opción Equilibrado o Estricto si la regla utiliza una de estas ubicaciones:

- Un grupo de almacenamiento en la nube en el día 0
- Un grupo de almacenamiento en la nube cuando la regla utiliza un tiempo de creación definido por el usuario como tiempo de referencia

Ver ["Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto"](#).

2. Seleccione **Crear**.

Se crea la regla ILM. La regla no se activa hasta que se agrega a una ["Política de ILM"](#) y esa política se activa.

Para ver los detalles de la regla, seleccione el nombre de la regla en la página de reglas de ILM.

Crear una regla ILM predeterminada

Antes de crear una política ILM, debe crear una regla predeterminada para colocar cualquier objeto que no coincida con otra regla en la política. La regla predeterminada no puede utilizar ningún filtro. Debe aplicarse a todos los inquilinos, todos los depósitos y todas las versiones de objetos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).

Acerca de esta tarea

La regla predeterminada es la última regla que se evalúa en una política ILM, por lo que no puede usar ningún filtro. Las instrucciones de ubicación de la regla predeterminada se aplican a cualquier objeto que no coincida con otra regla en la política.

En esta política de ejemplo, la primera regla se aplica solo a los objetos que pertenecen a test-tenant-1. La regla predeterminada, que es la última, se aplica a los objetos que pertenecen a todas las demás cuentas de inquilino.

Proposed policy name

Example ILM policy

Reason for change

Example

Manage rules

1. Select the rules you want to add to the policy.

2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	↕ EC for test-tenant-1	Tenant is test-tenant-1
Default	Default rule	—

Al crear la regla predeterminada, tenga en cuenta estos requisitos:

- La regla predeterminada se colocará automáticamente como última regla cuando la agregue a una política.
- La regla predeterminada no puede utilizar ningún filtro básico o avanzado.
- La regla predeterminada debe aplicarse a todas las versiones del objeto.
- La regla predeterminada debería crear copias replicadas.



No utilice una regla que cree copias con código de borrado como regla predeterminada para una política. Las reglas de codificación de borrado deben utilizar un filtro avanzado para evitar que se codifiquen por borrado objetos más pequeños.

- En general, la regla predeterminada debería conservar los objetos para siempre.
- Si está utilizando (o planea habilitar) la configuración global de bloqueo de objetos S3, la regla predeterminada debe ser compatible.

Pasos

1. Seleccione **ILM > Reglas**.
2. Seleccione **Crear**.

Aparece el paso 1 (Ingresar detalles) del asistente Crear regla ILM.

3. Introduzca un nombre único para la regla en el campo **Nombre de la regla**.
4. Opcionalmente, ingrese una breve descripción de la regla en el campo **Descripción**.
5. Deje el campo **Cuentas de inquilinos** en blanco.

La regla predeterminada debe aplicarse a todas las cuentas de inquilinos.

6. Deje la selección desplegable del nombre del depósito como **se aplica a todos los depósitos**.

La regla predeterminada debe aplicarse a todos los buckets S3.

7. Mantenga la respuesta predeterminada, **No**, para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?"
8. No agregue filtros avanzados.

La regla predeterminada no puede especificar ningún filtro.

9. Seleccione **Siguiente**.

Aparece el paso 2 (Definir ubicaciones).

10. Para el tiempo de referencia, seleccione cualquier opción.

Si mantuvo la respuesta predeterminada, **No**, para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores?" La hora no actual no se incluirá en la lista desplegable. La regla predeterminada debe aplicarse a todas las versiones del objeto.

11. Especifique las instrucciones de ubicación para la regla predeterminada.
 - La regla predeterminada debería conservar los objetos para siempre. Aparece una advertencia cuando se activa una nueva política si la regla predeterminada no retiene los objetos para siempre. Debes confirmar que este es el comportamiento que esperas.
 - La regla predeterminada debería crear copias replicadas.



No utilice una regla que cree copias con código de borrado como regla predeterminada para una política. Las reglas de codificación de borrado deben incluir el filtro avanzado **Tamaño de objeto (MB) mayor a 200 KB** para evitar que se codifiquen objetos más pequeños.

- Si está utilizando (o planea habilitar) la configuración global de Bloqueo de objetos S3, la regla predeterminada debe ser compatible:
 - Debe crear al menos dos copias del objeto replicado o una copia con código de borrado.
 - Estas copias deben existir en los nodos de almacenamiento durante toda la duración de cada línea en las instrucciones de ubicación.
 - Las copias de objetos no se pueden guardar en un grupo de almacenamiento en la nube.
 - Al menos una línea de las instrucciones de ubicación debe comenzar en el día 0, utilizando el tiempo de ingesta como tiempo de referencia.
 - Al menos una línea de las instrucciones de colocación debe ser "para siempre".

12. Mire el diagrama de retención para confirmar sus instrucciones de ubicación.

13. Seleccione **Continuar**.

Aparece el paso 3 (Seleccionar comportamiento de ingesta).

14. Seleccione la opción de ingesta que desea utilizar y seleccione **Crear**.

Administrar políticas de ILM

Utilice las políticas de ILM

Una política de gestión del ciclo de vida de la información (ILM) es un conjunto ordenado de reglas ILM que determina cómo el sistema StorageGRID gestiona los datos de los objetos a lo largo del tiempo.



Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irreparable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

Política ILM predeterminada

Cuando instala StorageGRID y agrega sitios, se crea automáticamente una política ILM predeterminada, de la siguiente manera:

- Si su cuadrícula contiene un sitio, la política predeterminada contiene una regla predeterminada que replica dos copias de cada objeto en ese sitio.
- Si su cuadrícula contiene más de un sitio, la regla predeterminada replica una copia de cada objeto en cada sitio.

Si la política predeterminada no cumple con sus requisitos de almacenamiento, puede crear sus propias reglas y políticas. Ver ["Crear una regla ILM"](#) y ["Crear una política ILM"](#).

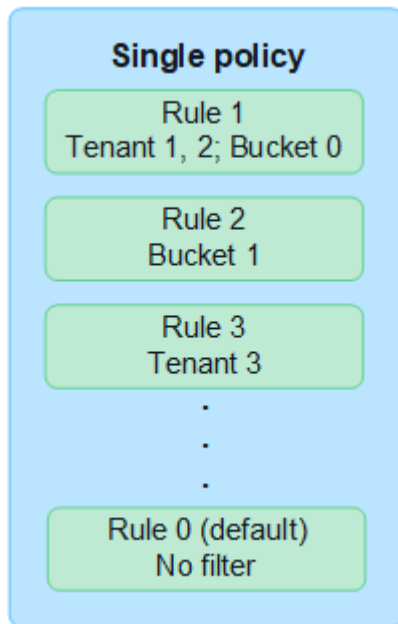
¿Una o varias políticas ILM activas?

Puede tener una o más políticas ILM activas a la vez.

Una política

Si su red utilizará un esquema de protección de datos simple con pocas reglas específicas para cada inquilino y cada depósito, utilice una única política ILM activa. Las reglas de ILM pueden contener filtros para

administrar diferentes grupos o inquilinos.



Cuando solo tiene una política y cambian los requisitos de un inquilino, debe crear una nueva política ILM o clonar la política existente para aplicar los cambios, simular y luego activar la nueva política ILM. Los cambios en la política de ILM podrían generar movimientos de objetos que podrían demorar muchos días y causar latencia del sistema.

Múltiples políticas

Para brindar diferentes opciones de calidad de servicio a los inquilinos, puede tener más de una política activa a la vez. Cada política puede administrar inquilinos, depósitos S3 y objetos específicos. Cuando se aplica o cambia una política para un conjunto específico de inquilinos u objetos, las políticas aplicadas a otros inquilinos y objetos no se ven afectadas.

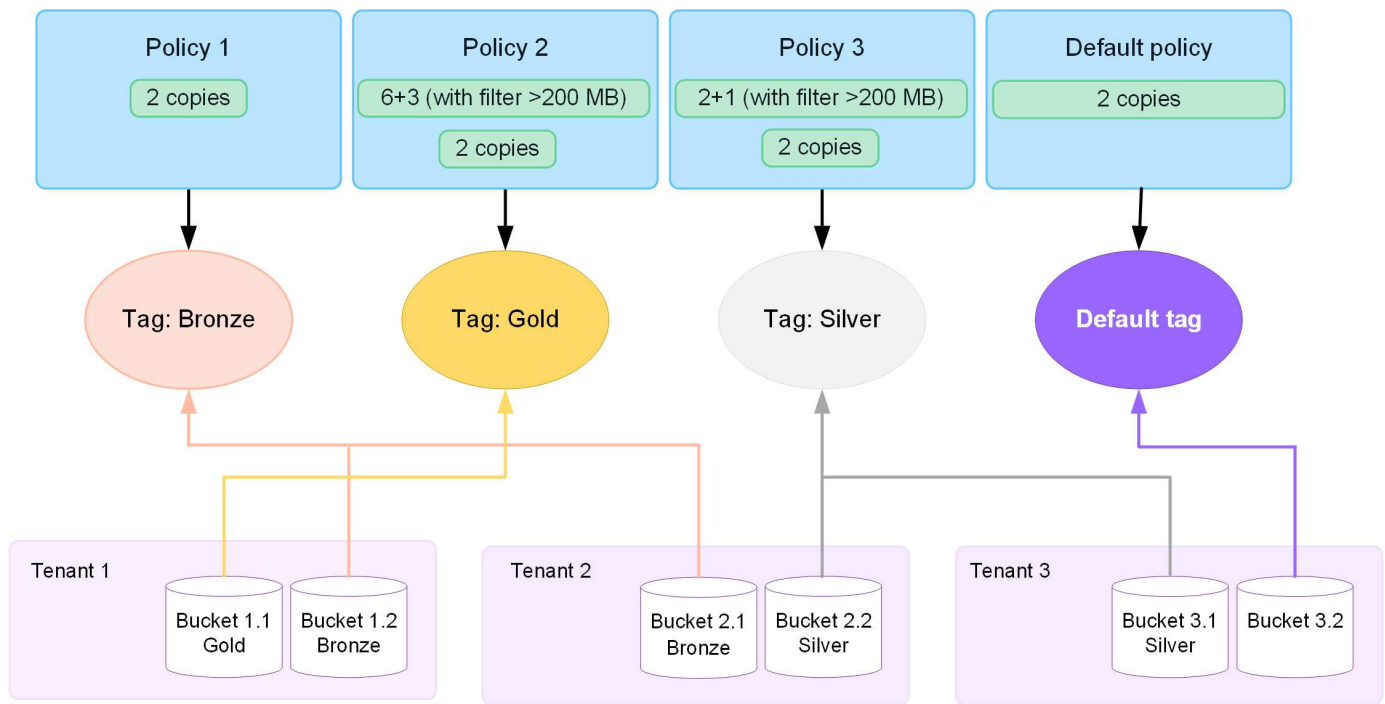
Etiquetas de política de ILM

Si desea permitir que los inquilinos cambien fácilmente entre múltiples políticas de protección de datos por depósito, utilice múltiples políticas ILM con *etiquetas de política ILM*. Asigna cada política de ILM a una etiqueta y luego los inquilinos etiquetan un depósito para aplicar la política a ese depósito. Puede configurar etiquetas de política ILM solo en depósitos S3.

Por ejemplo, podría tener tres etiquetas denominadas Oro, Plata y Bronce. Puede asignar una política ILM a cada etiqueta, en función de cuánto tiempo y dónde esa política almacena los objetos. Los inquilinos pueden elegir qué política utilizar etiquetando sus áreas. Un depósito etiquetado como Oro es administrado por la política Oro y recibe el nivel Oro de protección de datos y rendimiento.

Etiqueta de política ILM predeterminada

Se crea automáticamente una etiqueta de política ILM predeterminada cuando instala StorageGRID. Cada cuadrícula debe tener una política activa asignada a la etiqueta Predeterminada. La política predeterminada se aplica a cualquier depósito S3 sin etiquetar.



¿Cómo evalúa una política ILM los objetos?

Una política ILM activa controla la ubicación, la duración y la protección de datos de los objetos.

Cuando los clientes guardan objetos en StorageGRID, los objetos se evalúan en función del conjunto ordenado de reglas ILM en la política, de la siguiente manera:

1. Si los filtros de la primera regla de la política coinciden con un objeto, el objeto se ingiere de acuerdo con el comportamiento de ingesta de esa regla y se almacena de acuerdo con las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, este se evalúa en relación con cada regla posterior de la política hasta que se encuentre una coincidencia.
3. Si ninguna regla coincide con un objeto, se aplican el comportamiento de ingesta y las instrucciones de ubicación de la regla predeterminada en la política. La regla predeterminada es la última regla de una política. La regla predeterminada debe aplicarse a todos los inquilinos, todos los depósitos S3 y todas las versiones de objetos, y no puede usar ningún filtro avanzado.

Ejemplo de política ILM

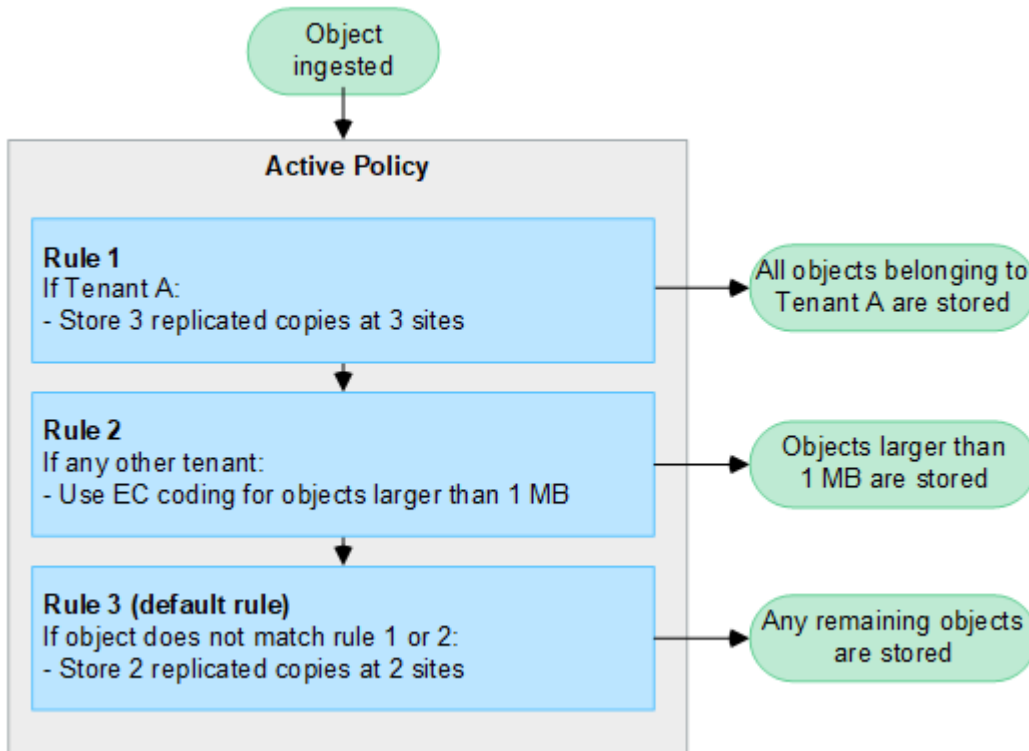
A modo de ejemplo, una política ILM podría contener tres reglas ILM que especifiquen lo siguiente:

- **Regla 1: Copias replicadas para el inquilino A**
 - Empareja todos los objetos que pertenecen al inquilino A.
 - Almacene estos objetos como tres copias replicadas en tres sitios.
 - Los objetos que pertenecen a otros inquilinos no coinciden con la Regla 1, por lo que se evalúan según la Regla 2.
- **Regla 2: Codificación de borrado para objetos mayores a 1 MB**
 - Coincide con todos los objetos de otros inquilinos, pero solo si son mayores a 1 MB. Estos objetos más grandes se almacenan utilizando codificación de borrado 6+3 en tres sitios.
 - No coincide con objetos de 1 MB o más pequeños, por lo que estos objetos se evalúan según la Regla

3.

- **Regla 3: 2 copias, 2 centros de datos** (predeterminado)

- Es la última regla predeterminada de la política. No utiliza filtros.
- Realice dos copias replicadas de todos los objetos que no coincidan con la Regla 1 o la Regla 2 (objetos que no pertenecen al Inquilino A y que tienen 1 MB o menos).



¿Qué son las políticas activas e inactivas?

Cada sistema StorageGRID debe tener al menos una política ILM activa. Si desea tener más de una política ILM activa, cree etiquetas de política ILM y asigne una política a cada etiqueta. Luego, los inquilinos aplican etiquetas a los depósitos S3. La política predeterminada se aplica a todos los objetos en depósitos que no tienen una etiqueta de política asignada.

Cuando crea por primera vez una política ILM, selecciona una o más reglas ILM y las organiza en un orden específico. Después de haber simulado la política para confirmar su comportamiento, actívela.

Cuando activa una política ILM, StorageGRID utiliza esa política para administrar todos los objetos, incluidos los objetos existentes y los objetos recientemente ingeridos. Los objetos existentes podrían trasladarse a nuevas ubicaciones cuando se implementen las reglas ILM en la nueva política.

Si activa más de una política ILM a la vez y los inquilinos aplican etiquetas de política a los depósitos S3, los objetos en cada depósito se administran de acuerdo con la política asignada a la etiqueta.

Un sistema StorageGRID rastrea el historial de políticas que se han activado o desactivado.

Consideraciones para la creación de una política ILM

- Utilice únicamente la política proporcionada por el sistema (política Baseline 2 copias) en los sistemas de prueba. Para StorageGRID 11.6 y versiones anteriores, la regla Hacer 2 copias en esta política utiliza el grupo de almacenamiento Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el

mismo sitio.



El grupo de almacenamiento Todos los nodos de almacenamiento se crea automáticamente durante la instalación de StorageGRID 11.6 y versiones anteriores. Si actualiza a una versión posterior de StorageGRID, el grupo de todos los nodos de almacenamiento seguirá existiendo. Si instala StorageGRID 11.7 o posterior como una instalación nueva, no se crea el grupo Todos los nodos de almacenamiento.

- Al diseñar una nueva política, tenga en cuenta todos los diferentes tipos de objetos que podrían incorporarse a su red. Asegúrese de que la política incluya reglas para hacer coincidir y colocar estos objetos según sea necesario.
- Mantenga la política de ILM lo más simple posible. Esto evita situaciones potencialmente peligrosas en las que los datos de los objetos no están protegidos como se espera cuando se realizan cambios en el sistema StorageGRID a lo largo del tiempo.
- Asegúrese de que las reglas de la política estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan mediante las reglas en el orden enumerado, comenzando desde arriba. Por ejemplo, si la primera regla de una política coincide con un objeto, ese objeto no será evaluado por ninguna otra regla.
- La última regla en cada política ILM es la regla ILM predeterminada, que no puede usar ningún filtro. Si un objeto no ha sido emparejado con otra regla, la regla predeterminada controla dónde se coloca ese objeto y durante cuánto tiempo se conserva.
- Antes de activar una nueva política, revise cualquier cambio que la política esté realizando en la ubicación de los objetos existentes. Cambiar la ubicación de un objeto existente puede generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

Crear políticas ILM

Cree una o más políticas ILM para satisfacer sus requisitos de calidad de servicio.

Tener una política ILM activa le permite aplicar las mismas reglas ILM a todos los inquilinos y grupos.

Tener múltiples políticas ILM activas le permite aplicar las reglas ILM adecuadas a inquilinos y grupos específicos para cumplir con múltiples requisitos de calidad de servicio.

Crear una política ILM

Acerca de esta tarea

Antes de crear su propia política, verifique que la [política ILM predeterminada](#) no cumple con sus requisitos de almacenamiento.



Utilice únicamente las políticas proporcionadas por el sistema, 2 copias de la política (para redes de un sitio) o 1 copia por sitio (para redes de varios sitios), en los sistemas de prueba. Para StorageGRID 11.6 y versiones anteriores, la regla predeterminada en esta política utiliza el grupo de almacenamiento Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.



Si el ["Se ha habilitado la configuración global de bloqueo de objetos S3"](#), debe asegurarse de que la política ILM cumpla con los requisitos de los depósitos que tienen habilitado el bloqueo de objetos S3. En esta sección, siga las instrucciones que mencionan tener habilitado el bloqueo de objetos S3.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["permisos de acceso necesarios"](#) .
- Tienes ["creó reglas ILM"](#) dependiendo de si el bloqueo de objetos S3 está habilitado.

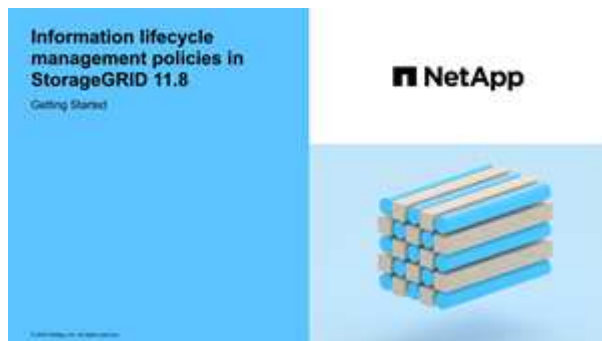
Bloqueo de objetos S3 no habilitado

- Tienes ["creó las reglas de ILM"](#) desea agregar a la política. Según sea necesario, puede guardar una política, crear reglas adicionales y luego editar la política para agregar las nuevas reglas.
- Tienes ["creó una regla ILM predeterminada"](#) que no contiene ningún filtro.

Bloqueo de objetos S3 habilitado

- El ["La configuración global de bloqueo de objetos S3 ya está habilitada"](#) para el sistema StorageGRID .
- Tienes ["creó las reglas ILM compatibles y no compatibles"](#) desea agregar a la política. Según sea necesario, puede guardar una política, crear reglas adicionales y luego editar la política para agregar las nuevas reglas.
- Tienes ["creó una regla ILM predeterminada"](#) para la política que se cumple.

- Opcionalmente has visto el vídeo: ["Vídeo: Resumen de las políticas de ILM"](#)



Consulte también ["Utilice las políticas de ILM"](#) .

Pasos

1. Seleccione **ILM > Políticas**.

Si la configuración global de Bloqueo de objetos S3 está habilitada, la página de políticas de ILM indica qué reglas de ILM son compatibles.

2. Determine cómo desea crear la política ILM.

Crear nueva política

- a. Seleccione **Crear política**.

Clonar política existente

- a. Seleccione la casilla de verificación de la política con la que desea comenzar y luego seleccione **Clonar**.

Editar la política existente

- a. Si una política está inactiva, puedes editarla. Seleccione la casilla de verificación de la política inactiva con la que desea comenzar y luego seleccione **Editar**.

3. En el campo **Nombre de la política**, ingrese un nombre único para la política.
4. Opcionalmente, en el campo **Motivo del cambio**, ingrese el motivo por el cual está creando una nueva política.
5. Para agregar reglas a la política, seleccione **Seleccionar reglas**. Seleccione un nombre de regla para ver la configuración de esa regla.

Si está clonando una política:

- Se seleccionan las reglas utilizadas por la política que estás clonando.
- Si la política que está clonando utilizó reglas sin filtros que no eran la regla predeterminada, se le solicitará que elimine todas esas reglas excepto una.
- Si la regla predeterminada utilizó un filtro, se le solicitará que seleccione una nueva regla predeterminada.
- Si la regla predeterminada no fue la última regla, puede mover la regla al final de la nueva política.

Bloqueo de objetos S3 no habilitado

- a. Seleccione una regla predeterminada para la política. Para crear una nueva regla predeterminada, seleccione **Página de reglas ILM**.

La regla predeterminada se aplica a cualquier objeto que no coincida con otra regla de la política. La regla predeterminada no puede usar ningún filtro y siempre se evalúa en último lugar.



No utilice la regla Hacer 2 copias como regla predeterminada para una política. La regla Hacer 2 copias utiliza un único grupo de almacenamiento, Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

Bloqueo de objetos S3 habilitado

- a. Seleccione una regla predeterminada para la política. Para crear una nueva regla predeterminada, seleccione **Página de reglas ILM**.

La lista de reglas contiene solo las reglas que cumplen los requisitos y no utilizan ningún filtro.



No utilice la regla Hacer 2 copias como regla predeterminada para una política. La regla Hacer 2 copias utiliza un único grupo de almacenamiento, Todos los nodos de almacenamiento, que contiene todos los sitios. Si utiliza esta regla, es posible que se coloquen varias copias de un objeto en el mismo sitio.

- b. Si necesita una regla "predeterminada" diferente para los objetos en depósitos S3 no compatibles, seleccione **Incluir una regla sin filtros para depósitos S3 no compatibles** y seleccione una regla no compatible que no use un filtro.

Por ejemplo, es posible que desee utilizar un grupo de almacenamiento en la nube para almacenar objetos en depósitos que no tengan habilitado el bloqueo de objetos S3.



Solo puede seleccionar una regla no compatible que no utilice un filtro.

Consulte también ["Ejemplo 7: Política ILM compatible con el bloqueo de objetos S3"](#) .

6. Cuando haya terminado de seleccionar la regla predeterminada, seleccione **Continuar**.
7. Para el paso Otras reglas, seleccione cualquier otra regla que desee agregar a la política. Estas reglas utilizan al menos un filtro (cuenta de inquilino, nombre del depósito, filtro avanzado o tiempo de referencia no actual). Luego seleccione **Seleccionar**.

La ventana Crear una política ahora enumera las reglas que seleccionó. La regla predeterminada está al final, con las demás reglas encima.

Si el bloqueo de objetos S3 está habilitado y también seleccionó una regla "predeterminada" no compatible, esa regla se agrega como la segunda a la última regla en la política.



Aparece una advertencia si alguna regla no retiene los objetos para siempre. Cuando activa esta política, debe confirmar que desea que StorageGRID elimine objetos cuando transcurran las instrucciones de ubicación de la regla predeterminada (a menos que un ciclo de vida de depósito conserve los objetos durante un período de tiempo más prolongado).

