Usar una cuenta de inquilino

StorageGRID 11.8

NetApp
March 19, 2024

Tabla de contenidos

Usar una cuenta de inquilino . . . 1
- Usar una cuenta de inquilino: Descripción general . . . 1
- Cómo iniciar sesión y salir . . . 2
- Conozca la consola de tenant Manager . . . 7
- API de gestión de inquilinos . . . 10
- Utilizar conexiones de federación de grid . . . 15
- Gestionar grupos y usuarios . . . 28
- Gestión de claves de acceso de S3 . . . 48
- Gestión de bloques S3 . . . 54
- Gestione servicios de plataformas S3 . . . 76

Usar una cuenta de inquilino

Usar una cuenta de inquilino: Descripción general

Una cuenta de inquilino permite usar la API DE REST de simple Storage Service (S3) o la API DE REST de Swift para almacenar y recuperar objetos en un sistema StorageGRID.

¿Qué es una cuenta de inquilino?

Cada cuenta de inquilino tiene sus propios grupos locales o federados, usuarios, bloques S3 o contenedores Swift, y objetos.

Las cuentas de arrendatario se pueden utilizar para segregar objetos almacenados por diferentes entidades. Por ejemplo, pueden utilizarse varias cuentas de inquilino en cualquiera de estos casos de uso:

- **Caso de uso empresarial:** Si el sistema StorageGRID se está utilizando dentro de una empresa, el almacenamiento de objetos de la cuadrícula puede estar segregado por los diferentes departamentos de la organización. Por ejemplo, puede haber cuentas de inquilino para el departamento de marketing, el departamento de soporte al cliente, el departamento de recursos humanos, etc.

  > Si utiliza el protocolo cliente S3, también puede utilizar bloques S3 y políticas de bucket para separar objetos entre los departamentos de una empresa. No es necesario crear cuentas de arrendatario independientes. Consulte las instrucciones de implementación "Bloques de S3 y políticas de bloques" si quiere más información.

- **Caso de uso del proveedor de servicios:** Si un proveedor de servicios utiliza el sistema StorageGRID, el almacenamiento de objetos de la cuadrícula puede estar segregado por las diferentes entidades que arriendan el almacenamiento. Por ejemplo, puede que haya cuentas de inquilino para la empresa A, la empresa B, la empresa C, etc.

Cómo crear una cuenta de inquilino

Las cuentas de inquilino se crean mediante una "El administrador de grid de StorageGRID que utiliza Grid Manager". Al crear una cuenta de inquilino, el administrador de grid especifica lo siguiente:

- Información básica, incluido el nombre del inquilino, el tipo de cliente (S3 o Swift) y la cuota de almacenamiento opcional.
- Permisos para la cuenta de inquilino, como si la cuenta de inquilino puede usar los servicios de la plataforma S3, configurar su propio origen de identidad, usar S3 Select o usar una conexión de federación de grid.
- Acceso raíz inicial para el inquilino, basado en si el sistema StorageGRID utiliza usuarios y grupos locales, federación de identidades o inicio de sesión único (SSO).

Además, los administradores de grid pueden habilitar la configuración de bloqueo de objetos de S3 para el sistema StorageGRID si las cuentas de inquilinos S3 necesitan cumplir con los requisitos normativos. Cuando se habilita el bloqueo de objetos S3, todas las cuentas de inquilinos S3 pueden crear y gestionar bloques conforme a la normativa.

Configure los inquilinos S3

Después de un "Se crea la cuenta de inquilino de S3", Puede acceder al Administrador de arrendatarios para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidad se comparta con la cuadrícula)
- Gestionar grupos y usuarios
- Utilice la federación de grid para la clonación de cuentas y la replicación entre grid
- Gestión de claves de acceso de S3
- Cree y gestione bloques de S3
- Utilice los servicios de la plataforma S3
- Utilice S3 Select
- Supervise el uso del almacenamiento

Aunque puede crear y administrar buckets S3 con el Gestor de inquilinos, debe utilizar un "Cliente S3" o. "S3 Consola" para procesar y gestionar objetos.