8. Arrastre las filas de las reglas no predeterminadas para determinar el orden en que se evaluarán estas reglas.

No puedes mover la regla predeterminada. Si el bloqueo de objetos S3 está habilitado, tampoco podrá mover la regla "predeterminada" no compatible si se seleccionó una.



Debes confirmar que las reglas de ILM estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan mediante las reglas en el orden enumerado, comenzando desde arriba.

9. Según sea necesario, seleccione **Seleccionar reglas** para agregar o eliminar reglas.
10. Cuando haya terminado, seleccione **Guardar**.
11. Repita estos pasos para crear políticas ILM adicionales.
12. [Simular una política ILM](#) . Siempre debe simular una política antes de activarla para asegurarse de que funcione como se espera.

Simular una política

Simule una política en objetos de prueba antes de activarla y aplicarla a sus datos de producción.

Antes de empezar

- Conoces la clave de objeto/depósito S3 para cada objeto que deseas probar.

Pasos

1. Usando un cliente S3 o el "[Consola S3](#)" , ingerir los objetos necesarios para probar cada regla.
2. En la página de políticas de ILM, seleccione la casilla de verificación de la política y luego seleccione **Simular**.
3. En el campo **Objeto**, ingrese el S3 bucket/object-key para un objeto de prueba. Por ejemplo, bucket-01/filename.png .
4. Si el control de versiones S3 está habilitado, ingrese opcionalmente un ID de versión para el objeto en el campo **ID de versión**.
5. Seleccione **Simular**.
6. En la sección Resultados de simulación, confirme que cada objeto coincidió con la regla correcta.
7. Para determinar qué grupo de almacenamiento o perfil de codificación de borrado está en vigor, seleccione el nombre de la regla coincidente para ir a la página de detalles de la regla.



Revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente puede generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

Resultados

Cualquier modificación a las reglas de la política se reflejará en los resultados de la simulación y mostrará el nuevo partido y el partido anterior. La ventana de política Simular conserva los objetos que probó hasta que

seleccione **Borrar todo** o el ícono de eliminar  para cada objeto en la lista de resultados de simulación.

Información relacionada

["Ejemplo de simulaciones de políticas de ILM"](#)

Activar una política

Cuando se activa una única política ILM nueva, los objetos existentes y los objetos recientemente ingeridos son administrados por esa política. Cuando se activan varias políticas, las etiquetas de política ILM asignadas a los depósitos determinan los objetos que se deben administrar.

Antes de activar una nueva política:

1. Simule la política para confirmar que se comporta como espera.
2. Revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes.
Cambiar la ubicación de un objeto existente puede generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.



Los errores en una política ILM pueden provocar una pérdida de datos irrecuperable.

Acerca de esta tarea

Cuando se activa una política ILM, el sistema distribuye la nueva política a todos los nodos. Sin embargo, es posible que la nueva política activa no entre en vigor hasta que todos los nodos de la red estén disponibles para recibirla. En algunos casos, el sistema espera para implementar una nueva política activa para garantizar que los objetos de la cuadrícula no se eliminen accidentalmente. Específicamente:

- Si realiza cambios de política que **aumentan la redundancia o durabilidad de los datos**, esos cambios se implementan de inmediato. Por ejemplo, si activa una nueva política que incluye una regla de tres copias en lugar de una regla de dos copias, esa política se implementará de inmediato porque aumenta la redundancia de datos.
- Si realiza cambios de política que **podrían disminuir la redundancia o durabilidad de los datos**, dichos cambios no se implementarán hasta que todos los nodos de la red estén disponibles. Por ejemplo, si activa una nueva política que utiliza una regla de dos copias en lugar de una regla de tres copias, la nueva política aparecerá en la pestaña Política activa, pero no tendrá efecto hasta que todos los nodos estén en línea y disponibles.

Pasos

Siga los pasos para activar una o varias políticas:

Activar una política

Siga estos pasos si solo tendrá una política activa. Si ya tiene una o más políticas activas y está activando políticas adicionales, siga los pasos para activar varias políticas.

1. Cuando esté listo para activar una política, seleccione **ILM > Políticas**.

Alternativamente, puede activar una sola política desde la página **ILM > Etiquetas de política**.

2. En la pestaña Políticas, seleccione la casilla de verificación de la política que desea activar y luego seleccione **Activar**.
3. Siga el paso apropiado:
 - Si un mensaje de advertencia le solicita que confirme que desea activar la política, seleccione **Aceptar**.
 - Si aparece un mensaje de advertencia que contiene detalles sobre la política:
 - i. Revise los detalles para asegurarse de que la política administre los datos como se espera.
 - ii. Si la regla predeterminada almacena objetos durante una cantidad limitada de días, revise el diagrama de retención y luego escriba esa cantidad de días en el cuadro de texto.
 - iii. Si la regla predeterminada almacena objetos para siempre, pero una o más reglas tienen una retención limitada, escriba **sí** en el cuadro de texto.
 - iv. Seleccione **Activar política**.

Activar múltiples políticas

Para activar varias políticas, debe crear etiquetas y asignar una política a cada etiqueta.



Cuando se utilizan varias etiquetas, si los inquilinos reasignan con frecuencia etiquetas de políticas a los depósitos, el rendimiento de la red podría verse afectado. Si tiene inquilinos que no son de confianza, considere usar solo la etiqueta Predeterminada.

1. Seleccione **ILM > Etiquetas de política**.
2. Seleccione **Crear**.
3. En el cuadro de diálogo Crear etiqueta de política, escriba un nombre de etiqueta y, opcionalmente, una descripción para la etiqueta.



Los nombres y descripciones de las etiquetas son visibles para los inquilinos. Elija valores que ayuden a los inquilinos a tomar una decisión informada al momento de seleccionar etiquetas de políticas para asignar a sus grupos. Por ejemplo, si la política asignada eliminará objetos después de un período de tiempo, podría comunicarlo en la descripción. No incluya información confidencial en estos campos.

4. Seleccione **Crear etiqueta**.
5. En la tabla de etiquetas de políticas de ILM, utilice el menú desplegable para seleccionar una política para asignar a la etiqueta.
6. Si aparecen advertencias en la columna Limitaciones de la política, seleccione **Ver detalles de la política** para revisar la política.
7. Asegúrese de que cada política gestione los datos como se espera.
8. Seleccione **Activar políticas asignadas**. O seleccione **Borrar cambios** para eliminar la asignación

de política.

9. En el cuadro de diálogo Activar políticas con nuevas etiquetas, revise las descripciones de cómo cada etiqueta, política y regla administrará los objetos. Realice los cambios necesarios para garantizar que las políticas administren los objetos como se espera.
10. Cuando esté seguro de que desea activar las políticas, escriba **sí** en el cuadro de texto y luego seleccione **Activar políticas**.

Información relacionada

["Ejemplo 6: Cambiar una política de ILM"](#)

Ejemplo de simulaciones de políticas de ILM

Los ejemplos de simulaciones de políticas ILM proporcionan pautas para estructurar y modificar simulaciones para su entorno.

Ejemplo 1: Verificar reglas al simular una política ILM

Este ejemplo describe cómo verificar reglas al simular una política.

En este ejemplo, se simula la **política ILM de ejemplo** contra los objetos ingeridos en dos buckets. La política incluye tres reglas, como sigue:

- La primera regla, **Dos copias, dos años para el contenedor a**, se aplica únicamente a los objetos del contenedor a.
- La segunda regla, **Objetos EC > 1 MB**, se aplica a todos los buckets, pero filtra los objetos mayores de 1 MB.
- La tercera regla, **Dos copias, dos centros de datos**, es la regla predeterminada. No incluye ningún filtro y no utiliza el tiempo de referencia no actual.

Después de simular la política, confirme que cada objeto coincida con la regla correcta.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
<button>Clear all</button> 				
Object 	Version ID 	Rule matched  	Previous match  	Actions
bucket-a/bucket-a object.pdf	—	Two copies, two years for bucket-a	—	
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	

En este ejemplo:

- bucket-a/bucket-a object.pdf coincidió correctamente con la primera regla, que filtra los objetos en `bucket-a`.

- `bucket-b/test object greater than 1 MB.pdf` está en `bucket-b`, por lo que no coincidía con la primera regla. En cambio, la segunda regla coincidió correctamente, ya que filtra objetos de más de 1 MB.
- `bucket-b/test object less than 1 MB.pdf` no coincidió con los filtros de las dos primeras reglas, por lo que se colocará por la regla predeterminada, que no incluye filtros.

Ejemplo 2: Reordenar reglas al simular una política ILM

Este ejemplo muestra cómo se pueden reordenar las reglas para cambiar los resultados al simular una política.

En este ejemplo, se está simulando la política **Demo**. Esta política, que tiene como objetivo encontrar objetos que tengan metadatos de usuario `series=x-men`, incluye tres reglas, como sigue:

- La primera regla, **PNGs**, filtra los nombres de clave que terminan en `.png`.
- La segunda regla, **X-men**, se aplica solo a los objetos del inquilino A y filtra para `series=x-men` metadatos del usuario.
- La última regla, **Dos copias, dos centros de datos**, es la regla predeterminada, que coincide con cualquier objeto que no coincida con las dos primeras reglas.

Pasos

1. Después de agregar las reglas y guardar la política, seleccione **Simular**.
2. En el campo **Objeto**, ingrese la clave de objeto/depósito S3 para un objeto de prueba y seleccione **Simular**.

Aparecen los resultados de la simulación, que muestran que `Havok.png` El objeto coincidió con la regla **PNGs**.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNGs	—	X

Sin embargo, `Havok.png` Estaba destinado a probar la regla de los **X-men**.

3. Para resolver el problema, reordene las reglas.
 - a. Seleccione **Finalizar** para cerrar la ventana Simular política ILM.
 - b. Seleccione **Editar** para editar la política.
 - c. Arrastre la regla **X-men** a la parte superior de la lista.
 - d. Seleccione **Guardar**.
4. Seleccione **Simular**.

Los objetos que probó anteriormente se vuelven a evaluar en función de la política actualizada y se muestran los nuevos resultados de la simulación. En el ejemplo, la columna Regla coincidente muestra que `Havok.png` El objeto ahora coincide con la regla de metadatos de X-Men, como se esperaba. La

columna Coincidencia anterior muestra que la regla PNG coincidió con el objeto en la simulación anterior.

Simulation results

Use this table to confirm the results of applying this policy to the selected objects.

Clear all

Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	X-men	PNGs	

Ejemplo 3: Corregir una regla al simular una política ILM

Este ejemplo muestra cómo simular una política, corregir una regla en la política y continuar la simulación.

En este ejemplo, se está simulando la política **Demo**. Esta política tiene como objetivo encontrar objetos que tengan `series=x-men` metadatos del usuario. Sin embargo, se produjeron resultados inesperados al simular esta política contra la `Beast.jpg` objeto. En lugar de coincidir con la regla de metadatos de X-Men, el objeto coincidió con la regla predeterminada: Dos copias, dos centros de datos.

Simulation results

Use this table to confirm the results of applying this policy to the selected objects.

Clear all

Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	Two copies two data centers	—	

Cuando un objeto de prueba no coincide con la regla esperada en la política, debe examinar cada regla en la política y corregir cualquier error.

Pasos

1. Seleccione **Finalizar** para cerrar el cuadro de diálogo Simular política. En la página de detalles de la política, seleccione **Diagrama de retención**. Luego, seleccione **Expandir todo** o **Ver detalles** para cada regla según sea necesario.
2. Revise la cuenta de inquilino de la regla, el tiempo de referencia y los criterios de filtrado.

A modo de ejemplo, supongamos que los metadatos para la regla de X-men se ingresaron como "x-men01" en lugar de "x-men".
3. Para resolver el error, corrija la regla de la siguiente manera:
 - Si la regla es parte de la política, puede clonar la regla o eliminarla de la política y luego editarla.
 - Si la regla es parte de la política activa, debe clonar la regla. No se puede editar ni eliminar una regla de la política activa.
4. Realice la simulación nuevamente.

En este ejemplo, la regla corregida de los X-Men ahora coincide con la `Beast.jpg` objeto basado en el `series=x-men` metadatos del usuario, como se esperaba.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	X-men	—	X

Administrar etiquetas de políticas de ILM

Puede ver los detalles de la etiqueta de política de ILM, editar una etiqueta o eliminar una etiqueta.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["permisos de acceso necesarios"](#).

Ver detalles de la etiqueta de política de ILM

Para ver los detalles de una etiqueta:

1. Seleccione **ILM > Etiquetas de política**.
2. Seleccione el nombre de la política de la tabla. Aparece la página de detalles de la etiqueta.
3. En la página de detalles, vea el historial anterior de políticas asignadas.
4. Ver una política seleccionándola.

Editar la etiqueta de política de ILM



Los nombres y descripciones de las etiquetas son visibles para los inquilinos. Elija valores que ayuden a los inquilinos a tomar una decisión informada al momento de seleccionar etiquetas de políticas para asignar a sus grupos. Por ejemplo, si la política asignada eliminará objetos después de un período de tiempo, podría comunicarlo en la descripción. No incluya información confidencial en estos campos.

Para editar la descripción de una etiqueta existente:

1. Seleccione **ILM > Etiquetas de política**.
2. Seleccione la casilla de verificación de la etiqueta y luego seleccione **Editar**.

Alternativamente, seleccione el nombre de la etiqueta. Aparecerá la página de detalles de la etiqueta y podrás seleccionar **Editar** en esa página.

3. Cambie la descripción de la etiqueta según sea necesario
4. Seleccione **Guardar**.

Eliminar la etiqueta de política de ILM

Cuando se elimina una etiqueta de política, a todos los depósitos que tengan asignada esa etiqueta se les

aplicará la política predeterminada.

Para eliminar una etiqueta:

1. Seleccione **ILM > Etiquetas de política**.
2. Seleccione la casilla de verificación de la etiqueta y luego seleccione **Eliminar**. Aparece un cuadro de diálogo de confirmación.

Alternativamente, seleccione el nombre de la etiqueta. Aparecerá la página de detalles de la etiqueta y podrás seleccionar **Eliminar** en esa página.

3. Seleccione **Sí** para eliminar la etiqueta.

Verificar una política de ILM con la búsqueda de metadatos de objetos

Después de haber activado una política ILM, ingiera objetos de prueba representativos en el sistema StorageGRID y luego realice una búsqueda de metadatos de objetos para confirmar que se estén realizando copias según lo previsto y se estén colocando en las ubicaciones correctas.

Antes de empezar

Tiene un identificador de objeto, que puede ser uno de los siguientes: * **UUID**: el identificador único universal del objeto. * **CBID**: El identificador único del objeto dentro de StorageGRID. Puede obtener el CBID de un objeto desde el registro de auditoría. Introduzca el CBD en mayúsculas. ***Clave de objeto y depósito S3**: cuando se ingiere un objeto a través de la interfaz S3, la aplicación cliente utiliza una combinación de clave de objeto y depósito para almacenar e identificar el objeto. Si el bucket S3 tiene versiones y desea buscar una versión específica de un objeto S3 usando la clave del bucket y del objeto, tendrá el **ID de versión**.

Pasos

1. Ingerir el objeto.
2. Seleccione **ILM > Búsqueda de metadatos de objetos**.
3. Escriba el identificador del objeto en el campo **Identificador**. Puede ingresar un UUID, CBID o una clave de objeto/depósito S3.
4. Opcionalmente, ingrese un ID de versión para el objeto (sólo S3).
5. Seleccione **Buscar**.

Aparecen los resultados de la búsqueda de metadatos del objeto. En esta página se enumeran los siguientes tipos de información:

- Metadatos del sistema, como ID de objeto (UUID), tipo de resultado (objeto, marcador de eliminación, depósito S3) y tamaño lógico del objeto. Consulte la captura de pantalla de ejemplo a continuación para obtener más detalles.
- Cualquier par clave-valor de metadatos de usuario personalizados asociados con el objeto.
- Para los objetos S3, cualquier par clave-valor de etiqueta de objeto asociado con el objeto.
- Para copias de objetos replicados, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos con código de borrado, la ubicación de almacenamiento actual de cada fragmento.
- Para las copias de objetos en un grupo de almacenamiento en la nube, la ubicación del objeto, incluido el nombre del depósito externo y el identificador único del objeto.

- Para objetos segmentados y objetos multiparte, una lista de segmentos de objetos que incluye identificadores de segmento y tamaños de datos. Para los objetos con más de 100 segmentos, solo se muestran los primeros 100 segmentos.
 - Todos los metadatos del objeto en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen metadatos internos del sistema que no se garantiza que persistan de una versión a otra.
6. Confirme que el objeto esté almacenado en la ubicación o ubicaciones correctas y que sea el tipo de copia correcto.

Si la opción Auditoría está habilitada, también puede supervisar el registro de auditoría para el mensaje Reglas de objeto ORLM cumplidas. El mensaje de auditoría de ORLM puede brindarle más información sobre el estado del proceso de evaluación de ILM, pero no puede brindarle información sobre la exactitud de la ubicación de los datos del objeto ni sobre la integridad de la política de ILM. Debes evaluar esto tú mismo. Para obtener más información, consulte ["Revisar los registros de auditoría"](#).

El siguiente ejemplo muestra los resultados de la búsqueda de metadatos de un objeto de prueba S3 que se almacena como dos copias replicadas.