Configure los inquilinos Swift

Después de un "Se crea la cuenta de inquilino de Swift", Puede acceder al Administrador de arrendatarios para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidad se comparta con la cuadrícula)
- Gestionar grupos y usuarios
- Supervise el uso del almacenamiento

Los usuarios de Swift deben tener el permiso de acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso de acceso raíz no permite que los usuarios se autentiquen en el "API REST de Swift" para crear contenedores y objetos de procesamiento. Los usuarios deben tener el permiso de administrador de Swift para autenticarse en la API DE REST de Swift.

Cómo iniciar sesión y salir

Inicie sesión en el Administrador de inquilinos

Para acceder al Administrador de arrendatarios, introduzca la dirección URL del arrendatario en la barra de direcciones de un "navegador web compatible".

Antes de empezar

- Tiene sus credenciales de inicio de sesión.
- Dispone de una dirección URL para acceder al gestor de inquilinos, tal y como proporciona el administrador de grid. La dirección URL tendrá el aspecto de uno de estos ejemplos:

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

```
https://FQDN_or_Admin_Node_IP:port/

https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

La URL siempre incluye un nombre de dominio completo (FQDN), la dirección IP de un nodo de administración o la dirección IP virtual de un grupo de alta disponibilidad de nodos de administración. También puede incluir un número de puerto, el ID de cuenta de inquilino de 20 dígitos o ambos.

- Si la URL no incluye el ID de cuenta de 20 dígitos del inquilino, tiene este ID de cuenta.
- Está utilizando un "navegador web compatible".
- Las cookies están habilitadas en su navegador web.
- Pertenece a un grupo de usuarios que tiene "permisos de acceso específicos".

Pasos

1. Inicie un "navegador web compatible".
2. En la barra de dirección del navegador, introduzca la URL para acceder al Administrador de inquilinos.
3. Si se le solicita una alerta de seguridad, instale el certificado con el asistente de instalación del explorador.
4. Inicie sesión en el Administrador de inquilinos.

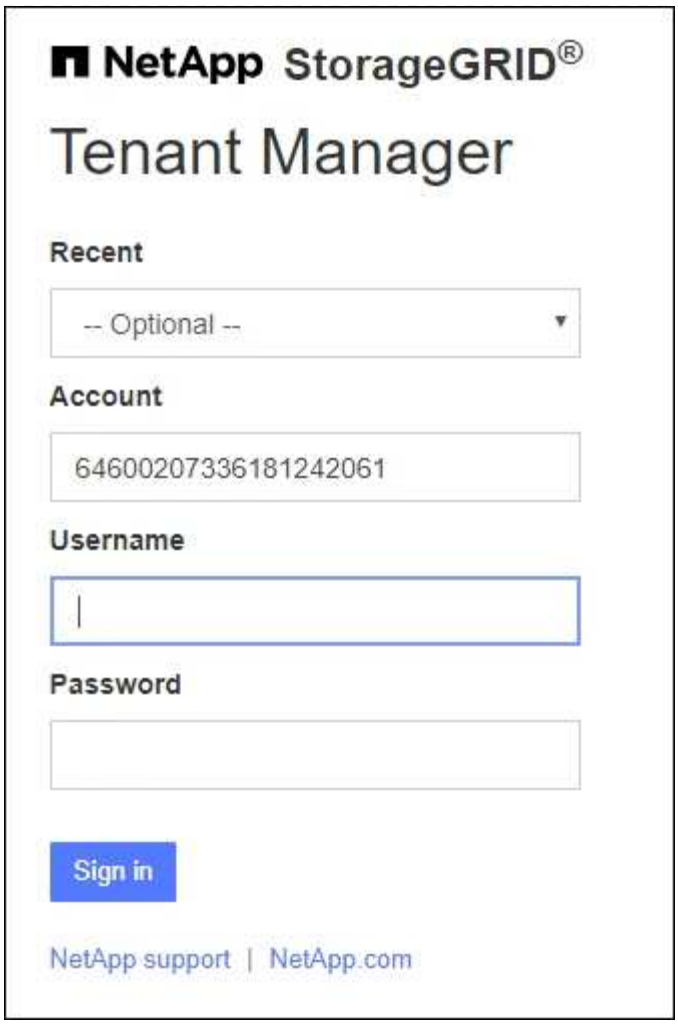
   La pantalla de inicio de sesión que aparece depende de la dirección URL introducida y de si se ha configurado el inicio de sesión único (SSO) para StorageGRID.

No se utiliza SSO

Si StorageGRID no utiliza SSO, aparecerá una de las siguientes pantallas:

- La página de inicio de sesión de Grid Manager. Seleccione el enlace **Inscrito de inquilino**.