La siguiente captura de pantalla es un ejemplo. Los resultados variarán según la versión de StorageGRID.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAHS": "2",

```

Información relacionada

["Utilice la API REST de S3"](#)

Trabajar con políticas y reglas de ILM

A medida que cambian sus requisitos de almacenamiento, es posible que necesite implementar políticas adicionales o modificar las reglas de ILM asociadas con una política. Puede ver las métricas de ILM para determinar el rendimiento del sistema.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .

Ver las políticas de ILM

Para ver las políticas ILM activas e inactivas y el historial de activación de políticas:

1. Seleccione **ILM > Políticas**.
2. Seleccione **Políticas** para ver una lista de políticas activas e inactivas. La tabla enumera el nombre de cada política, las etiquetas a las que está asignada la política y si la política está activa o inactiva.
3. Seleccione **Historial de activación** para ver una lista de las fechas de inicio y finalización de la activación de las políticas.
4. Seleccione un nombre de política para ver los detalles de la política.



Si visualiza los detalles de una política cuyo estado es Editado o Eliminado, aparece un mensaje que explica que está visualizando la versión de la política que estuvo activa durante el período de tiempo especificado y que desde entonces ha sido editada o eliminada.

Editar una política de ILM

Sólo puedes editar una política inactiva. Si desea editar una política activa, desactívela o cree un clon y edítelo.

Para editar una política:

1. Seleccione **ILM > Políticas**.
2. Seleccione la casilla de verificación de la política que desea editar y luego seleccione **Editar**.
3. Edite la política siguiendo las instrucciones en "[Crear políticas ILM](#)".
4. Simule la política antes de reactivarla.



Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irreparable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

Clonar una política de ILM

Para clonar una política ILM:

1. Seleccione **ILM > Políticas**.
2. Seleccione la casilla de verificación de la política que desea clonar y luego seleccione **Clonar**.
3. Cree una nueva política a partir de la política que ha clonado siguiendo las instrucciones en "[Crear políticas ILM](#)".



Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irreparable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

Eliminar una política de ILM

Solo puedes eliminar una política ILM si está inactiva. Para eliminar una política:

1. Seleccione **ILM > Políticas**.

2. Seleccione la casilla de verificación de la política inactiva que desea eliminar.
3. Seleccione **Eliminar**.

Ver detalles de las reglas de ILM

Para ver los detalles de una regla ILM, incluido el diagrama de retención y las instrucciones de ubicación de la regla:

1. Seleccione **ILM > Reglas**.
2. Seleccione el nombre de la regla cuyos detalles desea ver. Ejemplo:

Además, puede utilizar la página de detalles para clonar, editar o eliminar una regla. No puedes editar ni eliminar una regla si se utiliza en alguna política.

Clonar una regla ILM

Puede clonar una regla existente si desea crear una nueva regla que utilice algunas de las configuraciones de la regla existente. Si necesita editar una regla que se utiliza en alguna política, debe clonar la regla y realizar cambios en el clon. Después de realizar cambios en el clon, puede eliminar la regla original de la política y reemplazarla con la versión modificada según sea necesario.



No se puede clonar una regla ILM si se creó utilizando StorageGRID versión 10.2 o anterior.

Pasos

1. Seleccione **ILM > Reglas**.
2. Seleccione la casilla de verificación de la regla que desea clonar y luego seleccione **Clonar**.

Alternativamente, seleccione el nombre de la regla y luego seleccione **Clonar** en la página de detalles de la regla.

3. Actualice la regla clonada siguiendo los pasos para [editar una regla ILM](#) y ["Uso de filtros avanzados en las reglas de ILM"](#).

Al clonar una regla ILM, debe ingresar un nuevo nombre.

Editar una regla de ILM

Es posible que necesite editar una regla ILM para cambiar un filtro o una instrucción de ubicación.

No puedes editar una regla si se utiliza en alguna política de ILM. En cambio, puedes [clonar la regla](#) y realizar los cambios necesarios en la copia clonada.



Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irreparable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

Pasos

1. Seleccione **ILM > Reglas**.
2. Confirme que la regla que desea editar no se utiliza en ninguna política de ILM.
3. Si la regla que desea editar no está en uso, seleccione la casilla de verificación de la regla y seleccione **Acciones > Editar**. Alternativamente, seleccione el nombre de la regla y luego seleccione **Editar** en la página de detalles de la regla.
4. Complete los pasos del asistente Editar regla de ILM. Según sea necesario, siga los pasos para ["creando una regla ILM"](#) y ["Uso de filtros avanzados en las reglas de ILM"](#).

Al editar una regla ILM, no puedes cambiar su nombre.

Eliminar una regla ILM

Para mantener manejable la lista de reglas ILM actuales, elimine cualquier regla ILM que probablemente no utilice.

Pasos

Para eliminar una regla ILM que se utiliza actualmente en una política activa:

1. Clonar la política.
2. Eliminar la regla ILM del clon de política.
3. Guarde, simule y active la nueva política para asegurarse de que los objetos estén protegidos como se espera.
4. Vaya a los pasos para eliminar una regla ILM que se utiliza actualmente en una política inactiva.

Para eliminar una regla ILM que se utiliza actualmente en una política inactiva:

1. Seleccione la política inactiva.
2. Eliminar la regla ILM de la política o [eliminar la política](#).
3. Vaya a los pasos para eliminar una regla ILM que no se utiliza actualmente.

Para eliminar una regla ILM que no se utiliza actualmente:

1. Seleccione **ILM > Reglas**.
2. Confirme que la regla que desea eliminar no se utiliza en ninguna política.
3. Si la regla que desea eliminar no está en uso, selecciónela y seleccione **Acciones > Eliminar**. Puede seleccionar varias reglas y eliminarlas todas al mismo tiempo.
4. Seleccione **Sí** para confirmar que desea eliminar la regla ILM.

Ver métricas de ILM

Puede ver métricas de ILM, como la cantidad de objetos en la cola y la tasa de evaluación. Puede supervisar estas métricas para determinar el rendimiento del sistema. Una cola o tasa de evaluación grande podría indicar que el sistema no puede mantener el ritmo de la tasa de ingesta, que la carga de las aplicaciones cliente es excesiva o que existe alguna condición anormal.

Pasos

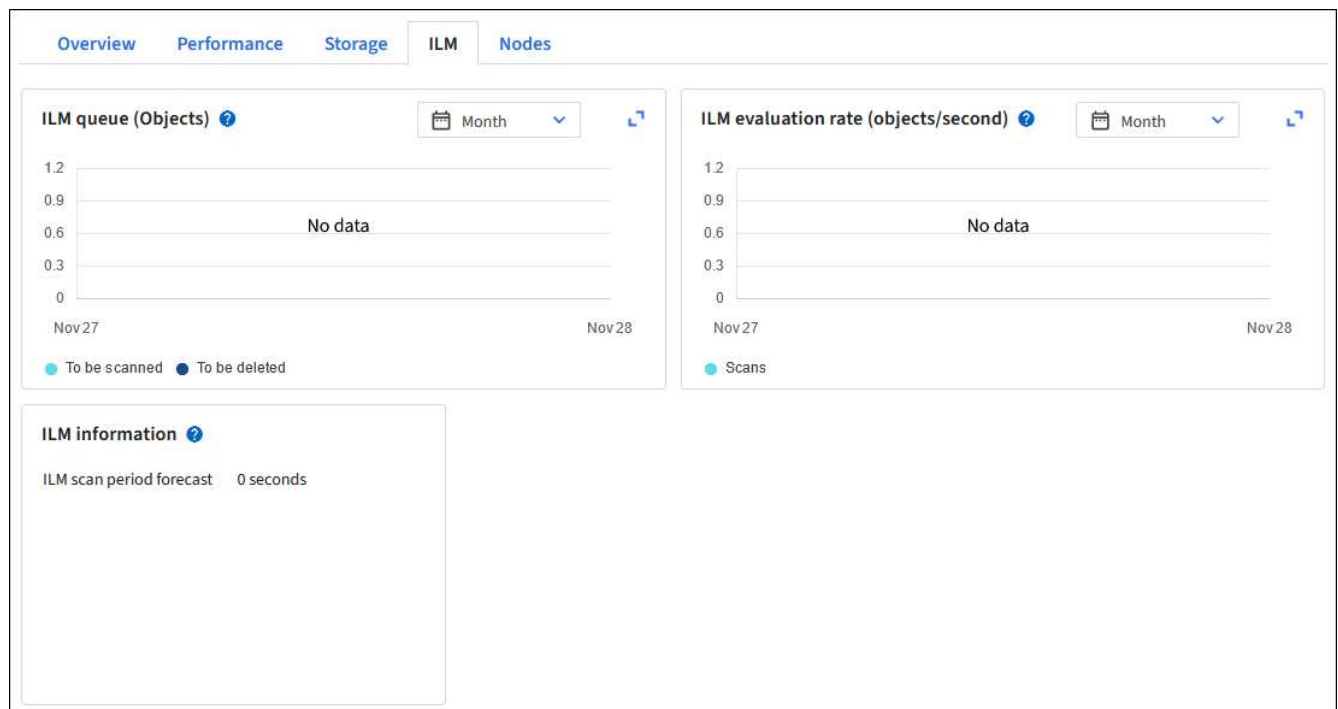
1. Seleccione **Panel de control > ILM**.



Debido a que el panel se puede personalizar, es posible que la pestaña ILM no esté disponible.

2. Supervise las métricas en la pestaña ILM.

Puedes seleccionar el signo de interrogación (?) para ver una descripción de los elementos en la pestaña ILM.



Usar bloqueo de objetos S3

Administrar objetos con S3 Object Lock

Como administrador de la red, puede habilitar el bloqueo de objetos S3 para su sistema StorageGRID e implementar una política ILM compatible para ayudar a garantizar que los objetos en depósitos S3 específicos no se eliminen ni se sobrescriban durante un período de tiempo específico.

¿Qué es el bloqueo de objetos S3?

La función StorageGRID S3 Object Lock es una solución de protección de objetos que es equivalente a S3 Object Lock en Amazon Simple Storage Service (Amazon S3).

Cuando la configuración global de Bloqueo de objetos S3 está habilitada para un sistema StorageGRID, una cuenta de inquilino S3 puede crear depósitos con o sin el Bloqueo de objetos S3 habilitado. Si un bucket tiene habilitado el bloqueo de objetos S3, se requiere el control de versiones del bucket y se habilita automáticamente.

Un depósito sin bloqueo de objetos S3 solo puede tener objetos sin configuraciones de retención especificadas. Ningún objeto ingerido tendrá configuraciones de retención.

Un depósito con bloqueo de objetos S3 puede tener objetos con y sin configuraciones de retención especificadas por las aplicaciones cliente S3. Algunos objetos ingeridos tendrán configuraciones de retención.

Un depósito con bloqueo de objetos S3 y retención predeterminada configurada puede tener objetos cargados con configuraciones de retención especificadas y objetos nuevos sin configuraciones de retención. Los nuevos objetos utilizan la configuración predeterminada, porque la configuración de retención no se ha configurado a nivel de objeto.

De hecho, todos los objetos recién ingeridos tienen configuraciones de retención cuando se configura la retención predeterminada. Los objetos existentes sin configuraciones de retención de objetos no se verán afectados.

Modos de retención

La función de bloqueo de objetos de StorageGRID S3 admite dos modos de retención para aplicar diferentes niveles de protección a los objetos. Estos modos son equivalentes a los modos de retención de Amazon S3.

- En modo de cumplimiento:
 - El objeto no se puede eliminar hasta que se alcance su fecha de conservación.
 - La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir.
 - La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha.
- En modo de gobernanza:
 - Los usuarios con permiso especial pueden usar un encabezado de omisión en las solicitudes para modificar ciertas configuraciones de retención.
 - Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación.
 - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.

Configuración de retención para versiones de objetos

Si se crea un depósito con el bloqueo de objetos S3 habilitado, los usuarios pueden usar la aplicación cliente S3 para especificar opcionalmente las siguientes configuraciones de retención para cada objeto que se agregue al depósito:

- **Modo de retención:** Cumplimiento o gobernanza.
- **Conservar hasta fecha:** si la fecha de conservación de una versión de un objeto está en el futuro, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal:** al aplicar una retención legal a una versión de un objeto, se bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesites colocar una retención legal en un objeto que esté relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, sino que permanece vigente hasta que se elimina explícitamente. Las retenciones legales son independientes de la fecha de conservación.



Si un objeto está bajo retención legal, nadie puede eliminarlo, independientemente de su modo de retención.

Para obtener detalles sobre la configuración de los objetos, consulte ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#).

Configuración de retención predeterminada para depósitos

Si se crea un depósito con el bloqueo de objetos S3 habilitado, los usuarios pueden especificar opcionalmente las siguientes configuraciones predeterminadas para el depósito:

- **Modo de retención predeterminado:** Cumplimiento o gobernanza.
- **Período de retención predeterminado:** durante cuánto tiempo se deben conservar las nuevas versiones de objetos agregadas a este depósito, a partir del día en que se agregan.

La configuración de depósito predeterminada se aplica únicamente a los objetos nuevos que no tienen su propia configuración de retención. Los objetos de bucket existentes no se ven afectados cuando agrega o cambia estas configuraciones predeterminadas.

Ver ["Crear un bucket S3"](#) y ["Actualizar la retención predeterminada de bloqueo de objetos S3"](#).

Comparación del bloqueo de objetos S3 con la conformidad heredada

El bloqueo de objetos S3 reemplaza la función de Cumplimiento que estaba disponible en versiones anteriores de StorageGRID. Debido a que la función de bloqueo de objetos S3 se ajusta a los requisitos de Amazon S3, deja obsoleta la función de cumplimiento patentada de StorageGRID, que ahora se denomina "cumplimiento heredado".



La configuración de Cumplimiento global está obsoleta. Si habilitó esta configuración utilizando una versión anterior de StorageGRID, la configuración de Bloqueo de objetos S3 se habilita automáticamente. Puede seguir usando StorageGRID para administrar las configuraciones de los depósitos compatibles existentes; sin embargo, no puede crear depósitos compatibles nuevos. Para más detalles, consulte ["Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"](#).

Si utilizó la función de Cumplimiento heredada en una versión anterior de StorageGRID, consulte la siguiente tabla para saber cómo se compara con la función de Bloqueo de objetos S3 en StorageGRID.

	Bloqueo de objetos S3	Cumplimiento (legado)
¿Cómo se habilita la función a nivel global?	Desde el Administrador de cuadrícula, seleccione CONFIGURACIÓN > Sistema > Bloqueo de objetos S3 .	Ya no se admite.
¿Cómo se habilita la función para un bucket?	Los usuarios deben habilitar el bloqueo de objetos S3 al crear un nuevo depósito mediante el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3.	Ya no se admite.
¿Se admite el control de versiones del bucket?	Sí. El control de versiones del depósito es necesario y se habilita automáticamente cuando S3 Object Lock está habilitado para el depósito.	No.
¿Cómo se establece la retención de objetos?	Los usuarios pueden establecer una fecha de retención para cada versión del objeto o pueden establecer un período de retención predeterminado para cada depósito.	Los usuarios deben establecer un período de retención para todo el depósito. El período de retención se aplica a todos los objetos del depósito.
¿Se puede modificar el periodo de conservación?	• En el modo de cumplimiento, la fecha de retención para una versión de objeto se puede aumentar, pero nunca disminuir. • En el modo de gobernanza, los usuarios con permisos especiales pueden disminuir o incluso eliminar la configuración de retención de un objeto.	El período de retención de un depósito se puede aumentar, pero nunca disminuir.
¿Dónde se controla la retención legal?	Los usuarios pueden colocar una retención legal o levantar una retención legal para cualquier versión de objeto en el depósito.	Se coloca una retención legal en el cubo y afecta a todos los objetos que se encuentran en el cubo.

	Bloqueo de objetos S3	Cumplimiento (legado)
¿Cuándo se pueden eliminar objetos?	• En el modo de cumplimiento, se puede eliminar una versión de un objeto una vez alcanzada la fecha de retención, siempre que el objeto no esté bajo retención legal. • En el modo de gobernanza, los usuarios con permisos especiales pueden eliminar un objeto antes de que se alcance su fecha de retención, siempre que el objeto no esté bajo retención legal.	Se puede eliminar un objeto una vez que expire el período de retención, siempre que el depósito no esté bajo retención legal. Los objetos se pueden eliminar de forma automática o manual.
¿Se admite la configuración del ciclo de vida del bucket?	Sí	No

Tareas de bloqueo de objetos S3

Como administrador de la red, debe coordinarse estrechamente con los usuarios inquilinos para garantizar que los objetos estén protegidos de una manera que satisfaga sus requisitos de retención.



La aplicación de la configuración de los inquilinos en toda la red podría demorar 15 minutos o más según la conectividad de la red, el estado del nodo y las operaciones de Cassandra.

Las siguientes listas para administradores de red y usuarios inquilinos contienen las tareas de alto nivel para usar la función de bloqueo de objetos S3.

Administrador de red

- Habilite la configuración global de bloqueo de objetos S3 para todo el sistema StorageGRID .
- Asegúrese de que las políticas de gestión del ciclo de vida de la información (ILM) sean *compatibles*; es decir, que cumplan con los requisitos "[Requisitos de los buckets con bloqueo de objetos S3 habilitado](#)".
- Según sea necesario, permita que un inquilino utilice Cumplimiento como modo de retención. De lo contrario, solo se permite el modo Gobernanza.
- Según sea necesario, establezca un período máximo de retención para un inquilino.

Usuario inquilino

- Revise las consideraciones para depósitos y objetos con bloqueo de objetos S3.
- Según sea necesario, comuníquese con el administrador de la red para habilitar la configuración global de bloqueo de objetos S3 y establecer permisos.
- Cree depósitos con el bloqueo de objetos S3 habilitado.
- De manera opcional, configure los ajustes de retención predeterminados para un depósito:

- Modo de retención predeterminado: Gobernanza o Cumplimiento, si lo permite el administrador de la red.
- Período de retención predeterminado: debe ser menor o igual al período de retención máximo establecido por el administrador de la red.
- Utilice la aplicación cliente S3 para agregar objetos y, opcionalmente, configurar la retención específica de objetos:
 - Modo de retención. Gobernanza o Cumplimiento, si lo permite el administrador de la red.
 - Conservar hasta la fecha: debe ser menor o igual a lo permitido por el período máximo de retención establecido por el administrador de la red.

Requisitos para el bloqueo de objetos S3

Debe revisar los requisitos para habilitar la configuración global de Bloqueo de objetos S3, los requisitos para crear reglas y políticas ILM compatibles y las restricciones que StorageGRID impone a los depósitos y objetos que usan Bloqueo de objetos S3.

Requisitos para utilizar la configuración global de bloqueo de objetos S3

- Debe habilitar la configuración global de Bloqueo de objetos S3 mediante el Administrador de cuadrícula o la API de administración de cuadrícula antes de que cualquier inquilino de S3 pueda crear un depósito con el Bloqueo de objetos S3 habilitado.
- Al habilitar la configuración global de Bloqueo de objetos S3, se permite que todas las cuentas de inquilinos de S3 creen depósitos con el Bloqueo de objetos S3 habilitado.
- Después de habilitar la configuración global de Bloqueo de objetos S3, no podrá deshabilitarla.
- No se puede habilitar el bloqueo de objetos S3 global a menos que la regla predeterminada en todas las políticas ILM activas sea *compatible* (es decir, la regla predeterminada debe cumplir con los requisitos de los depósitos con el bloqueo de objetos S3 habilitado).
- Cuando la configuración global de Bloqueo de objetos S3 está habilitada, no puede crear una nueva política ILM ni activar una política ILM existente a menos que la regla predeterminada en la política sea compatible. Una vez habilitada la configuración global de bloqueo de objetos S3, las páginas de reglas ILM y políticas ILM indican qué reglas ILM son compatibles.

Requisitos para el cumplimiento de las normas ILM

Si desea habilitar la configuración global de bloqueo de objetos S3, debe asegurarse de que la regla predeterminada en todas las políticas ILM activas sea compatible. Una regla compatible satisface los requisitos de ambos depósitos con S3 Object Lock habilitado y de cualquier depósito existente que tenga habilitada la conformidad heredada:

- Debe crear al menos dos copias del objeto replicado o una copia con código de borrado.
- Estas copias deben existir en los nodos de almacenamiento durante toda la duración de cada línea en las instrucciones de ubicación.
- Las copias de objetos no se pueden guardar en un grupo de almacenamiento en la nube.
- Al menos una línea de las instrucciones de ubicación debe comenzar en el día 0, utilizando **Hora de ingesta** como tiempo de referencia.
- Al menos una línea de las instrucciones de colocación debe ser "para siempre".

Requisitos para las políticas de ILM

Cuando la configuración global de Bloqueo de objetos S3 está habilitada, las políticas ILM activas e inactivas pueden incluir reglas compatibles y no compatibles.

- La regla predeterminada en una política ILM activa o inactiva debe ser compatible.
- Las reglas no conformes solo se aplican a los objetos en depósitos que no tienen habilitado el Bloqueo de objetos S3 o que no tienen habilitada la función de Cumplimiento heredada.
- Las reglas compatibles se pueden aplicar a objetos en cualquier bucket; no es necesario habilitar S3 Object Lock ni la conformidad heredada para el bucket.

"Ejemplo de una política ILM compatible con el bloqueo de objetos S3"

Requisitos para los buckets con el bloqueo de objetos S3 habilitado

- Si la configuración global de Bloqueo de objetos S3 está habilitada para el sistema StorageGRID , puede usar el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3 para crear depósitos con el Bloqueo de objetos S3 habilitado.
- Si planea utilizar S3 Object Lock, debe habilitar S3 Object Lock cuando cree el depósito. No se puede habilitar el bloqueo de objetos S3 para un depósito existente.
- Cuando S3 Object Lock está habilitado para un bucket, StorageGRID habilita automáticamente el control de versiones para ese bucket. No puedes deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones del depósito.
- De manera opcional, puede especificar un modo de retención predeterminado y un período de retención para cada depósito mediante el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3. La configuración de retención predeterminada del depósito se aplica únicamente a los objetos nuevos agregados al depósito que no tienen su propia configuración de retención. Puede anular estas configuraciones predeterminadas especificando un modo de retención y una fecha de retención para cada versión del objeto cuando se carga.
- La configuración del ciclo de vida del bucket es compatible con los buckets que tienen el bloqueo de objetos S3 habilitado.
- La replicación de CloudMirror no es compatible con depósitos con el bloqueo de objetos S3 habilitado.

Requisitos para objetos en depósitos con bloqueo de objetos S3 habilitado

- Para proteger una versión de objeto, puede especificar la configuración de retención predeterminada para el depósito o puede especificar la configuración de retención para cada versión de objeto. Las configuraciones de retención a nivel de objeto se pueden especificar mediante la aplicación cliente S3 o la API REST S3.
- Las configuraciones de retención se aplican a versiones de objetos individuales. Una versión de objeto puede tener una configuración de conservación hasta la fecha y una configuración de conservación legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta la fecha o de retención legal para un objeto, se protege únicamente la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras la versión anterior del objeto permanece bloqueada.

Ciclo de vida de objetos en buckets con S3 Object Lock habilitado

Cada objeto que se guarda en un bucket con el bloqueo de objetos S3 habilitado pasa por estas etapas:

1. Ingesta de objeto

Cuando se agrega una versión de objeto a un depósito que tiene habilitado el Bloqueo de objetos S3, las

configuraciones de retención se aplican de la siguiente manera:

- Si se especifican configuraciones de retención para el objeto, se aplican las configuraciones a nivel de objeto. Se ignoran todas las configuraciones de depósito predeterminadas.
- Si no se especifican configuraciones de retención para el objeto, se aplican las configuraciones de depósito predeterminadas, si existen.
- Si no se especifican configuraciones de retención para el objeto o el depósito, el objeto no estará protegido por el bloqueo de objetos S3.

Si se aplican configuraciones de retención, tanto el objeto como cualquier metadato definido por el usuario de S3 estarán protegidos.

2. Retención y eliminación de objetos

StorageGRID almacena varias copias de cada objeto protegido durante el período de retención especificado. La cantidad exacta y el tipo de copias de objetos y las ubicaciones de almacenamiento están determinados por las reglas compatibles con las políticas ILM activas. Si un objeto protegido se puede eliminar antes de que se alcance su fecha de retención depende de su modo de retención.

- Si un objeto está bajo retención legal, nadie puede eliminarlo, independientemente de su modo de retención.

Información relacionada

- ["Crear un bucket S3"](#)
- ["Actualizar la retención predeterminada de bloqueo de objetos S3"](#)
- ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)
- ["Ejemplo 7: Política ILM compatible con el bloqueo de objetos S3"](#)

Habilitar el bloqueo de objetos S3 globalmente

Si una cuenta de inquilino S3 necesita cumplir con requisitos reglamentarios al guardar datos de objetos, debe habilitar S3 Object Lock para todo su sistema StorageGRID . Al habilitar la configuración global de Bloqueo de objetos S3, cualquier usuario inquilino de S3 puede crear y administrar depósitos y objetos con Bloqueo de objetos S3.

Antes de empezar

- Tú tienes el ["Permiso de acceso root"](#) .
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Ha revisado el flujo de trabajo de bloqueo de objetos S3 y comprende las consideraciones.
- Ha confirmado que la regla predeterminada en la política ILM activa es compatible. Ver ["Crear una regla ILM predeterminada"](#) Para más detalles.

Acerca de esta tarea

Un administrador de red debe habilitar la configuración global de Bloqueo de objetos S3 para permitir que los usuarios inquilinos creen nuevos depósitos que tengan habilitado el Bloqueo de objetos S3. Una vez habilitada esta configuración, no se podrá deshabilitar.

Revise la configuración de cumplimiento de los inquilinos existentes después de habilitar la configuración global de Bloqueo de objetos S3. Cuando habilita esta configuración, las configuraciones de bloqueo de objetos S3 por inquilino dependen de la versión de StorageGRID en el momento en que se creó el inquilino.



La configuración de Cumplimiento global está obsoleta. Si habilitó esta configuración utilizando una versión anterior de StorageGRID, la configuración de Bloqueo de objetos S3 se habilita automáticamente. Puede seguir usando StorageGRID para administrar las configuraciones de los depósitos compatibles existentes; sin embargo, no puede crear depósitos compatibles nuevos. Para más detalles, consulte ["Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"](#) .

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Bloqueo de objetos S3**.

Aparece la página Configuración de bloqueo de objetos S3.

2. Seleccione **Habilitar bloqueo de objetos S3**.

3. Seleccione **Aplicar**.

Aparece un cuadro de diálogo de confirmación que le recuerda que no puede deshabilitar S3 Object Lock una vez habilitado.

4. Si está seguro de que desea habilitar permanentemente S3 Object Lock para todo el sistema, seleccione **Aceptar**.

Al seleccionar **Aceptar**:

- Si la regla predeterminada en la política ILM activa es compatible, el bloqueo de objetos S3 ahora está habilitado para toda la cuadrícula y no se puede deshabilitar.
- Si la regla predeterminada no se cumple, aparece un error. Debe crear y activar una nueva política ILM que incluya una regla compatible como regla predeterminada. Seleccione **Aceptar**. Luego, crea una nueva política, simulénala y actívala. Ver ["Crear una política ILM"](#) para obtener instrucciones.

Resolver errores de coherencia al actualizar el bloqueo de objetos S3 o la configuración de cumplimiento heredada

Si un sitio de un centro de datos o varios nodos de almacenamiento en un sitio dejan de estar disponibles, es posible que deba ayudar a los usuarios inquilinos de S3 a aplicar cambios en el bloqueo de objetos de S3 o en la configuración de cumplimiento heredada.

Los usuarios inquilinos que tienen depósitos con S3 Object Lock (o cumplimiento heredado) habilitado pueden cambiar ciertas configuraciones. Por ejemplo, un usuario inquilino que utiliza S3 Object Lock podría necesitar colocar una versión de objeto bajo retención legal.

Cuando un usuario inquilino actualiza la configuración de un depósito S3 o una versión de objeto, StorageGRID intenta actualizar inmediatamente los metadatos del depósito o del objeto en toda la red. Si el sistema no puede actualizar los metadatos porque un sitio del centro de datos o varios nodos de almacenamiento no están disponibles, devuelve un error:

```
503: Service Unavailable
```

```
Unable to update compliance settings because the settings can't be  
consistently applied on enough storage services. Contact your grid  
administrator for assistance.
```

Para resolver este error, siga estos pasos:

1. Intente que todos los nodos o sitios de almacenamiento vuelvan a estar disponibles lo antes posible.
2. Si no puede poner a disposición suficientes nodos de almacenamiento en cada sitio, comuníquese con el soporte técnico, que puede ayudarlo a recuperar nodos y garantizar que los cambios se apliquen de manera uniforme en toda la red.
3. Una vez que se haya resuelto el problema subyacente, recuérdelo al usuario inquilino que vuelva a intentar realizar los cambios de configuración.

Información relacionada

- ["Utilice una cuenta de inquilino"](#)
- ["Utilice la API REST de S3"](#)
- ["Recuperar y mantener"](#)

Ejemplo de reglas y políticas de ILM

Ejemplo 1: Reglas y políticas de ILM para el almacenamiento de objetos

Puede utilizar las siguientes reglas y políticas de ejemplo como punto de partida al definir una política ILM para cumplir con sus requisitos de retención y protección de objetos.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlrela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Regla 1 de ILM para el ejemplo 1: Copiar datos de objetos a dos sitios

Esta regla ILM de ejemplo copia datos de objetos en grupos de almacenamiento en dos sitios.

Definición de regla	Valor de ejemplo
Piscinas de almacenamiento en un solo sitio	Dos grupos de almacenamiento, cada uno con sitios diferentes, denominados Sitio 1 y Sitio 2.
Nombre de la regla	Dos copias, dos sitios
Tiempo de referencia	Tiempo de ingesta
Colocaciones	Desde el día 0 hasta siempre, conserve una copia replicada en el Sitio 1 y una copia replicada en el Sitio 2.

La sección de análisis de reglas del diagrama de retención establece:

- La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
- Los objetos procesados por esta regla no serán eliminados por ILM.

Reference time ⓘ

Ingest time

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store forever

Store objects by replicating

1

copies at Site 1

and store objects by replicating

1

copies at Site 2

Add other type or location

Add another time period

Retention diagram

Replicated copy

Rule analysis:

StorageGRID site-loss protection will apply for the duration of this rule.

Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

1 replicated copy - Site 1

1 replicated copy - Site 2

Duration Forever

Regla 2 de ILM para el ejemplo 1: Perfil de codificación de borrado con coincidencia de depósito

Esta regla ILM de ejemplo utiliza un perfil de codificación de borrado y un depósito S3 para determinar dónde y durante cuánto tiempo se almacena el objeto.

Definición de regla	Valor de ejemplo
Pool de almacenamiento con múltiples sitios	Un grupo de almacenamiento en tres sitios (sitios 1, 2 y 3) Utilice el esquema de codificación de borrado 6+3
Nombre de la regla	Registros financieros del depósito S3
Tiempo de referencia	Tiempo de ingesta
Colocaciones	Para los objetos en el bucket S3 llamado finance-records, cree una copia con código de borrado en el grupo especificado por el perfil de codificación de borrado. Conserve esta copia para siempre.

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store forever

X

Store objects by

erasure coding

using 6+3 EC scheme at Sites 1, 2, 3

X

Add other type or location

Add another time period

Retention diagram

Erasure-coded (EC) copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

EC 6+3 - Sites 1, 2, 3

Duration Forever

Política de ILM, por ejemplo 1

En la práctica, la mayoría de las políticas ILM son simples, aunque el sistema StorageGRID le permite diseñar políticas ILM sofisticadas y complejas.

Una política ILM típica para una red de múltiples sitios podría incluir reglas ILM como las siguientes:

- En la ingesta, almacene todos los objetos que pertenecen al bucket S3 denominado `finance-records` en un grupo de almacenamiento que contiene tres sitios. Utilice la codificación de borrado 6+3.
- Si un objeto no coincide con la primera regla ILM, utilice la regla ILM predeterminada de la política, Dos copias, dos centros de datos, para almacenar una copia de ese objeto en el Sitio 1 y una copia en el Sitio 2.

Información relacionada

- ["Utilice las políticas de ILM"](#)
- ["Crear políticas ILM"](#)

Ejemplo 2: Reglas y políticas de ILM para el filtrado del tamaño de objetos EC

Puede utilizar las siguientes reglas y políticas de ejemplo como puntos de partida para definir una política ILM que filtre por tamaño de objeto para cumplir con los requisitos de EC recomendados.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlere la para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Regla 1 de ILM para el ejemplo 2: utilizar EC para objetos mayores a 1 MB

Este ejemplo de código de borrado de reglas ILM codifica objetos que tienen más de 1 MB.



La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Solo objetos EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para el tamaño del objeto	Tamaño de objeto mayor a 1 MB
Colocaciones	Cree una copia con código de borrado 2+1 utilizando tres sitios

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ×

Object size ▼

greater than ▼

1 ↕

MB ▼ ×

Regla 2 de ILM para el ejemplo 2: Dos copias replicadas

Esta regla ILM de ejemplo crea dos copias replicadas y no filtra por tamaño de objeto. Esta regla es la regla predeterminada para la política. Dado que la primera regla filtra todos los objetos mayores a 1 MB, esta regla solo se aplica a objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de la regla	Dos copias replicadas
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para el tamaño del objeto	Ninguno
Colocaciones	Desde el día 0 hasta siempre, conserve una copia replicada en el Sitio 1 y una copia replicada en el Sitio 2.

Política de ILM para el ejemplo 2: utilizar EC para objetos mayores a 1 MB

Este ejemplo de política ILM incluye dos reglas ILM:

- La primera regla borra todos los objetos que tengan un tamaño superior a 1 MB.
- La segunda regla ILM (predeterminada) crea dos copias replicadas. Debido a que la regla 1 filtró los objetos de más de 1 MB, la regla 2 solo se aplica a objetos de 1 MB o menos.

Ejemplo 3: Reglas y políticas de ILM para una mejor protección de los archivos de imagen

Puede utilizar las siguientes reglas y políticas de ejemplo para garantizar que las imágenes de más de 1 MB tengan un código de borrado y que se hagan dos copias de imágenes más pequeñas.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlere la para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Regla 1 de ILM para el ejemplo 3: utilizar EC para archivos de imagen de más de 1 MB

Esta regla ILM de ejemplo utiliza filtrado avanzado para borrar el código de todos los archivos de imagen de más de 1 MB.



La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Archivos de imagen EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para el tamaño del objeto	Tamaño de objeto mayor a 1 MB
Filtros avanzados para clave	• Termina en .jpg • Termina en .png
Colocaciones	Cree una copia con código de borrado 2+1 utilizando tres sitios

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼ greater than ▼ 1 ▼ MB ✕

and Key ▼ ends with ▼ .jpg ✕

or Filter group 2 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼ greater than ▼ 1 ▼ MB ✕

and Key ▼ ends with ▼ .png ✕

Debido a que esta regla está configurada como la primera regla en la política, la instrucción de ubicación de codificación de borrado solo se aplica a archivos .jpg y .png que tengan más de 1 MB.

Regla 2 de ILM para el ejemplo 3: Crear 2 copias replicadas para todos los archivos de imagen restantes

Esta regla ILM de ejemplo utiliza filtrado avanzado para especificar que se repliquen archivos de imagen más pequeños. Dado que la primera regla de la política ya ha coincidido con archivos de imagen de más de 1 MB, esta regla se aplica a archivos de imagen de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de la regla	2 copias para archivos de imagen
Tiempo de referencia	Tiempo de ingesta
Filtros avanzados para clave	• Termina en .jpg • Termina en .png
Colocaciones	Cree 2 copias replicadas en dos grupos de almacenamiento

Política de ILM, por ejemplo 3: Mejor protección para los archivos de imagen

Este ejemplo de política ILM incluye tres reglas:

- La primera regla borra todos los archivos de imagen mayores a 1 MB.
- La segunda regla crea dos copias de cualquier archivo de imagen restante (es decir, imágenes de 1 MB o menos).
- La regla predeterminada se aplica a todos los objetos restantes (es decir, cualquier archivo que no sea imagen).

Ejemplo 4: Reglas y políticas de ILM para objetos versionados de S3

Si tiene un bucket S3 con control de versiones habilitado, puede administrar las versiones de objetos no actuales incluyendo reglas en su política ILM que utilicen "Hora no actual" como hora de referencia.



Si especifica un tiempo de retención limitado para los objetos, dichos objetos se eliminarán de forma permanente una vez alcanzado el período de tiempo. Asegúrese de comprender cuánto tiempo se conservarán los objetos.

Como muestra este ejemplo, puede controlar la cantidad de almacenamiento utilizada por objetos versionados mediante el uso de diferentes instrucciones de ubicación para versiones de objetos no actuales.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlrela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.



Para realizar una simulación de política ILM en una versión no actual de un objeto, debe conocer el UUID o CBID de la versión del objeto. Para encontrar el UUID y el CBID, utilice ["búsqueda de metadatos de objetos"](#) mientras el objeto todavía esté actual.

Información relacionada

"Cómo se eliminan los objetos"

Regla 1 de ILM, por ejemplo 4: Guardar tres copias durante 10 años

Esta regla ILM de ejemplo almacena una copia de cada objeto en tres sitios durante 10 años.

Esta regla se aplica a todos los objetos, independientemente de si tienen versiones o no.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Tres grupos de almacenamiento, cada uno de ellos compuesto por diferentes centros de datos, denominados Sitio 1, Sitio 2 y Sitio 3.
Nombre de la regla	Tres copias, diez años
Tiempo de referencia	Tiempo de ingesta
Colocaciones	El día 0, conserve tres copias replicadas durante 10 años (3652 días), una en el Sitio 1, una en el Sitio 2 y una en el Sitio 3. Al cabo de 10 años, elimine todas las copias del objeto.

Regla 2 de ILM, por ejemplo 4: Guardar dos copias de versiones no actuales durante 2 años

Esta regla ILM de ejemplo almacena dos copias de las versiones no actuales de un objeto versionado S3 durante 2 años.

Dado que la regla 1 de ILM se aplica a todas las versiones del objeto, debe crear otra regla para filtrar las versiones no actuales.

Para crear una regla que use "Hora no actual" como hora de referencia, seleccione **Sí** para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?" en el Paso 1 (Ingresar detalles) del asistente Crear una regla de ILM. Cuando selecciona **Sí**, se selecciona automáticamente *Hora no actual* como hora de referencia y no puede seleccionar una hora de referencia diferente.

1

Enter details

2

Define placements

3

Select ingest behavior

Rule name

Older Object Versions: Two Copies Two Years

Description (optional)

Older versions only

Basic filters (optional)

Specify which tenant accounts and buckets this rule applies to.

Tenant accounts ?

Select tenant accounts

Bucket name ?

matches all

Apply this rule to older object versions only (in S3 buckets with versioning enabled)? ?

☐ No ☒ Yes

En este ejemplo, solo se almacenan dos copias de las versiones no actuales, y esas copias se almacenarán durante dos años.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Dos grupos de almacenamiento, cada uno en diferentes centros de datos, Sitio 1 y Sitio 2.
Nombre de la regla	Versiones no actuales: dos copias dos años
Tiempo de referencia	Tiempo no actual Se selecciona automáticamente cuando selecciona Sí para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?" en el asistente Crear una regla de ILM.
Colocaciones	El día 0 en relación con el tiempo no actual (es decir, a partir del día en que la versión del objeto se convierte en la versión no actual), mantenga dos copias replicadas de las versiones no actuales del objeto durante 2 años (730 días), una en el Sitio 1 y otra en el Sitio 2. Al cabo de 2 años, elimine las versiones no actuales.

Política de ILM para el ejemplo 4: objetos versionados S3

Si desea administrar versiones anteriores de un objeto de forma diferente a la versión actual, las reglas que utilizan "Hora no actual" como hora de referencia deben aparecer en la política ILM antes que las reglas que se aplican a la versión actual del objeto.

Una política ILM para objetos versionados S3 podría incluir reglas ILM como las siguientes:

- Conserve cualquier versión anterior (no actual) de cada objeto durante 2 años, a partir del día en que la versión dejó de estar actual.



Las reglas de "Hora no actual" deben aparecer en la política antes de las reglas que se aplican a la versión actual del objeto. De lo contrario, las versiones de objetos no actuales nunca coincidirán con la regla "Tiempo no actual".

- Al momento de la ingesta, cree tres copias replicadas y almacene una copia en cada uno de los tres sitios. Conserve copias de la versión actual del objeto durante 10 años.

Al simular la política de ejemplo, esperaría que los objetos de prueba se evaluarán de la siguiente manera:

- Cualquier versión de objeto no actual se corresponderá con la primera regla. Si una versión no actual de un objeto tiene más de 2 años, ILM la elimina de forma permanente (todas las copias de la versión no actual se eliminan de la red).
- La versión actual del objeto coincidiría con la segunda regla. Cuando la versión actual del objeto se ha almacenado durante 10 años, el proceso ILM agrega un marcador de eliminación como la versión actual del objeto y hace que la versión anterior del objeto sea "no actual". La próxima vez que se realiza una evaluación ILM, esta versión no actual coincide con la primera regla. Como resultado, la copia en el Sitio 3 se elimina y las dos copias en el Sitio 1 y el Sitio 2 se almacenan durante 2 años más.

Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto

Puede utilizar un filtro de ubicación y el comportamiento de ingesta estricta en una regla para evitar que los objetos se guarden en una ubicación de centro de datos en particular.

En este ejemplo, un inquilino con sede en París no quiere almacenar algunos objetos fuera de la UE debido a cuestiones regulatorias. Otros objetos, incluidos todos los objetos de otras cuentas de inquilinos, se pueden almacenar en el centro de datos de París o en el centro de datos de EE. UU.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlrela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Información relacionada

- ["Opciones de ingesta"](#)
- ["Crear regla de ILM: Seleccionar comportamiento de ingesta"](#)

Regla 1 de ILM, por ejemplo 5: Ingesta estricta para garantizar el centro de datos de París

Esta regla ILM de ejemplo utiliza el comportamiento de ingesta estricta para garantizar que los objetos guardados por un inquilino con sede en París en depósitos S3 con la región configurada en eu-west-3 (París) nunca se almacenen en el centro de datos de EE. UU.

Esta regla se aplica a los objetos que pertenecen al inquilino de París y que tienen la región de depósito S3

establecida en eu-west-3 (París).

Definición de regla	Valor de ejemplo
Cuenta de inquilino	inquilino de París
Filtro avanzado	La restricción de ubicación es igual a eu-west-3
Pools de almacenamiento	Sitio 1 (París)
Nombre de la regla	Ingesta estricta para garantizar el centro de datos de París
Tiempo de referencia	Tiempo de ingesta
Colocaciones	El día 0, conserve dos copias replicadas para siempre en el Sitio 1 (París)
Comportamiento de ingesta	Estricto. Utilice siempre las ubicaciones de esta regla al ingerir. La ingesta falla si no es posible almacenar dos copias del objeto en el centro de datos de París.

Strict ingest to guarantee Paris data center

Compliant: Yes

Used in active policy: No

Used in proposed policy: No

Ingest behavior: Strict

Reference time: Ingest time

Clone

Edit

Remove

Filters

This rule applies if:

- Tenant is Paris tenant

And it only applies if objects have this metadata:

- Location constraint is eu-west-3

Time period and placements

Retention diagram

Placement instructions

Sort placements by

Time period

Storage pool

● Replicated copy

Rule analysis:

- StorageGRID site-loss protection will not apply from Day 0 - Forever.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Site 1

Duration

Forever

Regla 2 de ILM, por ejemplo 5: Ingesta equilibrada para otros objetos

Esta regla ILM de ejemplo utiliza el comportamiento de ingesta equilibrada para proporcionar una eficiencia ILM óptima para cualquier objeto que no coincida con la primera regla. Se almacenarán dos copias de todos los objetos que coincidan con esta regla: una en el centro de datos de EE. UU. y otra en el centro de datos de París. Si la regla no puede cumplirse inmediatamente, se almacenan copias provisionales en cualquier ubicación disponible.

Esta regla se aplica a los objetos que pertenecen a cualquier inquilino y a cualquier región.

Definición de regla	Valor de ejemplo
Cuenta de inquilino	Ignorar
Filtro avanzado	<i>No especificado</i>
Pools de almacenamiento	Sitio 1 (París) y Sitio 2 (EE. UU.)
Nombre de la regla	2 copias 2 centros de datos
Tiempo de referencia	Tiempo de ingesta
Colocaciones	El día 0, mantenga dos copias replicadas para siempre en dos centros de datos
Comportamiento de ingesta	Equilibrado. Los objetos que coinciden con esta regla se colocan de acuerdo con las instrucciones de ubicación de la regla, si es posible. De lo contrario, se realizan copias provisionales en cualquier lugar disponible.

Política ILM para el ejemplo 5: Combinación de comportamientos de ingesta

La política ILM de ejemplo incluye dos reglas que tienen diferentes comportamientos de ingesta.

Una política ILM que utiliza dos comportamientos de ingesta diferentes podría incluir reglas ILM como las siguientes:

- Almacene los objetos que pertenecen al inquilino de París y que tienen la región de depósito S3 configurada en eu-west-3 (París) solo en el centro de datos de París. Error en la ingesta si el centro de datos de París no está disponible.
- Almacene todos los demás objetos (incluidos aquellos que pertenecen al inquilino de París pero que tienen una región de depósito diferente) tanto en el centro de datos de EE. UU. como en el centro de datos de París. Haga copias provisionales en cualquier ubicación disponible si no se puede cumplir con las instrucciones de ubicación.

Al simular la política de ejemplo, espera que los objetos de prueba se evalúen de la siguiente manera:

- Todos los objetos que pertenecen al inquilino de París y que tienen la región de bucket S3 establecida en eu-west-3 coinciden con la primera regla y se almacenan en el centro de datos de París. Debido a que la primera regla utiliza ingesta estricta, estos objetos nunca se almacenan en el centro de datos de EE. UU. Si los nodos de almacenamiento en el centro de datos de París no están disponibles, la ingesta falla.

- Todos los demás objetos coinciden con la segunda regla, incluidos los objetos que pertenecen al inquilino de París y que no tienen la región de depósito S3 establecida en eu-west-3. Se guarda una copia de cada objeto en cada centro de datos. Sin embargo, debido a que la segunda regla utiliza ingesta equilibrada, si un centro de datos no está disponible, se guardan dos copias provisionales en cualquier ubicación disponible.

Ejemplo 6: Cambiar una política de ILM

Si necesita cambiar su protección de datos o agrega nuevos sitios, puede crear y activar una nueva política ILM.

Antes de cambiar una política, debe comprender cómo los cambios en las ubicaciones de ILM pueden afectar temporalmente el rendimiento general de un sistema StorageGRID .

En este ejemplo, se ha agregado un nuevo sitio StorageGRID en una expansión y se debe implementar una nueva política ILM activa para almacenar datos en el nuevo sitio. Para implementar una nueva política activa, primero ["crear una política"](#) . Después, debes ["simular"](#) y luego ["activar"](#) La nueva política.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlrela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Cómo afecta el cambio de una política de ILM al rendimiento

Cuando activa una nueva política ILM, el rendimiento de su sistema StorageGRID podría verse afectado temporalmente, especialmente si las instrucciones de ubicación de la nueva política requieren que muchos objetos existentes se muevan a nuevas ubicaciones.

Cuando activa una nueva política ILM, StorageGRID la utiliza para administrar todos los objetos, incluidos los objetos existentes y los objetos recientemente ingeridos. Antes de activar una nueva política ILM, revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente podría generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

Para garantizar que una nueva política de ILM no afecte la ubicación de los objetos replicados y codificados por borrado existentes, puede ["crear una regla ILM con un filtro de tiempo de ingesta"](#) . Por ejemplo, **La hora de ingesta es el o después de <fecha y hora>**, de modo que la nueva regla se aplica solo a los objetos ingeridos en o después de la fecha y hora especificadas.

Los tipos de cambios de política de ILM que pueden afectar temporalmente el rendimiento de StorageGRID incluyen los siguientes:

- Aplicar un perfil de codificación de borrado diferente a objetos con codificación de borrado existentes.



StorageGRID considera que cada perfil de codificación de borrado es único y no reutiliza fragmentos de codificación de borrado cuando se utiliza un nuevo perfil.

- Cambiar el tipo de copias necesarias para los objetos existentes; por ejemplo, convertir un gran porcentaje de objetos replicados en objetos con código de borrado.
- Mover copias de objetos existentes a una ubicación completamente diferente; por ejemplo, mover una gran cantidad de objetos hacia o desde un grupo de almacenamiento en la nube o hacia o desde un sitio remoto.

Política ILM activa, por ejemplo 6: Protección de datos en dos sitios

En este ejemplo, la política ILM activa se diseñó inicialmente para un sistema StorageGRID de dos sitios y utiliza dos reglas ILM.

Active policy

Policy history

Policy name:

Data Protection for Two Sites (2 rules)

Reason for change :

Data protection for two sites (using 2 rules)

Start date:

2022-10-11 10:37:11 MDT

Simulate

Policy rules

Retention diagram

Rule order ?	Rule name	Filters ?
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

En esta política ILM, los objetos que pertenecen al inquilino A están protegidos mediante codificación de borrado 2+1 en un solo sitio, mientras que los objetos que pertenecen a todos los demás inquilinos están protegidos en dos sitios mediante replicación de 2 copias.

Regla 1: Codificación de borrado de un sitio para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de la regla	Codificación de borrado de un sitio para el inquilino A
Cuenta de inquilino	Inquilino A
Pool de almacenamiento	Sitio 1
Colocaciones	Codificación de borrado 2+1 en el Sitio 1 desde el día 0 hasta la eternidad

Regla 2: Replicación en dos sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de la regla	Replicación de dos sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Sitio 1 y Sitio 2

Definición de regla	Valor de ejemplo
Colocaciones	Dos copias replicadas desde el día 0 hasta siempre: una copia en el Sitio 1 y una copia en el Sitio 2.

Política de ILM, ejemplo 6: Protección de datos en tres sitios

En este ejemplo, la política ILM se reemplaza por una nueva política para un sistema StorageGRID de tres sitios.

Después de realizar una expansión para agregar el nuevo sitio, el administrador de la red creó dos nuevos grupos de almacenamiento: un grupo de almacenamiento para el Sitio 3 y un grupo de almacenamiento que contiene los tres sitios (no el mismo que el grupo de almacenamiento predeterminado Todos los nodos de almacenamiento). Luego, el administrador creó dos nuevas reglas ILM y una nueva política ILM, diseñada para proteger los datos en los tres sitios.

Cuando se activa esta nueva política ILM, los objetos que pertenecen al Inquilino A estarán protegidos mediante codificación de borrado 2+1 en tres sitios, mientras que los objetos que pertenecen a otros inquilinos (y objetos más pequeños que pertenecen al Inquilino A) estarán protegidos en tres sitios mediante replicación de 3 copias.

Regla 1: Codificación de borrado de tres sitios para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de la regla	Codificación de borrado de tres sitios para el inquilino A
Cuenta de inquilino	Inquilino A
Pool de almacenamiento	Los 3 sitios (incluye el Sitio 1, el Sitio 2 y el Sitio 3)
Colocaciones	Codificación de borrado 2+1 en los 3 sitios desde el día 0 hasta siempre

Regla 2: Replicación en tres sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de la regla	Réplica de tres sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Sitio 1, Sitio 2 y Sitio 3
Colocaciones	Tres copias replicadas desde el día 0 hasta siempre: una copia en el Sitio 1, una copia en el Sitio 2 y una copia en el Sitio 3.

Activación de la política ILM por ejemplo 6

Cuando se activa una nueva política ILM, es posible que los objetos existentes se muevan a nuevas

ubicaciones o que se creen nuevas copias de objetos existentes, según las instrucciones de ubicación de cualquier regla nueva o actualizada.



Los errores en una política ILM pueden provocar una pérdida de datos irrecuperable. Revise cuidadosamente y simule la política antes de activarla para confirmar que funcionará según lo previsto.



Cuando activa una nueva política ILM, StorageGRID la utiliza para administrar todos los objetos, incluidos los objetos existentes y los objetos recientemente ingeridos. Antes de activar una nueva política ILM, revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente podría generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

¿Qué sucede cuando cambian las instrucciones de codificación de borrado?

En la política ILM actualmente activa para este ejemplo, los objetos que pertenecen al inquilino A están protegidos mediante codificación de borrado 2+1 en el sitio 1. En la nueva política ILM, los objetos que pertenecen al inquilino A estarán protegidos mediante codificación de borrado 2+1 en los sitios 1, 2 y 3.

Cuando se activa la nueva política ILM, se producen las siguientes operaciones ILM:

- Los nuevos objetos ingeridos por el inquilino A se dividen en dos fragmentos de datos y se agrega un fragmento de paridad. Luego, cada uno de los tres fragmentos se almacena en un sitio diferente.
- Los objetos existentes que pertenecen al inquilino A se vuelven a evaluar durante el proceso de escaneo ILM en curso. Debido a que las instrucciones de colocación de ILM utilizan un nuevo perfil de codificación de borrado, se crean fragmentos codificados de borrado completamente nuevos y se distribuyen a los tres sitios.



Los fragmentos 2+1 existentes en el Sitio 1 no se reutilizan. StorageGRID considera que cada perfil de codificación de borrado es único y no reutiliza fragmentos de codificación de borrado cuando se utiliza un nuevo perfil.

¿Qué sucede cuando cambian las instrucciones de replicación?

En la política ILM actualmente activa para este ejemplo, los objetos que pertenecen a otros inquilinos están protegidos mediante dos copias replicadas en grupos de almacenamiento en los sitios 1 y 2. En la nueva política de ILM, los objetos que pertenecen a otros inquilinos estarán protegidos mediante tres copias replicadas en grupos de almacenamiento en los sitios 1, 2 y 3.

Cuando se activa la nueva política ILM, se producen las siguientes operaciones ILM:

- Cuando cualquier inquilino que no sea el inquilino A ingiere un nuevo objeto, StorageGRID crea tres copias y guarda una copia en cada sitio.
- Los objetos existentes que pertenecen a estos otros inquilinos se vuelven a evaluar durante el proceso de escaneo ILM en curso. Dado que las copias de objetos existentes en el Sitio 1 y el Sitio 2 continúan satisfaciendo los requisitos de replicación de la nueva regla ILM, StorageGRID solo necesita crear una nueva copia del objeto para el Sitio 3.

Impacto en el rendimiento de la activación de esta política

Cuando se activa la política ILM en este ejemplo, el rendimiento general de este sistema StorageGRID se verá afectado temporalmente. Se requerirán niveles de recursos de red superiores a los normales para crear

nuevos fragmentos con código de borrado para los objetos existentes del Inquilino A y nuevas copias replicadas en el Sitio 3 para los objetos existentes de otros inquilinos.

Como resultado del cambio de política de ILM, las solicitudes de lectura y escritura del cliente podrían experimentar temporalmente latencias más altas de lo normal. Las latencias volverán a los niveles normales después de que las instrucciones de ubicación se implementen completamente en toda la red.

Para evitar problemas de recursos al activar una nueva política ILM, puede usar el filtro avanzado Tiempo de ingesta en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de ingesta para que sea mayor o igual al tiempo aproximado en que entrará en vigencia la nueva política para garantizar que los objetos existentes no se muevan innecesariamente.



Comuníquese con el soporte técnico si necesita reducir o aumentar la velocidad a la que se procesan los objetos después de un cambio de política de ILM.

Ejemplo 7: Política ILM compatible con el bloqueo de objetos S3

Puede usar el depósito S3, las reglas ILM y la política ILM en este ejemplo como punto de partida al definir una política ILM para cumplir con los requisitos de protección y retención de objetos para objetos en depósitos con el bloqueo de objetos S3 habilitado.



Si utilizó la función de Cumplimiento heredada en versiones anteriores de StorageGRID , también puede usar este ejemplo para ayudar a administrar cualquier depósito existente que tenga habilitada la función de Cumplimiento heredada.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlere la para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Información relacionada

- ["Administrar objetos con S3 Object Lock"](#)
- ["Crear una política ILM"](#)

Ejemplo de bloqueo de objetos y cubos para S3

En este ejemplo, una cuenta de inquilino S3 llamada Bank of ABC utilizó el Administrador de inquilinos para crear un depósito con el Bloqueo de objetos S3 habilitado para almacenar registros bancarios críticos.

Definición de cubo	Valor de ejemplo
Nombre de la cuenta del inquilino	Banco de ABC
Nombre del depósito	registros bancarios
Región del cubo	us-east-1 (predeterminado)

Cada objeto y versión de objeto que se agrega al depósito de registros bancarios utilizará los siguientes valores para `retain-until-date` y `legal hold` ajustes.

Configuración para cada objeto	Valor de ejemplo
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 de diciembre de 2030) Cada versión del objeto tiene su propia <code>retain-until-date</code> configuración. Este ajuste se puede aumentar, pero no disminuir.
<code>legal hold</code>	"OFF" (Sin efecto) Se puede colocar o levantar una retención legal sobre cualquier versión de un objeto en cualquier momento durante el período de retención. Si un objeto se encuentra bajo una retención legal, el objeto no se puede eliminar incluso si <code>retain-until-date</code> Se ha alcanzado.

Ejemplo de regla 1 de ILM para bloqueo de objetos S3: Perfil de codificación de borrado con coincidencia de depósito

Esta regla ILM de ejemplo se aplica únicamente a la cuenta de inquilino S3 denominada Banco ABC. Coincide con cualquier objeto del `bank-records` y luego utiliza codificación de borrado para almacenar el objeto en nodos de almacenamiento en tres sitios de centros de datos utilizando un perfil de codificación de borrado 6+3. Esta regla satisface los requisitos de los depósitos con el bloqueo de objetos S3 habilitado: se conserva una copia en los nodos de almacenamiento desde el día 0 hasta siempre, utilizando el tiempo de ingesta como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de la regla	Norma de cumplimiento: Objetos CE en el contenedor de registros bancarios - Banco ABC
Cuenta de inquilino	Banco de ABC
Nombre del depósito	<code>bank-records</code>
Filtro avanzado	Tamaño del objeto (MB) mayor a 1 Nota: Este filtro garantiza que la codificación de borrado no se utilice para objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Colocaciones	Desde el día 0 tienda para siempre
Perfil de codificación de borrado	• Cree una copia con código de borrado en los nodos de almacenamiento en tres sitios de centros de datos • Utiliza el esquema de codificación de borrado 6+3

Regla 2 de ILM para el ejemplo de bloqueo de objetos S3: regla no conforme

Esta regla ILM de ejemplo almacena inicialmente dos copias de objetos replicados en los nodos de almacenamiento. Después de un año, almacena una copia en un grupo de almacenamiento en la nube para siempre. Debido a que esta regla utiliza un grupo de almacenamiento en la nube, no es compatible y no se aplicará a los objetos en depósitos con el bloqueo de objetos S3 habilitado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Regla no conforme: utilizar el grupo de almacenamiento en la nube
Cuentas de inquilinos	No especificado
Nombre del depósito	No se especifica, pero solo se aplicará a los depósitos que no tengan habilitado el bloqueo de objetos S3 (o la función de cumplimiento heredada).
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Colocaciones	• El día 0, mantenga dos copias replicadas en los nodos de almacenamiento del centro de datos 1 y del centro de datos 2 durante 365 días • Después de 1 año, conserve una copia replicada en un grupo de almacenamiento en la nube para siempre

Regla 3 de ILM para el ejemplo de bloqueo de objetos S3: regla predeterminada

Esta regla ILM de ejemplo copia datos de objetos en grupos de almacenamiento en dos centros de datos. Esta regla de cumplimiento está diseñada para ser la regla predeterminada en la política ILM. No incluye ningún filtro, no utiliza el tiempo de referencia no actual y satisface los requisitos de los buckets con S3 Object Lock habilitado: se mantienen dos copias de objetos en los nodos de almacenamiento desde el día 0 hasta siempre, utilizando la ingesta como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de la regla	Regla de cumplimiento predeterminada: Dos copias, dos centros de datos
Cuenta de inquilino	No especificado
Nombre del depósito	No especificado
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Colocaciones	Desde el día 0 y para siempre, conserve dos copias replicadas: una en los nodos de almacenamiento del centro de datos 1 y otra en los nodos de almacenamiento del centro de datos 2.

Ejemplo de política ILM compatible con bloqueo de objetos S3

Para crear una política ILM que proteja eficazmente todos los objetos de su sistema, incluidos aquellos en depósitos con el bloqueo de objetos S3 habilitado, debe seleccionar reglas ILM que satisfagan los requisitos de almacenamiento de todos los objetos. Luego debes simular y activar la política.

Agregar reglas a la política

En este ejemplo, la política ILM incluye tres reglas ILM, en el siguiente orden:

1. Una regla compatible que utiliza codificación de borrado para proteger objetos de más de 1 MB en un depósito específico con S3 Object Lock habilitado. Los objetos se almacenan en nodos de almacenamiento desde el día 0 hasta siempre.
2. Una regla no conforme que crea dos copias de objetos replicados en nodos de almacenamiento durante un año y luego mueve una copia de objeto a un grupo de almacenamiento en la nube para siempre. Esta regla no se aplica a los depósitos con el bloqueo de objetos S3 habilitado porque utiliza un grupo de almacenamiento en la nube.
3. La regla compatible predeterminada que crea dos copias de objetos replicados en los nodos de almacenamiento desde el día 0 hasta siempre.

Simular la política

Después de haber agregado reglas a su política, elegido una regla compatible predeterminada y organizado las otras reglas, debe simular la política probando objetos del depósito con S3 Object Lock habilitado y de otros depósitos. Por ejemplo, al simular la política de ejemplo, esperaría que los objetos de prueba se evaluarán de la siguiente manera:

- La primera regla solo coincidirá con objetos de prueba que tengan más de 1 MB en el depósito de registros bancarios para el inquilino del Banco de ABC.
- La segunda regla hará coincidir todos los objetos en todos los depósitos no compatibles para todas las demás cuentas de inquilino.
- La regla predeterminada coincidirá con estos objetos:
 - Objetos de 1 MB o menos en el depósito de registros bancarios para el inquilino del Banco ABC.
 - Objetos en cualquier otro depósito que tenga habilitado el bloqueo de objetos S3 para todas las demás cuentas de inquilino.

Activar la política

Cuando esté completamente satisfecho de que la nueva política protege los datos del objeto como se esperaba, puede activarla.

Ejemplo 8: Prioridades para el ciclo de vida del depósito S3 y la política de ILM

Según la configuración de su ciclo de vida, los objetos siguen las configuraciones de retención del ciclo de vida del bucket S3 o de una política ILM.

Ejemplo de cómo el ciclo de vida del bucket tiene prioridad sobre la política de ILM

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conservar X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminada): el día 0, conservar X copias durante 50 días

Ciclo de vida del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Resultado

- Se ingiere un objeto llamado "docs/text". Coincide con el filtro del ciclo de vida del depósito del prefijo "docs/".
 - Después de 100 días, se crea un marcador de eliminación y "docs/text" deja de estar actualizado.
 - Después de 5 días, un total de 105 días desde la ingesta, se elimina "docs/text".
 - Después de 95 días, un total de 200 días desde la ingesta y 100 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación vencido.
- Se ingiere un objeto llamado "video/película". No coincide con el filtro y utiliza la política de retención ILM.
 - Después de 50 días, se crea un marcador de eliminación y el archivo "video/película" deja de estar vigente.
 - Después de 20 días, un total de 70 días desde la ingesta, se elimina "video/película".
 - Después de 30 días, un total de 100 días desde la ingesta y 50 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación vencido.

Ejemplo de ciclo de vida de un bucket que implícitamente se mantiene para siempre

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conservar X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminada): el día 0, conservar X copias durante 50 días

Ciclo de vida del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":  
true}
```