- La página de inicio de sesión del administrador de inquilinos. Es posible que el campo **Cuenta** ya esté completado, como se muestra a continuación.



i. Si no se muestra el ID de cuenta de 20 dígitos del arrendatario, seleccione el nombre de la cuenta de arrendatario si aparece en la lista de cuentas recientes o introduzca el ID de cuenta.

ii. Introduzca su nombre de usuario y contraseña.

iii. Seleccione **Iniciar sesión**.

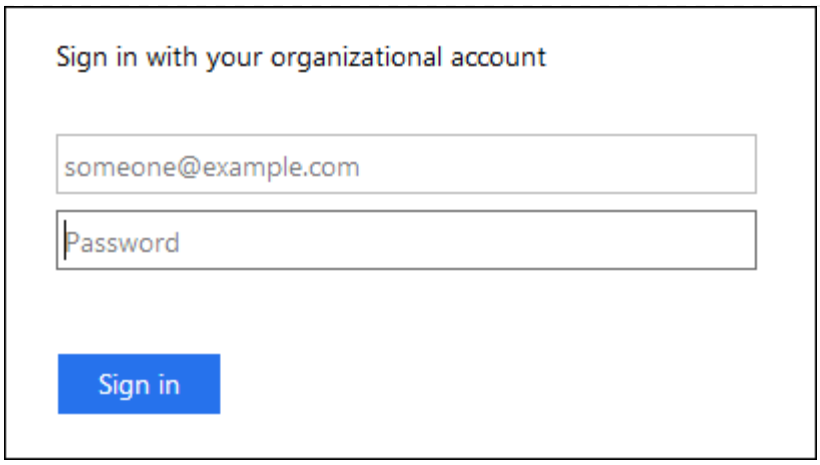
Aparece el panel de control del gestor de inquilinos.

iv. Si recibió una contraseña inicial de otra persona, seleccione ***username*** > **Cambiar contraseña** para proteger su cuenta.

Uso de SSO

Si StorageGRID utiliza SSO, aparece una de las siguientes pantallas:

◦ La página de SSO de su organización. Por ejemplo:



Ingrese sus credenciales estándar de SSO y seleccione **Iniciar sesión**.

- La página de inicio de sesión SSO de inquilino Manager.

i. Si no se muestra el ID de cuenta de 20 dígitos del arrendatario, seleccione el nombre de la cuenta de arrendatario si aparece en la lista de cuentas recientes o introduzca el ID de cuenta.

ii. Seleccione **Iniciar sesión**.

iii. Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

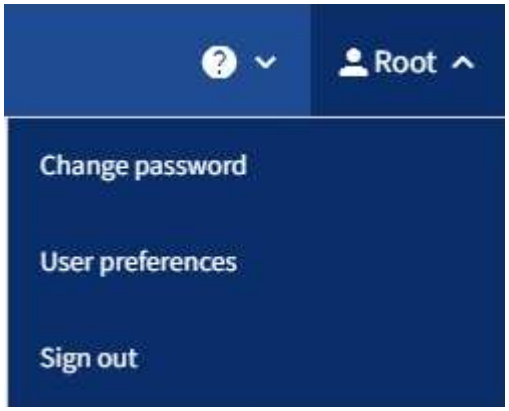
Aparece el panel de control del gestor de inquilinos.

Cierre la sesión del responsable de inquilinos

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

Pasos

1. Busque el menú desplegable username en la esquina superior derecha de la interfaz de usuario.



2. Seleccione el nombre de usuario y luego seleccione **Cerrar sesión**.

   - Si SSO no está en uso:

     Ha cerrado sesión en el nodo de administrador. Se muestra la página de inicio de sesión del administrador de inquilinos.

     > Si ha iniciado sesión en más de un nodo de administrador, debe cerrar la sesión de cada nodo.

   - Si SSO está habilitado:

     Inició sesión en todos los nodos de administrador a los que accedían. Aparece la página Inicio de sesión de StorageGRID. El nombre de la cuenta de arrendatario a la que acaba de acceder aparece como el valor predeterminado en el menú desplegable **Cuentas recientes**, y se muestra el **ID de cuenta** del arrendatario.

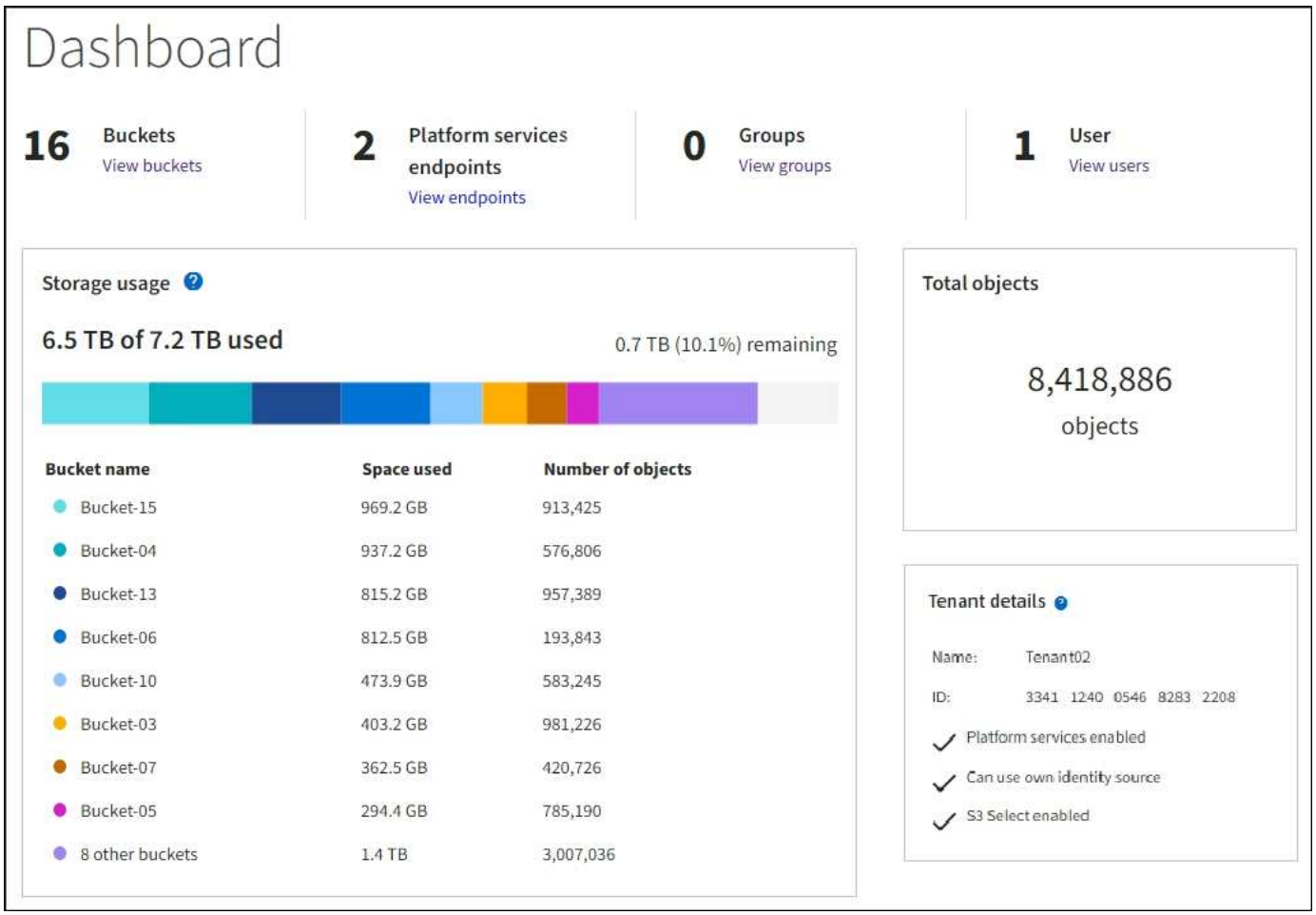
     > Si SSO está activado y también ha iniciado sesión en Grid Manager, también debe cerrar sesión en Grid Manager para cerrar sesión en SSO.

Conozca la consola de tenant Manager