Resultado

- Se ingiere un objeto llamado "docs/text". Coincide con el filtro del ciclo de vida del depósito del prefijo "docs/".

El `Expiration` La acción se aplica solo a los marcadores de eliminación vencidos, lo que implica mantener todo lo demás para siempre (comenzando con "docs/").

Los marcadores de eliminación que comienzan con "docs/" se eliminan cuando caducan.

- Se ingiere un objeto llamado "video/película". No coincide con el filtro y utiliza la política de retención ILM.
 - Después de 50 días, se crea un marcador de eliminación y el archivo "video/película" deja de estar vigente.
 - Después de 20 días, un total de 70 días desde la ingesta, se elimina "video/película".
 - Después de 30 días, un total de 100 días desde la ingesta y 50 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación vencido.

Ejemplo de uso del ciclo de vida del bucket para duplicar ILM y limpiar marcadores de eliminación vencidos

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conservar X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminada): el día 0, conservar X copias para siempre

Ciclo de vida del bucket

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Resultado

- La política ILM se duplica en el ciclo de vida del depósito.
 - La regla permanente de la política ILM está diseñada para eliminar objetos manualmente y limpiar versiones no actuales después de 20 días. En consecuencia, la regla de tiempo de ingesta mantendrá los marcadores de eliminación vencidos para siempre.
 - El ciclo de vida del depósito duplica el comportamiento de la política ILM al agregar "ExpiredObjectDeleteMarker": true, que elimina los marcadores de eliminación una vez que han expirado
- Se ingiere un objeto. Sin filtro significa que el ciclo de vida del depósito se aplica a todos los objetos y anula las configuraciones de retención de ILM.
 - Cuando un inquilino emite una solicitud de eliminación de un objeto, se crea un marcador de eliminación y el objeto deja de ser actual.
 - Después de 20 días, el objeto no actual se elimina y el marcador de eliminación caduca.
 - Poco después, se elimina el marcador de eliminación caducado.

Endurecimiento del sistema

Consideraciones generales para el fortalecimiento del sistema

El fortalecimiento del sistema es el proceso de eliminar tantos riesgos de seguridad como sea posible de un sistema StorageGRID .

A medida que instala y configura StorageGRID, utilice estas pautas para ayudarlo a cumplir con los objetivos de seguridad prescritos en materia de confidencialidad, integridad y disponibilidad.

Ya debería estar utilizando las mejores prácticas estándar de la industria para el fortalecimiento del sistema. Por ejemplo, utiliza contraseñas seguras para StorageGRID, usa HTTPS en lugar de HTTP y habilita la

autenticación basada en certificados cuando esté disponible.

StorageGRID sigue las ["Política de gestión de vulnerabilidades de NetApp"](#) . Las vulnerabilidades reportadas se verifican y abordan de acuerdo con el proceso de respuesta a incidentes de seguridad del producto.

Al fortalecer un sistema StorageGRID , tenga en cuenta lo siguiente:

- ¿*Cuál de las tres redes StorageGRID * ha implementado? Todos los sistemas StorageGRID deben usar la red Grid, pero también es posible que utilice la red de administración, la red de cliente o ambas. Cada red tiene diferentes consideraciones de seguridad.
- **El tipo de plataformas** que utiliza para los nodos individuales en su sistema StorageGRID . Los nodos StorageGRID se pueden implementar en máquinas virtuales VMware, dentro de un motor de contenedores en hosts Linux o como dispositivos de hardware dedicados. Cada tipo de plataforma tiene su propio conjunto de mejores prácticas de fortalecimiento.
- **Qué tan confiables son las cuentas de los inquilinos.** Si usted es un proveedor de servicios con cuentas de inquilinos que no son de confianza, tendrá preocupaciones de seguridad diferentes que si solo utiliza inquilinos internos y de confianza.
- **Qué requisitos y convenciones de seguridad** sigue su organización. Es posible que deba cumplir con requisitos corporativos o regulatorios específicos.

Pautas de refuerzo para las actualizaciones de software

Debe mantener su sistema StorageGRID y los servicios relacionados actualizados para defenderse de los ataques.

Actualizaciones del software StorageGRID

Siempre que sea posible, debe actualizar el software StorageGRID a la versión principal más reciente o a la versión principal anterior. Mantener StorageGRID actualizado ayuda a reducir la cantidad de tiempo que las vulnerabilidades conocidas están activas y reduce la superficie de ataque general. Además, las versiones más recientes de StorageGRID a menudo contienen funciones de refuerzo de seguridad que no están incluidas en versiones anteriores.

Consultar el ["Herramienta de matriz de interoperabilidad de NetApp"](#) (IMT) para determinar qué versión del software StorageGRID debería utilizar. Cuando se requiere una revisión, NetApp prioriza la creación de actualizaciones para las versiones más recientes. Es posible que algunos parches no sean compatibles con versiones anteriores.

- Para descargar las versiones y revisiones más recientes de StorageGRID , vaya a ["Descargas de NetApp : StorageGRID"](#) .
- Para actualizar el software StorageGRID , consulte la ["instrucciones de actualización"](#) .
- Para aplicar una revisión, consulte la ["Procedimiento de revisión de StorageGRID"](#) .

Actualizaciones de servicios externos

Los servicios externos pueden tener vulnerabilidades que afecten a StorageGRID indirectamente. Debe asegurarse de que los servicios de los que depende StorageGRID se mantengan actualizados. Estos servicios incluyen LDAP, KMS (o servidor KMIP), DNS y NTP.

Para obtener una lista de las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#) .

Actualizaciones de hipervisores

Si sus nodos StorageGRID se ejecutan en VMware u otro hipervisor, debe asegurarse de que el software y el firmware del hipervisor estén actualizados.

Para obtener una lista de las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#).

Actualizaciones a nodos Linux

Si sus nodos StorageGRID utilizan plataformas de host Linux, debe asegurarse de que las actualizaciones de seguridad y las actualizaciones del kernel se apliquen al sistema operativo host. Además, debe aplicar actualizaciones de firmware al hardware vulnerable cuando estas actualizaciones estén disponibles.

Para obtener una lista de las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#).

Pautas de fortalecimiento para redes StorageGRID

El sistema StorageGRID admite hasta tres interfaces de red por nodo de red, lo que le permite configurar la red para cada nodo de red individual para que coincida con sus requisitos de seguridad y acceso.

Para obtener información detallada sobre las redes StorageGRID, consulte la ["Tipos de red StorageGRID"](#).

Directrices para la red Grid

Debe configurar una red Grid para todo el tráfico interno de StorageGRID. Todos los nodos de la red están en la red de red y deben poder comunicarse con todos los demás nodos.

Al configurar la red Grid, siga estas pautas:

- Asegúrese de que la red esté protegida contra clientes que no sean de confianza, como aquellos en Internet abierto.
- Cuando sea posible, utilice la red Grid exclusivamente para el tráfico interno. Tanto la red de administración como la red de cliente tienen restricciones de firewall adicionales que bloquean el tráfico externo a los servicios internos. Se admite el uso de la red Grid para el tráfico de clientes externos, pero este uso ofrece menos capas de protección.
- Si la implementación de StorageGRID abarca varios centros de datos, utilice una red privada virtual (VPN) o equivalente en la red Grid para brindar protección adicional para el tráfico interno.
- Algunos procedimientos de mantenimiento requieren acceso a shell seguro (SSH) en el puerto 22 entre el nodo de administración principal y todos los demás nodos de la red. Utilice un firewall externo para restringir el acceso SSH a clientes confiables.

Pautas para la red de administración

La red de administración generalmente se utiliza para tareas administrativas (empleados de confianza que utilizan Grid Manager o SSH) y para comunicarse con otros servicios de confianza como LDAP, DNS, NTP o KMS (o servidor KMIP). Sin embargo, StorageGRID no exige este uso internamente.

Si está utilizando la red de administración, siga estas pautas:

- Bloquear todos los puertos de tráfico interno en la red de administración. Ver el ["lista de puertos internos"](#) .
- Si los clientes no confiables pueden acceder a la red de administración, bloquee el acceso a StorageGRID en la red de administración con un firewall externo.

Directrices para la red de clientes

La red de cliente normalmente se utiliza para inquilinos y para comunicarse con servicios externos, como el servicio de replicación CloudMirror u otro servicio de plataforma. Sin embargo, StorageGRID no exige este uso internamente.

Si está utilizando la red de cliente, siga estas pautas:

- Bloquear todos los puertos de tráfico interno en la red del cliente. Ver el ["lista de puertos internos"](#) .
- Acepte el tráfico de clientes entrante solo en puntos finales configurados explícitamente. Ver la información sobre ["gestión de controles de firewall"](#) .

Pautas de refuerzo para nodos StorageGRID

Los nodos StorageGRID se pueden implementar en máquinas virtuales VMware, dentro de un motor de contenedores en hosts Linux o como dispositivos de hardware dedicados. Cada tipo de plataforma y cada tipo de nodo tiene su propio conjunto de mejores prácticas de fortalecimiento.

Controlar el acceso remoto de IPMI a BMC

Puede habilitar o deshabilitar el acceso IPMI remoto para todos los dispositivos que contengan un BMC. La interfaz IPMI remota permite el acceso de hardware de bajo nivel a sus dispositivos StorageGRID por parte de cualquier persona con una cuenta y contraseña de BMC . Si no necesita acceso IPMI remoto al BMC, desactive esta opción.

- Para controlar el acceso remoto de IPMI al BMC en Grid Manager, vaya a **CONFIGURACIÓN > Seguridad > Configuración de seguridad > Dispositivos**:
 - Desmarque la casilla de verificación **Habilitar acceso IPMI remoto** para deshabilitar el acceso IPMI al BMC.
 - Seleccione la casilla de verificación **Habilitar acceso IPMI remoto** para habilitar el acceso IPMI al BMC.

Configuración del firewall

Como parte del proceso de fortalecimiento del sistema, debe revisar las configuraciones del firewall externo y modificarlas para que el tráfico se acepte solo desde las direcciones IP y en los puertos desde los que es estrictamente necesario.

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad de su red al permitirle controlar el acceso de la red al nodo. Debería ["Administrar los controles internos del firewall"](#) para evitar el acceso a la red en todos los puertos excepto aquellos necesarios para su implementación de red específica. Los cambios de configuración que realice en la página de control del Firewall se implementarán en cada nodo.

En concreto, puedes gestionar estas áreas:

- **Direcciones privilegiadas**: puede permitir que direcciones IP o subredes seleccionadas accedan a puertos que estén cerrados por la configuración en la pestaña Administrar acceso externo.

- **Administrar acceso externo:** puedes cerrar puertos que están abiertos por defecto, o reabrir puertos previamente cerrados.
- **Red de cliente no confiable:** puede especificar si un nodo confía en el tráfico entrante de la red de cliente, así como los puertos adicionales que desea que estén abiertos cuando se configura la red de cliente no confiable.

Si bien este firewall interno proporciona una capa adicional de protección contra algunas amenazas comunes, no elimina la necesidad de un firewall externo.

Para obtener una lista de todos los puertos internos y externos utilizados por StorageGRID, consulte ["Referencia del puerto de red"](#).

Deshabilitar servicios no utilizados

Para todos los nodos de StorageGRID, debe deshabilitar o bloquear el acceso a los servicios no utilizados. Por ejemplo, si no planea utilizar DHCP, utilice el Administrador de cuadrícula para cerrar el puerto 68. Seleccione **CONFIGURACIÓN > Control de firewall > Administrar acceso externo**. A continuación, cambie el interruptor de estado del puerto 68 de **Abierto** a **Cerrado**.

Virtualización, contenedores y hardware compartido

Para todos los nodos de StorageGRID, evite ejecutar StorageGRID en el mismo hardware físico que software no confiable. No asuma que las protecciones del hipervisor evitarán que el malware acceda a los datos protegidos por StorageGRID si tanto StorageGRID como el malware existen en el mismo hardware físico. Por ejemplo, los ataques Meltdown y Spectre explotan vulnerabilidades críticas en los procesadores modernos y permiten que los programas roben datos de la memoria de la misma computadora.

Proteger los nodos durante la instalación

No permita que usuarios no confiables accedan a los nodos de StorageGRID a través de la red cuando se estén instalando los nodos. Los nodos no son completamente seguros hasta que se unen a la red.

Pautas para los nodos de administración

Los nodos de administración brindan servicios de gestión como configuración del sistema, monitoreo y registro. Cuando inicia sesión en Grid Manager o Tenant Manager, se conecta a un nodo de administración.

Siga estas pautas para proteger los nodos de administración en su sistema StorageGRID :

- Proteja todos los nodos de administración de clientes que no sean de confianza, como aquellos en Internet abierto. Asegúrese de que ningún cliente no confiable pueda acceder a ningún nodo de administración en la red Grid, la red de administración o la red de clientes.
- Los grupos de StorageGRID controlan el acceso a las funciones de Grid Manager y Tenant Manager. Otorgue a cada grupo de usuarios los permisos mínimos requeridos para su rol y utilice el modo de acceso de solo lectura para evitar que los usuarios cambien la configuración.
- Al utilizar puntos finales del balanceador de carga StorageGRID, utilice nodos de puerta de enlace en lugar de nodos de administración para el tráfico de clientes que no sean de confianza.
- Si tiene inquilinos que no son de confianza, no les permita tener acceso directo al Administrador de inquilinos ni a la API de administración de inquilinos. En su lugar, haga que los inquilinos que no sean de confianza utilicen un portal de inquilinos o un sistema de gestión de inquilinos externo, que interactúe con la API de gestión de inquilinos.
- Opcionalmente, utilice un proxy de administración para tener más control sobre la comunicación de

AutoSupport desde los nodos de administración al soporte de NetApp . Vea los pasos para ["creando un proxy de administrador"](#) .

- Opcionalmente, utilice los puertos restringidos 8443 y 9443 para separar las comunicaciones entre Grid Manager y Tenant Manager. Bloquee el puerto compartido 443 y limite las solicitudes de inquilinos al puerto 9443 para obtener protección adicional.
- De manera opcional, utilice nodos de administración separados para administradores de red y usuarios inquilinos.

Para obtener más información, consulte las instrucciones para ["administración de StorageGRID"](#) .

Directrices para nodos de almacenamiento

Los nodos de almacenamiento administran y almacenan datos de objetos y metadatos. Siga estas pautas para proteger los nodos de almacenamiento en su sistema StorageGRID .

- No permita que clientes no confiables se conecten directamente a los nodos de almacenamiento. Utilice un punto final de balanceador de carga atendido por un nodo de puerta de enlace o un balanceador de carga de terceros.
- No habilite servicios salientes para inquilinos que no sean de confianza. Por ejemplo, al crear la cuenta para un inquilino que no es de confianza, no permita que el inquilino use su propia fuente de identidad y no permita el uso de los servicios de la plataforma. Vea los pasos para ["crear una cuenta de inquilino"](#) .
- Utilice un balanceador de carga de terceros para el tráfico de clientes que no sean de confianza. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques.
- De manera opcional, utilice un proxy de almacenamiento para tener más control sobre los grupos de almacenamiento en la nube y la comunicación de los servicios de la plataforma desde los nodos de almacenamiento a los servicios externos. Vea los pasos para ["creando un proxy de almacenamiento"](#) .
- Opcionalmente, conéctese a servicios externos utilizando la red del cliente. Luego, seleccione **CONFIGURACIÓN > Seguridad > Control de firewall > Redes de cliente no confiables** e indique que la red de cliente en el nodo de almacenamiento no es confiable. El nodo de almacenamiento ya no acepta tráfico entrante en la red del cliente, pero continúa permitiendo solicitudes salientes para los servicios de plataforma.

Directrices para los nodos de enlace

Los nodos de puerta de enlace proporcionan una interfaz de equilibrio de carga opcional que las aplicaciones cliente pueden usar para conectarse a StorageGRID. Siga estas pautas para proteger cualquier nodo de puerta de enlace en su sistema StorageGRID :

- Configurar y utilizar puntos finales del balanceador de carga. Ver ["Consideraciones para el equilibrio de carga"](#) .
- Utilice un equilibrador de carga de terceros entre el cliente y el nodo de puerta de enlace o los nodos de almacenamiento para el tráfico de clientes no confiables. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques. Si utiliza un balanceador de carga de terceros, el tráfico de red puede configurarse opcionalmente para pasar por un punto final del balanceador de carga interno o enviarse directamente a los nodos de almacenamiento.
- Si está utilizando puntos finales de balanceador de carga, opcionalmente puede hacer que los clientes se conecten a través de la red del cliente. Luego, seleccione **CONFIGURACIÓN > Seguridad > Control de firewall > Redes de clientes no confiables** e indique que la red de clientes en el nodo de puerta de enlace no es confiable. El nodo de puerta de enlace solo acepta tráfico entrante en los puertos configurados explícitamente como puntos finales del equilibrador de carga.

Directrices para los nodos de dispositivos de hardware

Los dispositivos de hardware StorageGRID están diseñados especialmente para su uso en un sistema StorageGRID. Algunos dispositivos pueden utilizarse como nodos de almacenamiento. Se pueden utilizar otros dispositivos como nodos de administración o nodos de puerta de enlace. Puede combinar nodos de dispositivos con nodos basados en software o implementar redes de dispositivos completamente diseñadas.

Siga estas pautas para proteger cualquier nodo de dispositivo de hardware en su sistema StorageGRID :

- Si el dispositivo utiliza SANtricity System Manager para la administración del controlador de almacenamiento, evite que los clientes no confiables accedan a SANtricity System Manager a través de la red.
- Si el dispositivo tiene un controlador de administración de placa base (BMC), tenga en cuenta que el puerto de administración de BMC permite el acceso al hardware de bajo nivel. Conecte el puerto de administración de BMC únicamente a una red de administración interna segura y confiable. Si no hay dicha red disponible, deje el puerto de administración de BMC desconectado o bloqueado, a menos que el soporte técnico solicite una conexión de BMC.
- Si el dispositivo admite la administración remota del hardware del controlador a través de Ethernet utilizando el estándar de Interfaz de administración de plataforma inteligente (IPMI), bloquee el tráfico no confiable en el puerto 623.



Puede habilitar o deshabilitar el acceso IPMI remoto para todos los dispositivos que contengan un BMC. La interfaz IPMI remota permite el acceso de hardware de bajo nivel a sus dispositivos StorageGRID por parte de cualquier persona con una cuenta y contraseña de BMC. Si no necesita acceso IPMI remoto al BMC, deshabilite esta opción utilizando uno de los siguientes métodos: + En Grid Manager, vaya a **CONFIGURACIÓN > Seguridad > Configuración de seguridad > Dispositivos** y desmarque la casilla de verificación **Habilitar acceso IPMI remoto**. + En la API de administración de Grid, use el punto final privado: PUT /private/bmc .

- Para los modelos de dispositivos que contienen unidades SED, FDE o FIPS NL-SAS que administra con SANtricity System Manager, "[Habilitar y configurar SANtricity Drive Security](#)".
- Para los modelos de dispositivos que contienen SSD NVMe SED o FIPS que administra mediante el instalador de dispositivos StorageGRID y el administrador de red, "[Habilitar y configurar el cifrado de unidad StorageGRID](#)".
- Para dispositivos sin unidades SED, FDE o FIPS, habilite y configure el cifrado del nodo de software StorageGRID "[utilizando un servidor de administración de claves \(KMS\)](#)".

Pautas de refuerzo para TLS y SSH

Debe reemplazar los certificados predeterminados creados durante la instalación y seleccionar la política de seguridad adecuada para las conexiones TLS y SSH.

Directrices de endurecimiento de los certificados

Debe reemplazar los certificados predeterminados creados durante la instalación con sus propios certificados personalizados.

Para muchas organizaciones, el certificado digital autofirmado para el acceso web de StorageGRID no cumple con sus políticas de seguridad de la información. En los sistemas de producción, debe instalar un certificado digital firmado por una CA para usarlo en la autenticación de StorageGRID.

En concreto, debe utilizar certificados de servidor personalizados en lugar de estos certificados predeterminados:

- **Certificado de interfaz de administración:** se utiliza para proteger el acceso al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos.
- **Certificado API S3:** se utiliza para proteger el acceso a los nodos de almacenamiento y los nodos de puerta de enlace, que las aplicaciones cliente S3 utilizan para cargar y descargar datos de objetos.

Ver ["Administrar certificados de seguridad"](#) para obtener más detalles e instrucciones.



StorageGRID administra los certificados utilizados para los puntos finales del equilibrador de carga por separado. Para configurar los certificados del balanceador de carga, consulte ["Configurar los puntos finales del balanceador de carga"](#).

Al utilizar certificados de servidor personalizados, siga estas pautas:

- Los certificados deben tener una `subjectAltName` que coincide con las entradas DNS para StorageGRID. Para obtener más detalles, consulte la sección 4.2.1.6, "Nombre alternativo del sujeto", en ["RFC 5280: Certificado PKIX y perfil CRL"](#).
- Siempre que sea posible, evite el uso de certificados comodín. Una excepción a esta directriz es el certificado para un punto final de estilo alojado virtual S3, que requiere el uso de un comodín si los nombres de los depósitos no se conocen de antemano.
- Cuando sea necesario utilizar comodines en los certificados, deberá tomar medidas adicionales para reducir los riesgos. Utilice un patrón comodín como `*.s3.example.com`, y no utilices el `s3.example.com` sufijo para otras aplicaciones. Este patrón también funciona con acceso S3 de estilo de ruta, como `dc1-s1.s3.example.com/mybucket`.
- Establezca tiempos de vencimiento de certificados cortos (por ejemplo, 2 meses) y utilice la API de administración de cuadrícula para automatizar la rotación de certificados. Esto es especialmente importante para los certificados comodín.

Además, los clientes deben utilizar una verificación estricta del nombre de host al comunicarse con StorageGRID.

Directrices de endurecimiento de las políticas TLS y SSH

Puede seleccionar una política de seguridad para determinar qué protocolos y cifrados se utilizan para establecer conexiones TLS seguras con aplicaciones cliente y conexiones SSH seguras con servicios internos de StorageGRID.

La política de seguridad controla cómo TLS y SSH cifran los datos en movimiento. Como práctica recomendada, debe deshabilitar las opciones de cifrado que no sean necesarias para la compatibilidad de la aplicación. Utilice la política moderna predeterminada, a menos que su sistema necesite cumplir con los Criterios comunes o necesite utilizar otros cifrados.

Ver ["Administrar la política TLS y SSH"](#) para obtener detalles e instrucciones.

Otras pautas de endurecimiento

Además de seguir las pautas de fortalecimiento para las redes y los nodos de StorageGRID, debe seguir las pautas de fortalecimiento para otras áreas del sistema StorageGRID.

Contraseña de instalación temporal

Para proteger el sistema StorageGRID durante la instalación, configure una contraseña en la página de contraseña del instalador temporal en la interfaz de usuario de instalación de StorageGRID o en la API de instalación. Cuando se configura, esta contraseña se aplica a todos los métodos para instalar StorageGRID, incluida la interfaz de usuario, la API de instalación y `configure-storagegrid.py` guion.

Para obtener más información, consulte:

- ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
- ["Instalar StorageGRID en Ubuntu o Debian"](#)
- ["Instalar StorageGRID en VMware"](#)
- ["Instalar el dispositivo StorageGRID"](#)

Registros y mensajes de auditoría

Proteja siempre los registros de StorageGRID y la salida de mensajes de auditoría de manera segura. Los registros y mensajes de auditoría de StorageGRID proporcionan información invaluable desde el punto de vista de soporte y disponibilidad del sistema. Además, la información y los detalles contenidos en los registros de StorageGRID y en los mensajes de auditoría resultantes generalmente son de naturaleza confidencial.

Configure StorageGRID para enviar eventos de seguridad a un servidor syslog externo. Si utiliza la exportación de syslog, seleccione TLS y RELP/TLS para los protocolos de transporte.

Ver el ["Referencia de archivos de registro"](#) para obtener más información sobre los registros de StorageGRID . Ver ["Mensajes de auditoría"](#) para obtener más información sobre los mensajes de auditoría de StorageGRID .

AutoSupport de NetApp

La función AutoSupport de StorageGRID le permite monitorear de manera proactiva el estado de su sistema y enviar paquetes automáticamente al sitio de soporte de NetApp , al equipo de soporte interno de su organización o a un socio de soporte. De forma predeterminada, el envío de paquetes de AutoSupport a NetApp está habilitado cuando StorageGRID se configura por primera vez.

La función AutoSupport se puede desactivar. Sin embargo, NetApp recomienda habilitarlo porque AutoSupport ayuda a acelerar la identificación y resolución de problemas en caso de que surja un problema en su sistema StorageGRID .

AutoSupport admite HTTPS, HTTP y SMTP como protocolos de transporte. Debido a la naturaleza sensible de los paquetes de AutoSupport , NetApp recomienda enfáticamente utilizar HTTPS como protocolo de transporte predeterminado para enviar paquetes de AutoSupport a NetApp.

Intercambio de recursos entre orígenes (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un bucket S3 si desea que ese bucket y los objetos que contiene sean accesibles para las aplicaciones web en otros dominios. En general, no habilite CORS a menos que sea necesario. Si se requiere CORS, límitelo a orígenes confiables.

Vea los pasos para ["Configuración del uso compartido de recursos entre orígenes \(CORS\)"](#) .

Dispositivos de seguridad externos

Una solución de fortalecimiento completa debe abordar los mecanismos de seguridad fuera de StorageGRID. El uso de dispositivos de infraestructura adicionales para filtrar y limitar el acceso a StorageGRID es una

forma eficaz de establecer y mantener una postura de seguridad estricta. Estos dispositivos de seguridad externos incluyen firewalls, sistemas de prevención de intrusiones (IPS) y otros dispositivos de seguridad.

Se recomienda un balanceador de carga de terceros para el tráfico de clientes que no son confiables. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques.

Mitigación de ransomware

Ayude a proteger los datos de sus objetos de los ataques de ransomware siguiendo las recomendaciones en ["Defensa contra ransomware con StorageGRID"](#) .

Configurar StorageGRID para FabricPool

Configurar StorageGRID para FabricPool

Si utiliza el software NetApp ONTAP , puede utilizar NetApp FabricPool para agrupar datos inactivos en un sistema de almacenamiento de objetos NetApp StorageGRID .

Utilice estas instrucciones para:

- Conozca las consideraciones y las mejores prácticas para configurar StorageGRID para una carga de trabajo de FabricPool .
- Aprenda a configurar un sistema de almacenamiento de objetos StorageGRID para su uso con FabricPool.
- Aprenda cómo proporcionar los valores necesarios a ONTAP al adjuntar StorageGRID como un nivel de nube de FabricPool .

Inicio rápido para configurar StorageGRID para FabricPool

1

Planifique su configuración

- Decida qué política de niveles de volumen de FabricPool utilizará para organizar en niveles los datos inactivos de ONTAP en StorageGRID.
- Planifique e instale un sistema StorageGRID para satisfacer sus necesidades de capacidad de almacenamiento y rendimiento.
- Familiarícese con el software del sistema StorageGRID , incluido el ["Administrador de red"](#) y el ["Administrador de inquilinos"](#) .
- Revise las mejores prácticas de FabricPool para ["Grupos HA"](#) , ["balanceo de carga"](#) , ["ILM"](#) , y ["más"](#) .
- Revise estos recursos adicionales, que brindan detalles sobre el uso y la configuración de ONTAP y FabricPool:

["TR-4598: Mejores prácticas de FabricPool en ONTAP"](#)

["Documentación de ONTAP para FabricPool"](#)

2

Realizar tareas previas

Obtener el ["Información necesaria para adjuntar StorageGRID como un nivel de nube"](#) , incluido:

- Direcciones IP
- Nombres de dominio
- Certificado SSL

Opcionalmente, configure ["federación de identidades"](#) y ["inicio de sesión único"](#) .

3

Configurar los ajustes de StorageGRID

Utilice StorageGRID para obtener los valores que ONTAP necesita para conectarse a la red.

Usando el ["Asistente de configuración de FabricPool"](#) Es la forma recomendada y más rápida de configurar todos los elementos, pero también puedes configurar cada entidad manualmente, si es necesario.

4

Configurar ONTAP y DNS

Utilice ONTAP para ["añadir un nivel de nube"](#) que utiliza los valores StorageGRID . Entonces, ["configurar entradas DNS"](#) para asociar direcciones IP a cualquier nombre de dominio que planea utilizar.

5

Monitorear y gestionar

Cuando su sistema esté en funcionamiento, realice tareas continuas en ONTAP y StorageGRID para administrar y monitorear la clasificación de datos de FabricPool a lo largo del tiempo.

¿Qué es FabricPool?

FabricPool es una solución de almacenamiento híbrido ONTAP que utiliza un agregado flash de alto rendimiento como nivel de rendimiento y un almacén de objetos como nivel de nube. El uso de agregados habilitados FabricPool le ayuda a reducir el costo de almacenamiento sin comprometer el rendimiento, la eficiencia ni la protección.

FabricPool asocia un nivel de nube (un almacén de objetos externo, como StorageGRID) con un nivel local (un agregado de almacenamiento ONTAP) para crear una colección compuesta de discos. Los volúmenes dentro de FabricPool pueden aprovechar la clasificación en niveles al mantener los datos activos (calientes) en un almacenamiento de alto rendimiento (el nivel local) y clasificar los datos inactivos (fríos) en el almacén de objetos externo (el nivel de nube).

No se requieren cambios arquitectónicos y puede continuar administrando sus datos y entorno de aplicaciones desde el sistema de almacenamiento central ONTAP .

¿Qué es StorageGRID?

NetApp StorageGRID es una arquitectura de almacenamiento que administra los datos como objetos, a diferencia de otras arquitecturas de almacenamiento como el almacenamiento de archivos o bloques. Los objetos se guardan dentro de un único contenedor (como un bucket) y no están anidados como archivos dentro de un directorio dentro de otros directorios. Aunque el almacenamiento de objetos generalmente ofrece un rendimiento menor que el almacenamiento de archivos o bloques, es significativamente más escalable. Los depósitos StorageGRID pueden contener petabytes de datos y miles de millones de objetos.

¿Por qué utilizar StorageGRID como un nivel de nube de FabricPool ?

FabricPool puede organizar datos de ONTAP en varios proveedores de almacenamiento de objetos, incluido StorageGRID. A diferencia de las nubes públicas, que pueden establecer una cantidad máxima de operaciones de entrada/salida admitidas por segundo (IOPS) a nivel de contenedor o bucket, el rendimiento de StorageGRID se escala con la cantidad de nodos en un sistema. El uso de StorageGRID como un nivel de nube de FabricPool le permite mantener sus datos fríos en su propia nube privada para obtener el máximo rendimiento y un control total sobre sus datos.

Además, no se requiere una licencia de FabricPool cuando se utiliza StorageGRID como nivel de nube.

Información necesaria para adjuntar StorageGRID como un nivel de nube

Antes de poder adjuntar StorageGRID como un nivel de nube para FabricPool, debe realizar pasos de configuración en StorageGRID y obtener ciertos valores para usar en ONTAP.

¿Qué valores necesito?

La siguiente tabla muestra los valores que debe configurar en StorageGRID y cómo ONTAP y el servidor DNS utilizan esos valores.

Valor	Donde se configura el valor	Dónde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto final del balanceador de carga	Administrador del sistema ONTAP > Agregar nivel de nube
Certificado SSL	StorageGRID > Punto final del balanceador de carga	Administrador del sistema ONTAP > Agregar nivel de nube
Nombre del servidor (FQDN)	StorageGRID > Punto final del balanceador de carga	Entrada DNS
ID de clave de acceso y clave de acceso secreta	StorageGRID > Inquilino y depósito	Administrador del sistema ONTAP > Agregar nivel de nube
Nombre del cubo/contenedor	StorageGRID > Inquilino y depósito	Administrador del sistema ONTAP > Agregar nivel de nube

¿Cómo obtengo estos valores?

Dependiendo de sus necesidades, puede realizar cualquiera de las siguientes acciones para obtener la información que necesita:

- Utilice el "[Asistente de configuración de FabricPool](#)". El asistente de configuración de FabricPool lo ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera un archivo que puede usar para configurar ONTAP System Manager. El asistente lo guía a través de los pasos necesarios y lo ayuda a garantizar que su configuración se ajuste a las mejores prácticas de StorageGRID y FabricPool .

- Configure cada elemento manualmente. Luego, ingrese los valores en el Administrador del sistema ONTAP o en la CLI de ONTAP . Siga estos pasos:
 - a. ["Configurar un grupo de alta disponibilidad \(HA\) para FabricPool"](#) .
 - b. ["Crear un punto final de balanceador de carga para FabricPool"](#) .
 - c. ["Crear una cuenta de inquilino para FabricPool"](#) .
 - d. Sign in en la cuenta del inquilino y ["Crea el depósito y las claves de acceso para el usuario raíz"](#) .
 - e. Cree una regla ILM para los datos de FabricPool y agréguela a sus políticas ILM activas. Ver ["Configurar ILM para datos de FabricPool"](#) .
 - f. Opcionalmente, ["crear una política de clasificación de tráfico para FabricPool"](#) .

Utilice el asistente de configuración de FabricPool

Utilizar el asistente de configuración de FabricPool : Consideraciones y requisitos

Puede utilizar el asistente de configuración de FabricPool para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de nube de FabricPool . Después de completar el asistente de configuración, puede ingresar los detalles necesarios en ONTAP System Manager.

Cuándo utilizar el asistente de configuración de FabricPool

El asistente de configuración de FabricPool lo guía a través de cada paso de la configuración de StorageGRID para su uso con FabricPool y configura automáticamente ciertas entidades para usted, como las políticas de clasificación de tráfico e ILM. Como parte de completar el asistente, descargará un archivo que puede usar para ingresar valores en ONTAP System Manager. Utilice el asistente para configurar su sistema más rápidamente y asegurarse de que sus configuraciones se ajusten a las mejores prácticas de StorageGRID y FabricPool .

Suponiendo que tiene permiso de acceso de root, puede completar el asistente de configuración de FabricPool cuando comience a usar StorageGRID Grid Manager, o puede acceder y completar el asistente en cualquier momento posterior. Dependiendo de sus requisitos, también puede configurar algunos o todos los elementos necesarios manualmente y luego usar el asistente para reunir los valores que ONTAP necesita en un solo archivo.



Utilice el asistente de configuración de FabricPool a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

Antes de utilizar el asistente

Confirme que ha completado estos pasos previos.

Revisar las mejores prácticas

- Tienes una comprensión general de la ["Información necesaria para adjuntar StorageGRID como un nivel de nube"](#) .
- Ha revisado las mejores prácticas de FabricPool para:
 - ["Grupos de alta disponibilidad \(HA\)"](#)
 - ["Equilibrio de carga"](#)

- ["Normas y políticas de ILM"](#)

Obtener direcciones IP y configurar interfaces VLAN

Si configura un grupo de alta disponibilidad, sabrá a qué nodos se conectará ONTAP y qué red StorageGRID se utilizará. También sabe qué valores ingresar para el CIDR de subred, la dirección IP de puerta de enlace y las direcciones IP virtuales (VIP).

Si planea utilizar una LAN virtual para segregar el tráfico de FabricPool, ya ha configurado la interfaz VLAN. Ver ["Configurar interfaces VLAN"](#).

Configurar la federación de identidades y el SSO

Si planea utilizar la federación de identidad o el inicio de sesión único (SSO) para su sistema StorageGRID, debe habilitar estas funciones. También sabe qué grupo federado debe tener acceso raíz para la cuenta de inquilino que utilizará ONTAP. Ver ["Utilizar la federación de identidades"](#) y ["Configurar el inicio de sesión único"](#).

Obtener y configurar nombres de dominio

- Sabe qué nombre de dominio completo (FQDN) utilizar para StorageGRID. Las entradas del servidor de nombres de dominio (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad que cree mediante el asistente. Ver ["Configurar el servidor DNS"](#).
- Si planea utilizar solicitudes alojadas virtuales de estilo S3, debe ["nombres de dominio de punto final S3 configurados"](#). ONTAP utiliza URL de estilo de ruta de manera predeterminada, pero se recomienda utilizar solicitudes de estilo alojado virtualmente.

Revisar los requisitos del balanceador de carga y del certificado de seguridad

Si planea utilizar el balanceador de carga StorageGRID, ha revisado las instrucciones generales ["Consideraciones para el equilibrio de carga"](#). Tienes los certificados que cargarás o los valores que necesitas para generar un certificado.

Si planea utilizar un punto final de balanceador de carga externo (de terceros), debe tener el nombre de dominio completo (FQDN), el puerto y el certificado para ese balanceador de carga.

Confirmar la configuración del grupo de almacenamiento de ILM

Si instaló inicialmente StorageGRID 11.6 o una versión anterior, habrá configurado el grupo de almacenamiento que utilizará. En general, debe crear un grupo de almacenamiento para cada sitio StorageGRID que utilizará para almacenar datos de ONTAP.



Este requisito previo no se aplica si instaló inicialmente StorageGRID 11.7 o 11.8. Cuando instala inicialmente cualquiera de estas versiones, se crean automáticamente grupos de almacenamiento para cada sitio.

Relación entre ONTAP y el nivel de nube StorageGRID

El asistente de FabricPool lo guía a través del proceso de creación de un único nivel de nube StorageGRID que incluye un inquilino StorageGRID, un conjunto de claves de acceso y un depósito StorageGRID. Puede conectar este nivel de nube de StorageGRID a uno o más niveles locales de ONTAP.

La mejor práctica general es conectar un único nivel de nube a varios niveles locales en un clúster. Sin embargo, dependiendo de sus requisitos, es posible que desee utilizar más de un depósito o incluso más de

un inquilino de StorageGRID para los niveles locales en un solo clúster. El uso de diferentes depósitos e inquilinos le permite aislar los datos y el acceso a los datos entre los niveles locales de ONTAP , pero es un poco más complejo de configurar y administrar.

NetApp no recomienda adjuntar un solo nivel de nube a niveles locales en múltiples clústeres.



Para conocer las mejores prácticas para usar StorageGRID con NetApp MetroCluster™ y FabricPool Mirror, consulte ["TR-4598: Mejores prácticas de FabricPool en ONTAP"](#) .

Opcional: utilice un depósito diferente para cada nivel local

Para usar más de un bucket para los niveles locales en un clúster de ONTAP , agregue más de un nivel de nube StorageGRID en ONTAP. Cada nivel de nube comparte el mismo grupo de alta disponibilidad, punto final del equilibrador de carga, inquilino y claves de acceso, pero utiliza un contenedor diferente (depósito StorageGRID). Siga estos pasos generales:

1. Desde StorageGRID Grid Manager, complete el asistente de configuración de FabricPool para el primer nivel de nube.
2. Desde ONTAP System Manager, agregue un nivel de nube y use el archivo que descargó de StorageGRID para proporcionar los valores requeridos.
3. Desde StorageGRID Tenant Manager, inicie sesión en el inquilino creado por el asistente y cree un segundo depósito.
4. Complete nuevamente el asistente de FabricPool . Seleccione el grupo HA existente, el punto final del balanceador de carga y el inquilino. Luego, seleccione el nuevo depósito que creó manualmente. Cree una nueva regla ILM para el nuevo depósito y active una política ILM para incluir esa regla.
5. Desde ONTAP, agregue un segundo nivel de nube pero proporcione el nuevo nombre del depósito.

Opcional: utilice un inquilino y un depósito diferentes para cada nivel local

Para usar más de un inquilino y diferentes conjuntos de claves de acceso para los niveles locales en un clúster de ONTAP , agregue más de un nivel de nube StorageGRID en ONTAP. Cada nivel de nube comparte el mismo grupo de alta disponibilidad y punto final del equilibrador de carga, pero utiliza un inquilino, claves de acceso y contenedor diferentes (depósito StorageGRID). Siga estos pasos generales:

1. Desde StorageGRID Grid Manager, complete el asistente de configuración de FabricPool para el primer nivel de nube.
2. Desde ONTAP System Manager, agregue un nivel de nube y use el archivo que descargó de StorageGRID para proporcionar los valores requeridos.
3. Complete nuevamente el asistente de FabricPool . Seleccione el grupo HA existente y el punto final del balanceador de carga. Cree un nuevo inquilino y un depósito. Cree una nueva regla ILM para el nuevo depósito y active una política ILM para incluir esa regla.
4. Desde ONTAP, agregue un segundo nivel de nube, pero proporcione la nueva clave de acceso, la clave secreta y el nombre del depósito.

Acceda y complete el asistente de configuración de FabricPool

Puede utilizar el asistente de configuración de FabricPool para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de nube de FabricPool .

Antes de empezar

- Usted ha revisado el ["Consideraciones y requisitos"](#) para utilizar el asistente de configuración de FabricPool .



Si desea configurar StorageGRID para su uso con cualquier otra aplicación cliente S3, vaya a ["Utilice el asistente de configuración de S3"](#) .

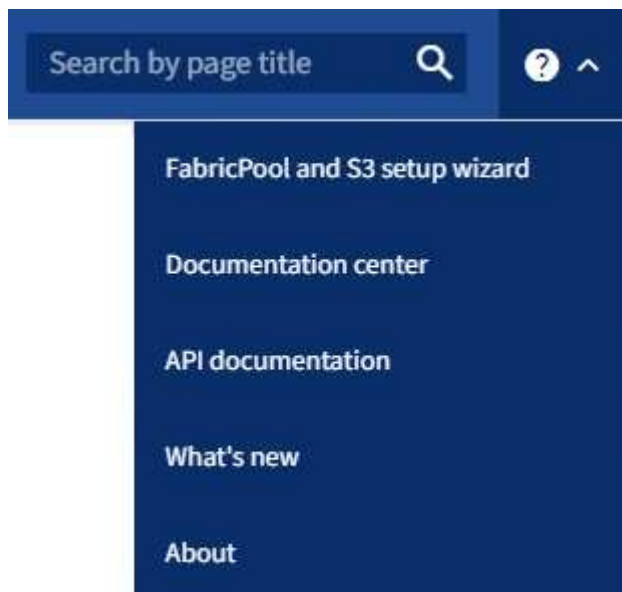
- Tú tienes el ["Permiso de acceso root"](#) .

Acceder al asistente

Puede completar el asistente de configuración de FabricPool cuando comience a utilizar StorageGRID Grid Manager, o puede acceder y completar el asistente en cualquier momento posterior.

Pasos

1. Sign in en Grid Manager usando un ["navegador web compatible"](#) .
2. Si aparece el banner **Asistente de configuración de FabricPool y S3** en el panel, seleccione el enlace en el banner. Si el banner ya no aparece, seleccione el ícono de ayuda en la barra de encabezado en el Administrador de cuadrícula y seleccione **Asistente de configuración de FabricPool y S3**.



3. En la sección FabricPool de la página del asistente de configuración de FabricPool y S3, seleccione **Configurar ahora**.

Aparece **Paso 1 de 9: Configurar el grupo HA**.

Paso 1 de 9: Configurar el grupo de alta disponibilidad

Un grupo de alta disponibilidad (HA) es una colección de nodos que contienen cada uno el servicio StorageGRID Load Balancer. Un grupo de alta disponibilidad puede contener nodos de puerta de enlace, nodos de administración o ambos.

Puede utilizar un grupo HA para ayudar a mantener disponibles las conexiones de datos de FabricPool . Un grupo de alta disponibilidad utiliza direcciones IP virtuales (VIP) para proporcionar acceso de alta disponibilidad al servicio Load Balancer. Si falla la interfaz activa en el grupo HA, una interfaz de respaldo puede administrar la carga de trabajo con poco impacto en las operaciones de FabricPool.

Para obtener más detalles sobre esta tarea, consulte ["Administrar grupos de alta disponibilidad"](#) y ["Mejores prácticas para grupos de alta disponibilidad"](#) .

Pasos

1. Si planea utilizar un balanceador de carga externo, no necesita crear un grupo de alta disponibilidad.
Seleccione **Omitir este paso** y vaya a [Paso 2 de 9: Configurar el punto final del balanceador de carga](#) .
2. Para utilizar el equilibrador de carga StorageGRID , cree un nuevo grupo de alta disponibilidad o utilice un grupo de alta disponibilidad existente.

Crear un grupo de alta disponibilidad

- a. Para crear un nuevo grupo de HA, seleccione **Crear grupo de HA**.
- b. Para el paso **Ingresar detalles**, complete los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo HA.
Descripción (opcional)	La descripción de este grupo HA.

- c. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo de HA.

Utilice los encabezados de columna para ordenar las filas o ingrese un término de búsqueda para localizar interfaces más rápidamente.

Puede seleccionar uno o más nodos, pero solo puede seleccionar una interfaz para cada nodo.

- d. Para el paso **Priorizar interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo de HA.

Arrastre filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.

Si el grupo HA incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de respaldo, y así sucesivamente. Cuando se resuelven las fallas, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

- e. Para el paso **Ingresar direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de 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 configurado. Por ejemplo, 192.16.0.0/22 .
Dirección IP de la puerta de enlace (opcional)	Opcional. Si las direcciones IP de ONTAP utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID , ingrese la dirección IP de la puerta de enlace local VIP de StorageGRID . La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	Ingrese al menos una y no más de diez direcciones VIP para la interfaz activa en el grupo HA. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa. Al menos una dirección debe ser IPv4. Opcionalmente, puede especificar direcciones IPv4 e IPv6 adicionales.

f. Seleccione **Crear grupo HA** y luego seleccione **Finalizar** para regresar al asistente de configuración de FabricPool .

g. Seleccione **Continuar** para ir al paso del balanceador de carga.

Utilizar el grupo HA existente

a. Para utilizar un grupo de HA existente, seleccione el nombre del grupo de HA en la lista desplegable **Seleccionar un grupo de HA**.

b. Seleccione **Continuar** para ir al paso del balanceador de carga.

Paso 2 de 9: Configurar el punto final del balanceador de carga

StorageGRID utiliza un equilibrador de carga para administrar la carga de trabajo de las aplicaciones cliente, como FabricPool. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en múltiples nodos de almacenamiento.

Puede utilizar el servicio StorageGRID Load Balancer, que existe en todos los nodos de puerta de enlace y de administración, o puede conectarse a un balanceador de carga externo (de terceros). Se recomienda utilizar el balanceador de carga StorageGRID .

Para obtener más detalles sobre esta tarea, consulte la información general. "[Consideraciones para el equilibrio de carga](#)" y el "[Mejores prácticas para el equilibrio de carga para FabricPool](#)" .

Pasos

1. Seleccione o cree un punto final de balanceador de carga StorageGRID o utilice un balanceador de carga externo.

Crear punto final

- Seleccione **Crear punto final**.
- Para el paso **Ingresar detalles del punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final.
Puerto	El puerto StorageGRID que desea utilizar para equilibrar la carga. Este campo tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede ingresar cualquier puerto externo no utilizado. Si ingresa 80 o 443, el punto final se configura solo en los nodos de puerta de enlace, porque estos puertos están reservados en los nodos de administración. Nota: No se permiten los puertos utilizados por otros servicios de red. Ver el "Referencia del puerto de red".
Tipo de cliente	Debe ser S3 .
Protocolo de red	Seleccione HTTPS. Nota: Se admite la comunicación con StorageGRID sin cifrado TLS, pero no se recomienda.

- Para el paso **Seleccionar modo de enlace**, especifique el modo de enlace. El modo de enlace controla cómo se accede al punto final utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice la configuración Global (predeterminada) a menos que necesite restringir la accesibilidad de este punto final.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o FQDN correspondiente) de un grupo de HA para acceder a este punto final. Todos los puntos finales con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de HA que seleccione para los puntos finales no se superpongan.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.