La consola de tenant Manager proporciona información general de la configuración de una cuenta de inquilino y la cantidad de espacio que usan los objetos de los bloques del inquilino (S3) o los contenedores (Swift). Si el inquilino tiene una cuota, la consola muestra cuánta cuota se usa y cuánta queda. Si hay algún error relacionado con la cuenta de inquilino, los errores se muestran en el panel de control.

Los valores de espacio utilizado son estimaciones. Estas estimaciones se ven afectadas por el tiempo de los ingests, la conectividad de red y el estado del nodo.

Cuando se han cargado objetos, el panel de control tiene el siguiente ejemplo:



Resumen de la cuenta de inquilino

La parte superior del panel contiene la siguiente información:

- El número de bloques o contenedores, grupos y usuarios configurados
- El número de extremos de servicios de plataforma, si se han configurado alguno

Puede seleccionar los enlaces para ver los detalles.

La parte derecha del panel contiene la siguiente información:

- Número total de objetos para el arrendatario.

  Para una cuenta S3, si no se ha ingerido ningún objeto y tiene el "Permiso de acceso raíz", aparecen las directrices de inicio en lugar del número total de objetos.

- Detalles de inquilinos, incluidos el nombre e ID de la cuenta de inquilino y si este puede usar "servicios de plataforma", "su propia fuente de identidad", "federación de grid", o. "S3 Select" (sólo se muestran los permisos habilitados).

Aprovechamiento del almacenamiento y de la cuota

El panel uso del almacenamiento contiene la siguiente información:

- La cantidad de datos de objeto para el inquilino.

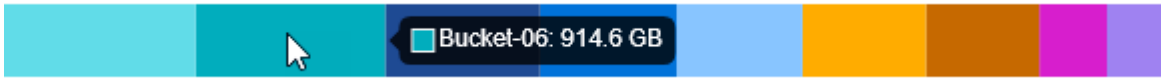
  Este valor indica la cantidad total de datos de objeto cargados y no representa el espacio utilizado para almacenar copias de esos objetos y sus metadatos.

- Si se establece una cuota, la cantidad total de espacio disponible para los datos del objeto y la cantidad y el porcentaje de espacio restante. La cuota limita la cantidad de datos de objetos que se pueden procesar.

  El uso de la cuota se basa en estimaciones internas y puede superarse en algunos casos. Por ejemplo, StorageGRID comprueba la cuota cuando un inquilino comienza a cargar objetos y rechaza nuevas búsquedas si el inquilino ha superado la cuota. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha superado la cuota. Si se eliminan objetos, se puede evitar temporalmente que un arrendatario cargue nuevos objetos hasta que se vuelva a calcular el uso de cuota. Los cálculos de uso de cuotas pueden tardar 10 minutos o más.

- Un gráfico de barras que representa los tamaños relativos de los cubos o contenedores más grandes.

  Puede colocar el cursor sobre cualquiera de los segmentos del gráfico para ver el espacio total consumido por ese cucharón o contenedor.



- Para corresponder con el gráfico de barras, una lista de los cubos o contenedores más grandes, incluida la cantidad total de datos de objeto y el número de objetos de cada cucharón o contenedor.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

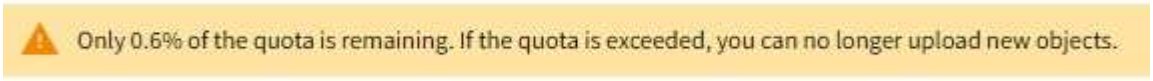
Si el inquilino tiene más de nueve cubos o contenedores, el resto de cubos o contenedores se combinan en una sola entrada al final de la lista.

Para cambiar las unidades para los valores de almacenamiento que se muestran en el Administrador de inquilinos, seleccione el menú desplegable de usuario en la parte superior derecha del Administrador de inquilinos y, a continuación, seleccione **Preferencias de usuario**.

Alertas de uso de cuotas

Si se han habilitado alertas de uso de cuota en Grid Manager, aparecerán en el Gestor de arrendatarios cuando la cuota sea baja o excedida, de la siguiente manera:

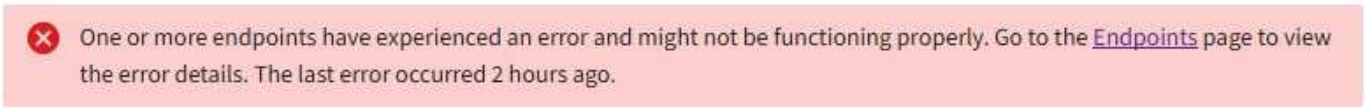
Si se ha utilizado un 90% o más de la cuota de un inquilino, se activa la alerta **uso de cuota de inquilino alto**. Realice las acciones recomendadas para la alerta.



Si excedes tu cuota, no podrás cargar nuevos objetos.

Errores de punto final

Si ha utilizado Grid Manager para configurar uno o más puntos finales para su uso con servicios de plataforma, el panel de control de tenant Manager muestra una alerta si se han producido errores de punto final en los últimos siete días.



Para ver los detalles acerca de "errores de punto final de servicios de plataforma", Seleccione **Endpoints** para mostrar la página Endpoints.

API de gestión de inquilinos

Comprender la API de gestión de inquilinos

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

API de gestión de inquilinos:

- Utiliza la plataforma API de código abierto de Swagger. Swagger proporciona una interfaz de usuario intuitiva que permite a los desarrolladores y no desarrolladores interactuar con la API. La interfaz de usuario de Swagger proporciona detalles y documentación completos para cada operación de API.

- Utiliza "creación de versiones para dar cabida a actualizaciones no disruptivas".

Para acceder a la documentación de Swagger para la API de gestión de inquilinos:

1. Inicie sesión en el Administrador de inquilinos.
2. En la parte superior del Administrador de inquilinos, selecciona el icono de ayuda y selecciona **Documentación de API**.