Modo	Descripción
Tipo de nodo	Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este punto final.

d. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (predeterminado)	Todas las cuentas de inquilinos pueden usar este punto final para acceder a sus depósitos. Permitir todos los inquilinos es casi siempre la opción adecuada para el punto final del balanceador de carga utilizado para FabricPool. Debe seleccionar esta opción si está utilizando el asistente de configuración de FabricPool para un nuevo sistema StorageGRID y aún no ha creado ninguna cuenta de inquilino.
Permitir inquilinos seleccionados	Solo las cuentas de inquilinos seleccionadas pueden usar este punto final para acceder a sus depósitos.
Bloquear inquilinos seleccionados	Las cuentas de inquilinos seleccionadas no pueden usar este punto final para acceder a sus depósitos. Todos los demás inquilinos pueden utilizar este punto final.

e. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utilice esta opción para cargar un certificado de servidor firmado por una CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Utilice esta opción para generar un certificado autofirmado. Ver " Configurar los puntos finales del balanceador de carga " para obtener detalles de qué ingresar.
Utilice el certificado StorageGRID S3	Esta opción solo está disponible si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID . Ver " Configurar certificados de API S3 " Para más detalles.

f. Seleccione **Finalizar** para regresar al asistente de configuración de FabricPool .

g. Seleccione **Continuar** para ir al paso de inquilino y depósito.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utilice el punto final del balanceador de carga existente

- Seleccione el nombre de un punto final existente de la lista desplegable **Seleccionar un punto final del balanceador de carga**.
- Seleccione **Continuar** para ir al paso de inquilino y depósito.

Utilice un balanceador de carga externo

- Complete los siguientes campos para el balanceador de carga externo.

Campo	Descripción
Nombre de dominio completo (FQDN)	El nombre de dominio completo (FQDN) del balanceador de carga externo.
Puerto	El número de puerto que FabricPool utilizará para conectarse al balanceador de carga externo.
Certificado	Copie el certificado del servidor para el balanceador de carga externo y péguelo en este campo.

- Seleccione **Continuar** para ir al paso de inquilino y depósito.

Paso 3 de 9: Inquilino y cubo

Un inquilino es una entidad que puede utilizar aplicaciones S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, depósitos, objetos y un conjunto específico de capacidades. Debe crear un inquilino de StorageGRID antes de poder crear el depósito que utilizará FabricPool .

Un bucket es un contenedor que se utiliza para almacenar objetos y metadatos de objetos de un inquilino. Aunque algunos inquilinos pueden tener muchos grupos, el asistente le permite crear o seleccionar solo un inquilino y un grupo a la vez. Más adelante podrá utilizar el Administrador de inquilinos para agregar cualquier grupo adicional que necesite.

Puede crear un nuevo inquilino y un depósito para uso de FabricPool , o puede seleccionar un inquilino y un depósito existentes. Si crea un nuevo inquilino, el sistema crea automáticamente el ID de clave de acceso y la clave de acceso secreta para el usuario raíz del inquilino.

Para obtener más detalles sobre esta tarea, consulte ["Crear una cuenta de inquilino para FabricPool"](#) y ["Cree un bucket S3 y obtenga una clave de acceso"](#) .

Pasos

Cree un nuevo inquilino y un depósito o seleccione un inquilino existente.

Nuevo inquilino y cubo

1. Para crear un nuevo inquilino y depósito, ingrese un **Nombre del inquilino**. Por ejemplo, `FabricPool tenant`.
2. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza "federación de identidades", "inicio de sesión único (SSO)", o ambos.

Opción	Haz esto
Si la federación de identidad no está habilitada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidad está habilitada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si tanto la federación de identidad como el inicio de sesión único (SSO) están habilitados	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

3. Para **Nombre del depósito**, ingrese el nombre del depósito que FabricPool utilizará para almacenar datos de ONTAP. Por ejemplo, `fabricpool-bucket`.



No puedes cambiar el nombre del depósito después de crearlo.

4. Seleccione la **Región** para este bucket.

Utilice la región predeterminada(`us-east-1`) a menos que espere utilizar ILM en el futuro para filtrar objetos según la región del depósito.

5. Seleccione **Crear y continuar** para crear el inquilino y el depósito y pasar al paso de descarga de datos.

Seleccionar inquilino y depósito

La cuenta de inquilino existente debe tener al menos un depósito que no tenga habilitada la función de control de versiones. No puede seleccionar una cuenta de inquilino existente si no existe ningún depósito para ese inquilino.

1. Seleccione el inquilino existente de la lista desplegable **Nombre del inquilino**.
2. Seleccione el depósito existente de la lista desplegable **Nombre del depósito**.

FabricPool no admite el control de versiones de objetos, por lo que los depósitos que tienen el control de versiones habilitado no se muestran.



No seleccione un depósito que tenga habilitado el bloqueo de objetos S3 para su uso con FabricPool.

3. Seleccione **Continuar** para ir al paso de descarga de datos.

Paso 4 de 9: Descargar la configuración de ONTAP

Durante este paso, descargará un archivo que puede usar para ingresar valores en ONTAP System Manager.

Pasos

1. Opcionalmente, seleccione el icono de copia () para copiar tanto el ID de la clave de acceso como la clave de acceso secreta al portapapeles.

Estos valores están incluidos en el archivo de descarga, pero es posible que desee guardarlos por separado.

2. Seleccione ***Descargar configuración de ONTAP *** para descargar un archivo de texto que contiene los valores que ha ingresado hasta ahora.

El `ONTAP_FabricPool_settings_bucketname.txt` El archivo incluye la información que necesita para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de nube FabricPool, que incluye:

- Detalles de la conexión del balanceador de carga, incluido el nombre del servidor (FQDN), el puerto y el certificado
- Nombre del depósito
- ID de clave de acceso y clave de acceso secreta para el usuario raíz de la cuenta de inquilino

3. Guarde las claves copiadas y el archivo descargado en una ubicación segura.



No cierre esta página hasta que haya copiado ambas claves de acceso, descargado la configuración de ONTAP o ambas cosas. Las claves no estarán disponibles después de cerrar esta página. Asegúrese de guardar esta información en una ubicación segura porque puede usarse para obtener datos de su sistema StorageGRID.

4. Seleccione la casilla de verificación para confirmar que ha descargado o copiado el ID de la clave de acceso y la clave de acceso secreta.
5. Seleccione **Continuar** para ir al paso del grupo de almacenamiento ILM.

Paso 5 de 9: Seleccionar un grupo de almacenamiento

Un grupo de almacenamiento es un grupo de nodos de almacenamiento. Cuando selecciona un grupo de almacenamiento, determina qué nodos utilizará StorageGRID para almacenar los datos en niveles desde ONTAP.

Para obtener más detalles sobre este paso, consulte ["Crear un grupo de almacenamiento"](#).

Pasos

1. En la lista desplegable **Sitio**, seleccione el sitio StorageGRID que desea utilizar para los datos organizados en niveles desde ONTAP.
2. En la lista desplegable **Grupo de almacenamiento**, seleccione el grupo de almacenamiento para ese sitio.

El grupo de almacenamiento de un sitio incluye todos los nodos de almacenamiento de ese sitio.

3. Seleccione **Continuar** para ir al paso de la regla ILM.

Paso 6 de 9: Revisar la regla ILM para FabricPool

Las reglas de administración del ciclo de vida de la información (ILM) controlan la ubicación, la duración y el comportamiento de ingesta de todos los objetos en su sistema StorageGRID .

El asistente de configuración de FabricPool crea automáticamente la regla ILM recomendada para el uso de FabricPool . Esta regla se aplica únicamente al depósito que usted especificó. Utiliza codificación de borrado 2+1 en un solo sitio para almacenar los datos organizados en niveles desde ONTAP.

Para obtener más detalles sobre este paso, consulte ["Crear regla ILM"](#) y ["Mejores prácticas para usar ILM con datos de FabricPool"](#) .

Pasos

1. Revise los detalles de la regla.

Campo	Descripción
Nombre de la regla	Se genera automáticamente y no se puede cambiar.
Descripción	Se genera automáticamente y no se puede cambiar.
Filtrar	El nombre del cubo Esta regla solo se aplica a los objetos que se guardan en el depósito que usted especificó.
Tiempo de referencia	Tiempo de ingesta La instrucción de ubicación comienza cuando los objetos se guardan inicialmente en el depósito.
Instrucciones de colocación	Utilice la codificación de borrado 2+1

2. Ordene el diagrama de retención por **Período de tiempo** y **Grupo de almacenamiento** para confirmar la instrucción de ubicación.
 - El **Período de tiempo** de la regla es **Día 0 - para siempre**. **Día 0** significa que la regla se aplica cuando los datos se organizan en niveles desde ONTAP. **Para siempre** significa que StorageGRID ILM no eliminará datos que se hayan organizado en niveles desde ONTAP.
 - El **Grupo de almacenamiento** de la regla es el grupo de almacenamiento que usted seleccionó. **EC 2+1** significa que los datos se almacenarán utilizando codificación de borrado 2+1. Cada objeto se guardará como dos fragmentos de datos y un fragmento de paridad. Los tres fragmentos de cada objeto se guardarán en diferentes nodos de almacenamiento en un solo sitio.
3. Seleccione **Crear y continuar** para crear esta regla e ir al paso de política ILM.

Paso 7 de 9: Revisar y activar la política de ILM

Después de que el asistente de configuración de FabricPool crea la regla ILM para el uso de FabricPool , crea una política ILM. Debe simular y revisar cuidadosamente esta política antes de activarla.

Para obtener más detalles sobre este paso, consulte ["Crear una política ILM"](#) y ["Mejores prácticas para usar ILM con datos de FabricPool"](#).



Cuando activa una nueva política ILM, StorageGRID utiliza esa política para administrar la ubicación, la duración y la protección de datos de todos los objetos en la red, incluidos los objetos existentes y los objetos recientemente ingeridos. En algunos casos, la activación de una nueva política puede provocar que los objetos existentes se muevan a nuevas ubicaciones.



Para evitar la pérdida de datos, no utilice una regla ILM que caduque o elimine los datos del nivel de nube de FabricPool. Establezca el período de retención en **para siempre** para garantizar que StorageGRID ILM no elimine los objetos de FabricPool.

Pasos

1. Opcionalmente, actualice el **Nombre de la política** generado por el sistema. De forma predeterminada, el sistema agrega "+ FabricPool" al nombre de su política activa o inactiva, pero puede proporcionar su propio nombre.
2. Revise la lista de reglas en la política inactiva.
 - Si su cuadrícula no tiene una política ILM inactiva, el asistente crea una política inactiva clonando su política activa y agregando la nueva regla en la parte superior.
 - Si su red ya tiene una política ILM inactiva y esa política utiliza las mismas reglas y el mismo orden que la política ILM activa, el asistente agrega la nueva regla en la parte superior de la política inactiva.
 - Si su política inactiva contiene reglas diferentes o un orden diferente al de la política activa, el asistente crea una nueva política inactiva clonando su política activa y agregando la nueva regla en la parte superior.

3. Revise el orden de las reglas en la nueva política inactiva.

Debido a que la regla FabricPool es la primera regla, todos los objetos en el depósito FabricPool se colocan antes de que se evalúen las demás reglas de la política. Los objetos en cualquier otro grupo se colocan mediante reglas posteriores en la política.

4. Revise el diagrama de retención para aprender cómo se retendrán los diferentes objetos.
 - a. Seleccione **Expandir todo** para ver un diagrama de retención para cada regla en la política inactiva.
 - b. Seleccione **Período de tiempo y Grupo de almacenamiento** para revisar el diagrama de retención. Confirme que todas las reglas que se aplican al depósito o inquilino de FabricPool conservan los objetos **para siempre**.
5. Cuando haya revisado la política inactiva, seleccione **Activar y continuar** para activar la política y pasar al paso de clasificación de tráfico.



Los errores en una política ILM pueden provocar una pérdida de datos irreparable. Revise la política cuidadosamente antes de activar.

Paso 8 de 9: Crear una política de clasificación de tráfico

Como opción, el asistente de configuración de FabricPool puede crear una política de clasificación de tráfico que puede usar para monitorear la carga de trabajo de FabricPool. La política creada por el sistema utiliza una regla coincidente para identificar todo el tráfico de red relacionado con el depósito que usted creó. Esta política solo monitorea el tráfico; no limita el tráfico de FabricPool ni de ningún otro cliente.

Para obtener más detalles sobre este paso, consulte ["Crear una política de clasificación de tráfico para"](#)

Pasos

1. Revise la política.
2. Si desea crear esta política de clasificación de tráfico, seleccione **Crear y continuar**.

Tan pronto como FabricPool comience a organizar los datos en niveles en StorageGRID, podrá ir a la página Políticas de clasificación de tráfico para ver las métricas de tráfico de red para esta política. Más adelante, también puede agregar reglas para limitar otras cargas de trabajo y garantizar que la carga de trabajo de FabricPool tenga la mayor parte del ancho de banda.

3. De lo contrario, seleccione **Omitir este paso**.

Paso 9 de 9: Revisar el resumen

El resumen proporciona detalles sobre los elementos que configuró, incluido el nombre del balanceador de carga, el inquilino y el depósito, la política de clasificación de tráfico y la política ILM activa.

Pasos

1. Revise el resumen.
2. Seleccione **Finalizar**.

Próximos pasos

Después de completar el asistente de FabricPool , realice estos pasos adicionales.

Pasos

1. Ir a "[Configurar el Administrador del sistema ONTAP](#)" para ingresar los valores guardados y completar el lado ONTAP de la conexión. Debe agregar StorageGRID como un nivel de nube, adjuntar el nivel de nube a un nivel local para crear un FabricPool y establecer políticas de niveles de volumen.
2. Ir a "[Configurar el servidor DNS](#)" y asegúrese de que el DNS incluya un registro para asociar el nombre del servidor StorageGRID (nombre de dominio completo) a cada dirección IP de StorageGRID que utilizará.
3. Ir a "[Otras prácticas recomendadas para StorageGRID y FabricPool](#)" para conocer las mejores prácticas para los registros de auditoría de StorageGRID y otras opciones de configuración global.

Configurar StorageGRID manualmente

Cree un grupo de alta disponibilidad (HA) para FabricPool

Al configurar StorageGRID para su uso con FabricPool, puede crear opcionalmente uno o más grupos de alta disponibilidad (HA). Un grupo de alta disponibilidad es una colección de nodos que contienen cada uno el servicio StorageGRID Load Balancer. Un grupo de alta disponibilidad puede contener nodos de puerta de enlace, nodos de administración o ambos.

Puede utilizar un grupo HA para ayudar a mantener disponibles las conexiones de datos de FabricPool . Un grupo de alta disponibilidad utiliza direcciones IP virtuales (VIP) para proporcionar acceso de alta disponibilidad al servicio Load Balancer. Si la interfaz activa en el grupo HA falla, una interfaz de respaldo puede administrar la carga de trabajo con poco impacto en las operaciones de FabricPool .

Para obtener más detalles sobre esta tarea, consulte "[Administrar grupos de alta disponibilidad](#)" . Para utilizar

el asistente de configuración de FabricPool para completar esta tarea, vaya a ["Acceda y complete el asistente de configuración de FabricPool"](#) .

Antes de empezar

- Usted ha revisado el ["Mejores prácticas para grupos de alta disponibilidad"](#) .
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Si planea utilizar una VLAN, habrá creado la interfaz VLAN. Ver ["Configurar interfaces VLAN"](#) .

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
2. Seleccione **Crear**.
3. Para el paso **Ingresar detalles**, complete los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo HA.
Descripción (opcional)	La descripción de este grupo HA.

4. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo de HA.

Utilice los encabezados de columna para ordenar las filas o ingrese un término de búsqueda para localizar interfaces más rápidamente.

Puede seleccionar uno o más nodos, pero solo puede seleccionar una interfaz para cada nodo.

5. Para el paso **Priorizar interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo de HA.

Arrastre filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.

Si el grupo HA incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de respaldo, y así sucesivamente. Cuando se resuelven las fallas, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

6. Para el paso **Ingresar direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de 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 configurado. Por ejemplo, 192.16.0.0/22 .

Campo	Descripción
Dirección IP de la puerta de enlace (opcional)	Opcional. Si las direcciones IP de ONTAP utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID, ingrese la dirección IP de la puerta de enlace local VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.
Dirección IP virtual	Ingrese al menos una y no más de diez direcciones VIP para la interfaz activa en el grupo HA. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. Opcionalmente, puede especificar direcciones IPv4 e IPv6 adicionales.

7. Seleccione **Crear grupo HA** y luego seleccione **Finalizar**.

Crear un punto final de balanceador de carga para FabricPool

StorageGRID utiliza un equilibrador de carga para administrar la carga de trabajo de las aplicaciones cliente, como FabricPool. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en múltiples nodos de almacenamiento.

Al configurar StorageGRID para su uso con FabricPool, debe configurar un punto final del equilibrador de carga y cargar o generar un certificado de punto final del equilibrador de carga, que se utiliza para proteger la conexión entre ONTAP y StorageGRID.

Para utilizar el asistente de configuración de FabricPool para completar esta tarea, vaya a ["Acceda y complete el asistente de configuración de FabricPool"](#).

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).
- Has revisado la información general ["Consideraciones para el equilibrio de carga"](#) así como el ["Mejores prácticas para el equilibrio de carga para FabricPool"](#).

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
2. Seleccione **Crear**.
3. Para el paso **Ingresar detalles del punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final.

Campo	Descripción
Puerto	El puerto StorageGRID que desea utilizar para equilibrar la carga. Este campo tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede ingresar cualquier puerto externo no utilizado. Si ingresa 80 o 443, el punto final se configura solo en los nodos de puerta de enlace. Estos puertos están reservados en los nodos de administración. Nota: No se permiten los puertos utilizados por otros servicios de red. Ver el "Referencia del puerto de red". Proporcionará este número a ONTAP cuando adjunte StorageGRID como un nivel de nube de FabricPool.
Tipo de cliente	Seleccione S3 .
Protocolo de red	Seleccione HTTPS. Nota: Se admite la comunicación con StorageGRID sin cifrado TLS, pero no se recomienda.

4. Para el paso **Seleccionar modo de enlace**, especifique el modo de enlace. El modo de enlace controla cómo se accede al punto final utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice la configuración Global (predeterminada) a menos que necesite restringir la accesibilidad de este punto final.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o FQDN correspondiente) de un grupo de HA para acceder a este punto final. Todos los puntos finales con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de HA que seleccione para los puntos finales no se superpongan.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo	Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este punto final.

5. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (predeterminado)	Todas las cuentas de inquilinos pueden usar este punto final para acceder a sus depósitos. Permitir todos los inquilinos es casi siempre la opción adecuada para el punto final del balanceador de carga utilizado para FabricPool. Debe seleccionar esta opción si aún no ha creado ninguna cuenta de inquilino.
Permitir inquilinos seleccionados	Solo las cuentas de inquilinos seleccionadas pueden usar este punto final para acceder a sus depósitos.
Bloquear inquilinos seleccionados	Las cuentas de inquilinos seleccionadas no pueden usar este punto final para acceder a sus depósitos. Todos los demás inquilinos pueden utilizar este punto final.

6. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utilice esta opción para cargar un certificado de servidor firmado por una CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Utilice esta opción para generar un certificado autofirmado. Ver" Configurar los puntos finales del balanceador de carga " para obtener detalles de qué ingresar.
Utilice el certificado StorageGRID S3	Esta opción solo está disponible si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID . Ver" Configurar certificados de API S3 " Para más detalles.

7. Seleccione **Crear**.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Crear una cuenta de inquilino para FabricPool

Debe crear una cuenta de inquilino en Grid Manager para usar FabricPool .

Las cuentas de inquilino permiten que las aplicaciones cliente almacenen y recuperen objetos en StorageGRID. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios autorizados, depósitos y objetos.

Para obtener más detalles sobre esta tarea, consulte"[Crear una cuenta de inquilino](#)" . Para utilizar el asistente

de configuración de FabricPool para completar esta tarea, vaya a ["Acceda y complete el asistente de configuración de FabricPool"](#) .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .

Pasos

1. Seleccione **INQUILINOS**.
2. Seleccione **Crear**.
3. Para los pasos de Ingresar detalles, ingrese la siguiente información.

Campo	Descripción
Nombre	Un nombre para la cuenta del inquilino. Los nombres de los inquilinos no necesitan ser únicos. Cuando se crea la cuenta de inquilino, recibe un ID de cuenta numérico único.
Descripción (opcional)	Una descripción para ayudar a identificar al inquilino.
Tipo de cliente	Debe ser S3 para FabricPool.
Cuota de almacenamiento (opcional)	Deje este campo en blanco para FabricPool.

4. Para el paso Seleccionar permisos:

- a. No seleccione **Permitir servicios de plataforma**.

Los inquilinos de FabricPool normalmente no necesitan utilizar servicios de plataforma, como la replicación de CloudMirror.

- b. Opcionalmente, seleccione **Usar fuente de identidad propia**.

- c. No seleccione **Permitir selección S3**.

Los inquilinos de FabricPool normalmente no necesitan utilizar S3 Select.

- d. Opcionalmente, seleccione **Usar conexión de federación de red** para permitir que el inquilino utilice una ["conexión de federación de red"](#) para clonación de cuentas y replicación entre redes. Luego, seleccione la conexión de federación de red que desea utilizar.

5. Para el paso Definir acceso raíz, especifique qué usuario tendrá el permiso de acceso raíz inicial para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza ["federación de identidades"](#) , ["inicio de sesión único \(SSO\)"](#) , o ambos.

Opción	Haz esto
Si la federación de identidad no está habilitada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.

Opción	Haz esto
Si la federación de identidad está habilitada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si tanto la federación de identidad como el inicio de sesión único (SSO) están habilitados	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

6. Seleccione **Crear inquilino**.

Cree un depósito S3 y obtenga claves de acceso

Antes de usar StorageGRID con una carga de trabajo de FabricPool, debe crear un depósito S3 para sus datos de FabricPool. También debe obtener una clave de acceso y una clave de acceso secreta para la cuenta de inquilino que utilizará para FabricPool.

Para obtener más detalles sobre esta tarea, consulte ["Crear un depósito S3"](#) y ["Crea tus propias claves de acceso S3"](#). Para utilizar el asistente de configuración de FabricPool para completar esta tarea, vaya a ["Acceda y complete el asistente de configuración de FabricPool"](#).

Antes de empezar

- Ha creado una cuenta de inquilino para uso de FabricPool.
- Tiene acceso root a la cuenta del inquilino.

Pasos

1. Sign in en el Administrador de inquilinos.

Puede realizar cualquiera de las siguientes acciones:

- Desde la página Cuentas de inquilino en el Administrador de cuadrícula, seleccione el enlace * Sign in* para el inquilino e ingrese sus credenciales.
- Ingrese la URL de la cuenta de inquilino en un navegador web e ingrese sus credenciales.

2. Cree un depósito S3 para los datos de FabricPool.

Debe crear un depósito único para cada clúster de ONTAP que planea utilizar.

- Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
- Seleccione **Crear depósito**.
- Ingrese el nombre del depósito StorageGRID que desea utilizar con FabricPool. Por ejemplo, `fabricpool-bucket`.



No puedes cambiar el nombre del depósito después de crearlo.

d. Seleccione la región para este bucket.

De forma predeterminada, todos los depósitos se crean en el `us-east-1` región.

- e. Seleccione **Continuar**.
- f. Seleccione **Crear depósito**.



No seleccione **Habilitar control de versiones de objetos** para el depósito FabricPool . De manera similar, no edite un bucket FabricPool para usar **Disponible** o una consistencia no predeterminada. La consistencia recomendada para los buckets de FabricPool es **Lectura después de una nueva escritura**, que es la consistencia predeterminada para un nuevo bucket.

3. Crea una clave de acceso y una clave de acceso secreta.

- a. Seleccione **ALMACENAMIENTO (S3) > Mis claves de acceso**.
- b. Seleccione **Crear clave**.
- c. Seleccione **Crear clave de acceso**.
- d. Copie el ID de la clave de acceso y la clave de acceso secreta a una ubicación segura, o seleccione **Descargar .csv** para guardar un archivo de hoja de cálculo que contenga el ID de la clave de acceso y la clave de acceso secreta.

Ingresa estos valores en ONTAP cuando configures StorageGRID como un nivel de nube de FabricPool .



Si genera una nueva clave de acceso y una clave de acceso secreta en StorageGRID en el futuro, ingrese las nuevas claves en ONTAP antes de eliminar los valores antiguos de StorageGRID. De lo contrario, ONTAP podría perder temporalmente su acceso a StorageGRID.

Configurar ILM para datos de FabricPool

Puede utilizar esta sencilla política de ejemplo como punto de partida para sus propias reglas y políticas de ILM.

Este ejemplo supone que está diseñando las reglas ILM y una política ILM para un sistema StorageGRID que tiene cuatro nodos de almacenamiento en un solo centro de datos en Denver, Colorado. Los datos de FabricPool en este ejemplo utilizan un depósito llamado `fabricpool-bucket` .



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlrela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas. Para obtener más información, consulte ["Administrar objetos con ILM"](#) .



Para evitar la pérdida de datos, no utilice una regla ILM que caduque o elimine los datos del nivel de nube de FabricPool . Establezca el período de retención en **para siempre** para garantizar que StorageGRID ILM no elimine los objetos de FabricPool .

Antes de empezar

- Usted ha revisado el ["Mejores prácticas para usar ILM con datos de FabricPool"](#) .
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso ILM o root"](#) .

- Si actualizó a StorageGRID 11.9 desde una versión anterior de StorageGRID , habrá configurado el grupo de almacenamiento que utilizará. En general, debe crear un grupo de almacenamiento para cada sitio StorageGRID que utilizará para almacenar datos.



Este requisito previo no se aplica si instaló inicialmente StorageGRID 11.7 o 11.8. Cuando instala inicialmente cualquiera de estas versiones, se crean automáticamente grupos de almacenamiento para cada sitio.

Pasos

1. Cree una regla ILM que se aplique únicamente a los datos en `fabricpool-bucket`. Esta regla de ejemplo crea copias con código de borrado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Codificación de borrado 2 + 1 para datos de FabricPool
Nombre del depósito	<code>fabricpool-bucket</code> También puede filtrar por cuenta de inquilino de FabricPool .
Filtros avanzados	Tamaño del objeto mayor a 0,2 MB. Nota: FabricPool solo escribe objetos de 4 MB, pero debe agregar un filtro de tamaño de objeto porque esta regla usa codificación de borrado.
Tiempo de referencia	Tiempo de ingesta
Periodo de tiempo y ubicaciones	Desde el día 0 tienda para siempre Almacene objetos mediante codificación de borrado utilizando el esquema EC 2+1 en Denver y conserve esos objetos en StorageGRID para siempre. Para evitar la pérdida de datos, no utilice una regla ILM que caduque o elimine los datos del nivel de nube de FabricPool .
Comportamiento de ingesta	Equilibrado

2. Cree una regla ILM predeterminada que creará dos copias replicadas de cualquier objeto que no coincida con la primera regla. No seleccione un filtro básico (cuenta de inquilino o nombre de depósito) ni ningún filtro avanzado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Dos copias replicadas

Definición de regla	Valor de ejemplo
Nombre del depósito	<i>ninguno</i>
Filtros avanzados	<i>ninguno</i>
Tiempo de referencia	Tiempo de ingesta
Periodo de tiempo y ubicaciones	Desde el día 0 tienda para siempre Almacene objetos replicando 2 copias en Denver.
Comportamiento de ingesta	Equilibrado

3. Cree una política ILM y seleccione las dos reglas. Debido a que la regla de replicación no utiliza ningún filtro, puede ser la regla predeterminada (última) para la política.
4. Ingerir objetos de prueba en la red.
5. Simular la política con los objetos de prueba para verificar el comportamiento.
6. Activar la política.

Cuando se activa esta política, StorageGRID coloca los datos de los objetos de la siguiente manera:

- Los datos organizados en niveles desde FabricPool en `fabricpool-bucket` se codificarán mediante borrado utilizando el esquema de codificación de borrado 2+1. Se colocarán dos fragmentos de datos y un fragmento de paridad en tres nodos de almacenamiento diferentes.
- Se replicarán todos los objetos de todos los demás depósitos. Se crearán dos copias y se colocarán en dos nodos de almacenamiento diferentes.
- Las copias se mantendrán en StorageGRID para siempre. StorageGRID ILM no eliminará estos objetos.

Crear una política de clasificación de tráfico para FabricPool

Opcionalmente, puede diseñar una política de clasificación de tráfico de StorageGRID para optimizar la calidad del servicio para la carga de trabajo de FabricPool .

Para obtener más detalles sobre esta tarea, consulte ["Administrar políticas de clasificación de tráfico"](#) . Para utilizar el asistente de configuración de FabricPool para completar esta tarea, vaya a ["Acceda y complete el asistente de configuración de FabricPool"](#) .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .

Acerca de esta tarea

Las mejores prácticas para crear una política de clasificación de tráfico para FabricPool dependen de la carga de trabajo, de la siguiente manera:

- Si planea agrupar los datos de la carga de trabajo principal de FabricPool en StorageGRID, debe asegurarse de que la carga de trabajo de FabricPool tenga la mayor parte del ancho de banda. Puede

crear una política de clasificación de tráfico para limitar todas las demás cargas de trabajo.



En general, es más importante priorizar las operaciones de lectura de FabricPool que las operaciones de escritura.

Por ejemplo, si otros clientes S3 utilizan este sistema StorageGRID , debe crear una política de clasificación de tráfico. Puede limitar el tráfico de red para los demás depósitos, inquilinos, subredes IP o puntos finales del balanceador de carga.

- Por lo general, no debe imponer límites de calidad de servicio en ninguna carga de trabajo de FabricPool ; solo debe limitar las demás cargas de trabajo.
- Los límites impuestos a otras cargas de trabajo deben tener en cuenta el comportamiento de esas cargas de trabajo. Los límites impuestos también variarán en función del tamaño y las capacidades de su red y de la cantidad de utilización esperada.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Clasificación de tráfico**.
2. Seleccione **Crear**.
3. Ingrese un nombre y una descripción (opcional) para la política y seleccione **Continuar**.
4. Para el paso Agregar reglas coincidentes, agregue al menos una regla.
 - a. Seleccione **Agregar regla**
 - b. Para Tipo, seleccione **Punto final del balanceador de carga** y seleccione el punto final del balanceador de carga que creó para FabricPool.

También puede seleccionar la cuenta de inquilino o el depósito de FabricPool .
 - c. Si desea que esta política de tráfico limite el tráfico hacia los demás puntos finales, seleccione **Coincidencia inversa**.
5. Opcionalmente, agregue uno o más límites para controlar el tráfico de red que coincide con la regla.



StorageGRID recopila métricas incluso si no agrega ningún límite, para que pueda comprender las tendencias de tráfico.

- a. Seleccione **Agregar un límite**.
 - b. Seleccione el tipo de tráfico que desea limitar y el límite a aplicar.
6. Seleccione **Continuar**.
 7. Lea y revise la política de clasificación de tráfico. Utilice el botón **Anterior** para volver atrás y realizar los cambios necesarios. Cuando esté satisfecho con la política, seleccione **Guardar y continuar**.

Después de terminar

["Ver métricas de tráfico de red"](#) para verificar que las políticas estén haciendo cumplir los límites de tráfico esperados.

Configurar el Administrador del sistema ONTAP

Una vez que haya obtenido la información de StorageGRID requerida, puede ir a ONTAP para agregar StorageGRID como un nivel de nube.

Antes de empezar

- Si completó el asistente de configuración de FabricPool , tendrá la `ONTAP_FabricPool_settings_bucketname.txt` archivo que descargaste.
- Si configuró StorageGRID manualmente, tiene el nombre de dominio completo (FQDN) que está usando para StorageGRID o la dirección IP virtual (VIP) para el grupo HA de StorageGRID , el número de puerto para el punto final del balanceador de carga, el certificado del balanceador de carga, la ID de clave de acceso y la clave secreta para el usuario raíz de la cuenta del inquilino y el nombre del depósito que ONTAP usará en ese inquilino.

Administrador del sistema Access ONTAP

Estas instrucciones describen cómo utilizar ONTAP System Manager para agregar StorageGRID como un nivel de nube. Puede completar la misma configuración utilizando la CLI de ONTAP . Para obtener instrucciones, vaya a ["Documentación de ONTAP para FabricPool"](#) .

Pasos

1. Acceda al Administrador del sistema para el clúster ONTAP que desea conectar a StorageGRID.
2. Sign in como administrador del clúster.
3. Vaya a **ALMACENAMIENTO > Niveles > Agregar nivel de nube**.
4. Seleccione * StorageGRID* de la lista de proveedores de almacenamiento de objetos.

Introduzca los valores de StorageGRID

Ver ["Documentación de ONTAP para FabricPool"](#) Para más información.

Pasos

1. Complete el formulario Agregar nivel de nube, utilizando el `ONTAP_FabricPool_settings_bucketname.txt` archivo o los valores obtenidos manualmente.

Campo	Descripción
Nombre	Ingrese un nombre único para este nivel de nube. Puede aceptar el valor predeterminado.
Estilo de URL	Si usted "nombres de dominio de punto final S3 configurados" , seleccione URL de estilo alojado virtual. Path-Style URL es el valor predeterminado para ONTAP, pero se recomienda usar solicitudes de estilo alojado virtual para StorageGRID. Debe utilizar URL de estilo de ruta si proporciona una dirección IP en lugar de un nombre de dominio para el campo Nombre del servidor (FQDN).

Campo	Descripción
Nombre del servidor (FQDN)	Ingrese el nombre de dominio completo (FQDN) que está utilizando para StorageGRID o la dirección IP virtual (VIP) para el grupo HA de StorageGRID . Por ejemplo, <code>s3.storagegrid.company.com</code> . Tenga en cuenta lo siguiente: • La dirección IP o el nombre de dominio que especifique aquí debe coincidir con el certificado que cargó o generó para el punto final del balanceador de carga de StorageGRID . • Si proporciona un nombre de dominio, el registro DNS debe asignarse a cada dirección IP que utilizará para conectarse a StorageGRID. Ver "Configurar el servidor DNS" .
SSL	Habilitado (predeterminado).
Certificado de almacén de objetos	Pegue el certificado PEM que está utilizando para el punto final del balanceador de carga StorageGRID , incluido: <pre>-----BEGIN CERTIFICATE----- y -----END CERTIFICATE----- .</pre> Nota: Si una CA intermedia emitió el certificado StorageGRID , debe proporcionar el certificado de CA intermedia. Si el certificado StorageGRID fue emitido directamente por la CA raíz, debe proporcionar el certificado de la CA raíz.
Puerto	Ingrese el puerto utilizado por el punto final del balanceador de carga de StorageGRID . ONTAP utilizará este puerto cuando se conecte a StorageGRID. Por ejemplo, 10433.
Clave de acceso y clave secreta	Ingrese el ID de la clave de acceso y la clave de acceso secreta para el usuario raíz de la cuenta de inquilino de StorageGRID . Sugerencia: Si genera una nueva clave de acceso y una clave de acceso secreta en StorageGRID en el futuro, ingrese las nuevas claves en ONTAP antes de eliminar los valores antiguos de StorageGRID. De lo contrario, ONTAP podría perder temporalmente su acceso a StorageGRID.
Nombre del contenedor	Ingrese el nombre del depósito StorageGRID que creó para usar con este nivel de ONTAP .

2. Complete la configuración final de FabricPool en ONTAP.

- Adjunte uno o más agregados al nivel de nube.
- Opcionalmente, cree una política de niveles de volumen.

Configurar el servidor DNS

Después de configurar grupos de alta disponibilidad, puntos finales del equilibrador de carga y nombres de dominio de puntos finales S3, debe asegurarse de que el DNS

incluya las entradas necesarias para StorageGRID. Debe incluir una entrada DNS para cada nombre en el certificado de seguridad y para cada dirección IP que pueda utilizar.

Ver ["Consideraciones para el equilibrio de carga"](#) .

Entradas DNS para el nombre del servidor StorageGRID

Agregue entradas DNS para asociar el nombre del servidor StorageGRID (nombre de dominio completo) a cada dirección IP de StorageGRID que utilizará. Las direcciones IP que ingrese en el DNS dependen de si está utilizando un grupo HA de nodos de equilibrio de carga:

- Si ha configurado un grupo de HA, ONTAP se conectará a las direcciones IP virtuales de ese grupo de HA.
- Si no está utilizando un grupo HA, ONTAP puede conectarse al servicio StorageGRID Load Balancer usando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración.
- Si el nombre del servidor se resuelve en más de una dirección IP, ONTAP establece conexiones de cliente con todas las direcciones IP (hasta un máximo de 16 direcciones IP). Las direcciones IP se seleccionan mediante un método rotatorio cuando se establecen conexiones.

Entradas DNS para solicitudes de estilo alojado virtual

Si has definido ["Nombres de dominio de punto final S3"](#) y utilizará solicitudes de estilo alojado virtual, agregará entradas DNS para todos los nombres de dominio de punto final S3 requeridos, incluidos los nombres comodín.

Prácticas recomendadas de StorageGRID para FabricPool

Mejores prácticas para grupos de alta disponibilidad (HA)

Antes de adjuntar StorageGRID como un nivel de nube de FabricPool , obtenga información sobre los grupos de alta disponibilidad (HA) de StorageGRID y revise las mejores prácticas para usar grupos de HA con FabricPool.

¿Qué es un grupo HA?

Un grupo de alta disponibilidad (HA) es una colección de interfaces de varios nodos de puerta de enlace de StorageGRID , nodos de administración o ambos. Un grupo HA ayuda a mantener disponibles las conexiones de datos del cliente. Si la interfaz activa en el grupo HA falla, una interfaz de respaldo puede administrar la carga de trabajo con poco impacto en las operaciones de FabricPool .

Cada grupo HA proporciona acceso de alta disponibilidad a los servicios compartidos en los nodos asociados. Por ejemplo, un grupo de alta disponibilidad que consta de interfaces solo en nodos de puerta de enlace o en nodos de administración y nodos de puerta de enlace proporciona acceso de alta disponibilidad al servicio de balanceador de carga compartido.

Para obtener más información sobre los grupos de alta disponibilidad, consulte ["Administrar grupos de alta disponibilidad \(HA\)"](#) .

Uso de grupos de HA

Las mejores prácticas para crear un grupo StorageGRID HA para FabricPool dependen de la carga de trabajo.

- Si planea utilizar FabricPool con datos de carga de trabajo principales, debe crear un grupo de alta disponibilidad que incluya al menos dos nodos de equilibrio de carga para evitar interrupciones en la

recuperación de datos.

- Si planea utilizar la política de niveles de volumen de solo instantáneas de FabricPool o niveles de rendimiento local no primarios (por ejemplo, ubicaciones de recuperación ante desastres o destinos de NetApp SnapMirror), puede configurar un grupo de alta disponibilidad con solo un nodo.

Estas instrucciones describen cómo configurar un grupo HA para HA de respaldo activo (un nodo es activo y el otro es de respaldo). Sin embargo, es posible que prefieras utilizar DNS Round Robin o Active-Active HA. Para conocer los beneficios de estas otras configuraciones de HA, consulte ["Opciones de configuración para grupos de alta disponibilidad"](#).

Mejores prácticas para el equilibrio de carga para FabricPool

Antes de adjuntar StorageGRID como un nivel de nube de FabricPool, revise las mejores prácticas para usar balanceadores de carga con FabricPool.

Para obtener información general sobre el balanceador de carga StorageGRID y el certificado del balanceador de carga, consulte ["Consideraciones para el equilibrio de carga"](#).

Prácticas recomendadas para el acceso de los inquilinos al punto final del balanceador de carga utilizado para FabricPool

Puede controlar qué inquilinos pueden usar un punto final de balanceador de carga específico para acceder a sus depósitos. Puede permitir a todos los inquilinos, permitir a algunos inquilinos o bloquear a algunos inquilinos. Al crear un punto final de equilibrio de carga para el uso de FabricPool, seleccione **Permitir todos los inquilinos**. ONTAP cifra los datos que se colocan en los depósitos StorageGRID, por lo que esta capa de seguridad adicional proporcionaría poca seguridad adicional.

Mejores prácticas para el certificado de seguridad

Cuando crea un punto final de balanceador de carga StorageGRID para uso de FabricPool, proporciona el certificado de seguridad que permitirá que ONTAP se autentique con StorageGRID.

En la mayoría de los casos, la conexión entre ONTAP y StorageGRID debe utilizar el cifrado de seguridad de la capa de transporte (TLS). Se admite el uso de FabricPool sin cifrado TLS, pero no se recomienda. Cuando seleccione el protocolo de red para el punto final del balanceador de carga StorageGRID, seleccione **HTTPS**. Luego proporcione el certificado de seguridad que permitirá que ONTAP se autentique con StorageGRID.

Para obtener más información sobre el certificado de servidor para un punto final de equilibrio de carga:

- ["Administrar certificados de seguridad"](#)
- ["Consideraciones para el equilibrio de carga"](#)
- ["Pautas de refuerzo para certificados de servidor"](#)

Agregar certificado a ONTAP

Cuando agrega StorageGRID como un nivel de nube de FabricPool, debe instalar el mismo certificado en el clúster de ONTAP, incluidos los certificados raíz y cualquier certificado de autoridad de certificación (CA) subordinada.

Administrar la expiración del certificado



Si el certificado utilizado para proteger la conexión entre ONTAP y StorageGRID caduca, FabricPool dejará de funcionar temporalmente y ONTAP perderá temporalmente el acceso a los datos almacenados en StorageGRID.

Para evitar problemas de vencimiento de certificados, siga estas prácticas recomendadas:

- Supervise atentamente cualquier alerta que advierta sobre fechas de vencimiento de certificados próximas, como las alertas **Vencimiento del certificado del punto final del equilibrador de carga** y **Vencimiento del certificado del servidor global para la API de S3**.
- Mantenga siempre sincronizadas las versiones StorageGRID y ONTAP del certificado. Si reemplaza o renueva el certificado utilizado para un punto final del balanceador de carga, debe reemplazar o renovar el certificado equivalente utilizado por ONTAP para el nivel de nube.
- Utilice un certificado CA firmado públicamente. Si utiliza un certificado firmado por una CA, puede utilizar la API de administración de Grid para automatizar la rotación de certificados. Esto le permite reemplazar certificados que están a punto de vencer sin interrupciones.
- Si ha generado un certificado StorageGRID autofirmado y ese certificado está a punto de caducar, debe reemplazarlo manualmente tanto en StorageGRID como en ONTAP antes de que caduque el certificado existente. Si un certificado autofirmado ya ha expirado, desactive la validación del certificado en ONTAP para evitar la pérdida de acceso.

Ver ["Base de conocimientos de NetApp : Cómo configurar un nuevo certificado de servidor autofirmado de StorageGRID en una implementación existente de ONTAP FabricPool"](#) para obtener instrucciones.

Mejores prácticas para usar ILM con datos de FabricPool

Si está utilizando FabricPool para organizar datos en niveles en StorageGRID, debe comprender los requisitos para usar la gestión del ciclo de vida de la información (ILM) de StorageGRID con datos de FabricPool .



FabricPool no tiene conocimiento de las reglas o políticas de StorageGRID ILM. Puede ocurrir pérdida de datos si la política ILM de StorageGRID está mal configurada. Para obtener información detallada, consulte ["Utilice reglas ILM para administrar objetos"](#) y ["Crear políticas ILM"](#) .

Pautas para usar ILM con FabricPool

Cuando utiliza el asistente de configuración de FabricPool , este crea automáticamente una nueva regla ILM para cada bucket S3 que cree y agrega esa regla a una política inactiva. Se le solicitará que active la política. La regla creada automáticamente sigue las mejores prácticas recomendadas: utiliza codificación de borrado 2+1 en un solo sitio.

Si está configurando StorageGRID manualmente en lugar de utilizar el asistente de configuración de FabricPool , revise estas pautas para asegurarse de que sus reglas y políticas de ILM sean adecuadas para los datos de FabricPool y los requisitos de su negocio. Es posible que necesite crear nuevas reglas y actualizar sus políticas ILM activas para cumplir con estas pautas.

- Puede utilizar cualquier combinación de reglas de replicación y codificación de borrado para proteger los datos de nivel de nube.

La mejor práctica recomendada es utilizar codificación de borrado 2+1 dentro de un sitio para lograr una protección de datos rentable. La codificación de borrado utiliza más CPU, pero ofrece significativamente

menos capacidad de almacenamiento que la replicación. Los esquemas 4+1 y 6+1 utilizan menos capacidad que el esquema 2+1. Sin embargo, los esquemas 4+1 y 6+1 son menos flexibles si necesita agregar nodos de almacenamiento durante la expansión de la red. Para obtener más información, consulte ["Añadir capacidad de almacenamiento para objetos con código de borrado"](#) .

- Cada regla aplicada a los datos de FabricPool debe utilizar codificación de borrado o debe crear al menos dos copias replicadas.



Una regla ILM que crea solo una copia replicada por cada período de tiempo pone los datos en riesgo de pérdida permanente. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

- Si es necesario ["eliminar datos de FabricPool de StorageGRID"](#) , use ONTAP para recuperar todos los datos del volumen FabricPool y promoverlo al nivel de rendimiento.



Para evitar la pérdida de datos, no utilice una regla ILM que caduque o elimine los datos del nivel de nube de FabricPool . Establezca el período de retención en cada regla ILM en **para siempre** para garantizar que StorageGRID ILM no elimine los objetos de FabricPool .

- No cree reglas que muevan los datos del nivel de nube de FabricPool fuera del depósito a otra ubicación. No se puede utilizar un grupo de almacenamiento en la nube para mover datos de FabricPool a otro almacén de objetos.



No se admite el uso de grupos de almacenamiento en la nube con FabricPool debido a la latencia adicional para recuperar un objeto del destino del grupo de almacenamiento en la nube.

- A partir de ONTAP 9.8, puede crear opcionalmente etiquetas de objetos para ayudar a clasificar y ordenar datos escalonados para una gestión más sencilla. Por ejemplo, puede establecer etiquetas solo en los volúmenes de FabricPool adjuntos a StorageGRID. Luego, cuando crea reglas ILM en StorageGRID, puede usar el filtro avanzado Etiqueta de objeto para seleccionar y colocar estos datos.

Otras prácticas recomendadas para StorageGRID y FabricPool

Al configurar un sistema StorageGRID para su uso con FabricPool, es posible que deba cambiar otras opciones de StorageGRID . Antes de cambiar una configuración global, considere cómo afectará el cambio a otras aplicaciones S3.

Destinos de mensajes y registros de auditoría

Las cargas de trabajo de FabricPool a menudo tienen una alta tasa de operaciones de lectura, lo que puede generar un gran volumen de mensajes de auditoría.

- Si no necesita un registro de las operaciones de lectura del cliente para FabricPool o cualquier otra aplicación S3, vaya opcionalmente a **CONFIGURACIÓN > Monitoreo > Servidor de auditoría y syslog**. Cambie la configuración **Lecturas de cliente** a **Error** para disminuir la cantidad de mensajes de auditoría registrados en el registro de auditoría. Ver ["Configurar mensajes de auditoría y destinos de registro"](#) Para más detalles.
- Si tiene una red grande, utiliza varios tipos de aplicaciones S3 o desea conservar todos los datos de auditoría, configure un servidor syslog externo y guarde la información de auditoría de forma remota. El

uso de un servidor externo minimiza el impacto en el rendimiento del registro de mensajes de auditoría sin reducir la integridad de los datos de auditoría. Ver "[Consideraciones para el servidor syslog externo](#)" Para más detalles.

Cifrado de objetos

Al configurar StorageGRID, puede habilitar opcionalmente la "[Opción global para el cifrado de objetos almacenados](#)". Si se requiere cifrado de datos para otros clientes de StorageGRID. Los datos que se almacenan en niveles desde FabricPool a StorageGRID ya están cifrados, por lo que no es necesario habilitar la configuración de StorageGRID. Las claves de cifrado del lado del cliente son propiedad de ONTAP.

Compresión de objetos

Al configurar StorageGRID, no habilite la "[Opción global para comprimir objetos almacenados](#)". Los datos almacenados en niveles desde FabricPool a StorageGRID ya están comprimidos. El uso de la opción StorageGRID no reducirá aún más el tamaño de un objeto.

Consistencia del cubo

Para los buckets de FabricPool, la consistencia recomendada es **Lectura después de una nueva escritura**, que es la consistencia predeterminada para un bucket nuevo. No edite los depósitos de FabricPool para usar **Disponible** o **Sitio fuerte**.

Nivelación de FabricPool

Si un nodo StorageGRID usa almacenamiento asignado desde un sistema NetApp ONTAP, confirme que el volumen no tenga habilitada una política de niveles de FabricPool. Por ejemplo, si un nodo StorageGRID se ejecuta en un host VMware, asegúrese de que el volumen que respalda el almacén de datos para el nodo StorageGRID no tenga una política de niveles de FabricPool habilitada. Deshabilitar la organización en niveles de FabricPool para los volúmenes utilizados con nodos StorageGRID simplifica la resolución de problemas y las operaciones de almacenamiento.



Nunca use FabricPool para agrupar datos relacionados con StorageGRID en StorageGRID mismo. La organización de los datos de StorageGRID en niveles en StorageGRID aumenta la resolución de problemas y la complejidad operativa.

Eliminar datos de FabricPool de StorageGRID

Si necesita eliminar los datos de FabricPool que actualmente están almacenados en StorageGRID, debe usar ONTAP para recuperar todos los datos del volumen de FabricPool y promoverlo al nivel de rendimiento.

Antes de empezar

- Has revisado las instrucciones y consideraciones en "[Promocionar datos al nivel de rendimiento](#)".
- Está utilizando ONTAP 9.8 o posterior.
- Estás usando un "[navegador web compatible](#)".
- Pertenece a un grupo de usuarios de StorageGRID para la cuenta de inquilino de FabricPool que tiene la "[Administrar todos los depósitos o permisos de acceso raíz](#)".

Acerca de esta tarea

Estas instrucciones explican cómo mover datos desde StorageGRID a FabricPool. Realice este procedimiento utilizando ONTAP y StorageGRID Tenant Manager.

Pasos

1. Desde ONTAP, emita el `volume modify` dominio.

Colocar `tiering-policy` a `none` Para detener la nueva clasificación y establecer `cloud-retrieval-policy` a `promote` para devolver todos los datos que anteriormente estaban almacenados en StorageGRID.

Ver ["Promocionar todos los datos de un volumen FabricPool al nivel de rendimiento"](#) .

2. Espere a que se complete la operación.

Puedes utilizar el `volume object-store` comando con el `tiering` opción a ["comprobar el estado de la promoción del nivel de rendimiento"](#) .

3. Una vez completada la operación de promoción, inicie sesión en StorageGRID Tenant Manager para la cuenta de inquilino de FabricPool .
4. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
5. Confirme que el depósito FabricPool ahora esté vacío.
6. Si el cubo está vacío, ["eliminar el depósito"](#) .

Después de terminar

Cuando se elimina el bucket, la organización en niveles de FabricPool a StorageGRID ya no puede continuar. Sin embargo, debido a que el nivel local aún está conectado al nivel de nube StorageGRID , ONTAP System Manager devolverá mensajes de error que indican que el depósito es inaccesible.

Para evitar estos mensajes de error, realice una de las siguientes acciones:

- Utilice FabricPool Mirror para adjuntar un nivel de nube diferente al agregado.
- Mueva los datos del agregado FabricPool a un agregado que no sea FabricPool y luego elimine el agregado no utilizado.

Ver el ["Documentación de ONTAP para FabricPool"](#) para obtener instrucciones.

Información de copyright

Copyright © 2025 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.