Operaciones de API

La API de gestión de inquilinos organiza las operaciones de API disponibles en las siguientes secciones:

- **CUENTA**: Operaciones en la cuenta de inquilino actual, incluida la obtención de información de uso de almacenamiento.
- **AUTH**: Operaciones para realizar la autenticación de sesión de usuario.

  La API de administración de arrendatarios admite el esquema de autenticación de token Bearer. Para el inicio de sesión de un inquilino, debe proporcionar un nombre de usuario, una contraseña y un ID de cuenta en el cuerpo JSON de la solicitud de autenticación (es decir, `POST /api/v3/authorize`). Si el usuario se autentica correctamente, se devuelve un token de seguridad. Este token se debe proporcionar en el encabezado de las posteriores solicitudes de API ("autorización: Token del portador").

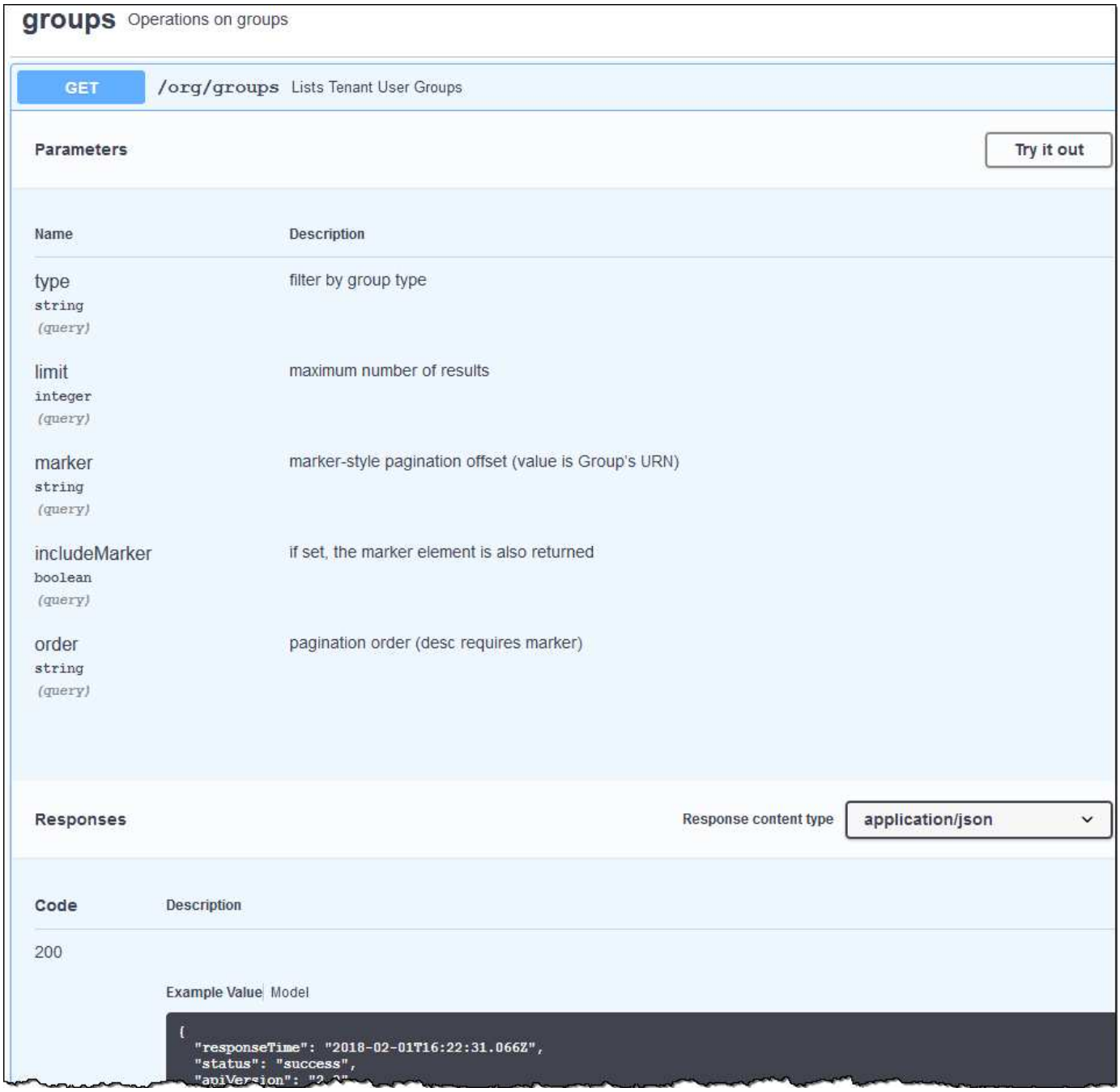
  Para obtener información acerca de cómo mejorar la seguridad de autenticación, consulte "Protección contra falsificación de solicitudes entre sitios".

  > Si está habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, debe realizar diferentes pasos para la autenticación. Consulte "Instrucciones de uso de la API de gestión de grid".

- **Config**: Operaciones relacionadas con el lanzamiento del producto y versiones de la API de Gestión de Inquilinos. Puede mostrar la versión de la versión del producto y las versiones principales de la API que admite esa versión.
- **Contenedores**: Operaciones en S3 cubos o contenedores Swift.
- **Funciones desactivadas**: Operaciones para ver características que podrían haber sido desactivadas.
- **Endpoints**: Operaciones para gestionar un endpoint. Los extremos permiten que un bloque de S3 use un servicio externo para la replicación de CloudMirror de StorageGRID, notificaciones o integración de búsqueda.
- **Grid-federation-connections**: Operaciones en conexiones de federación de grid y replicación entre grid.
- **GRUPOS**: Operaciones para administrar grupos de inquilinos locales y para recuperar grupos de inquilinos federados de una fuente de identidad externa.
- **Identity-source**: Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información federada del grupo y del usuario.
- **ilm**: Operaciones en la configuración de gestión del ciclo de vida de la información (ILM).
- **REGIONS**: Operaciones para determinar qué regiones se han configurado para el sistema StorageGRID.
- **S3**: Operaciones para administrar las claves de acceso S3 para los usuarios inquilinos.
- **S3-OBJECT-LOCK**: Operaciones en la configuración global de S3 Object Lock, utilizada para apoyar el cumplimiento normativo.
- **Usuarios**: Operaciones para ver y administrar usuarios inquilinos.

Detalles de la operación

Al expandir cada operación de API, puede ver su acción HTTP, su URL de extremo, una lista de cualquier parámetro requerido o opcional, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.



Emita solicitudes API

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

Pasos

1. Seleccione la acción HTTP para ver los detalles de la solicitud.

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

Creación de versiones de la API de gestión de inquilinos

La API de gestión de inquilinos utiliza versiones para dar cabida a actualizaciones no disruptivas.

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

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

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

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

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

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

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

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

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

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

Determine qué versiones de API son compatibles con la versión actual

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

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

Especifique una versión API para una solicitud

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

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

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

Protección contra falsificación de solicitudes entre sitios (CSRF)

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

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

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

Para habilitar la función, configure la `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 verdadero, un `GridCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en Grid Manager y en `AccountCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio 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 una de las siguientes:

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

Para configurar la protección CSRF, utilice "API de gestión de grid" o. "API de gestión de inquilinos".

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

Utilizar conexiones de federación de grid

Clone los usuarios y los grupos de inquilinos

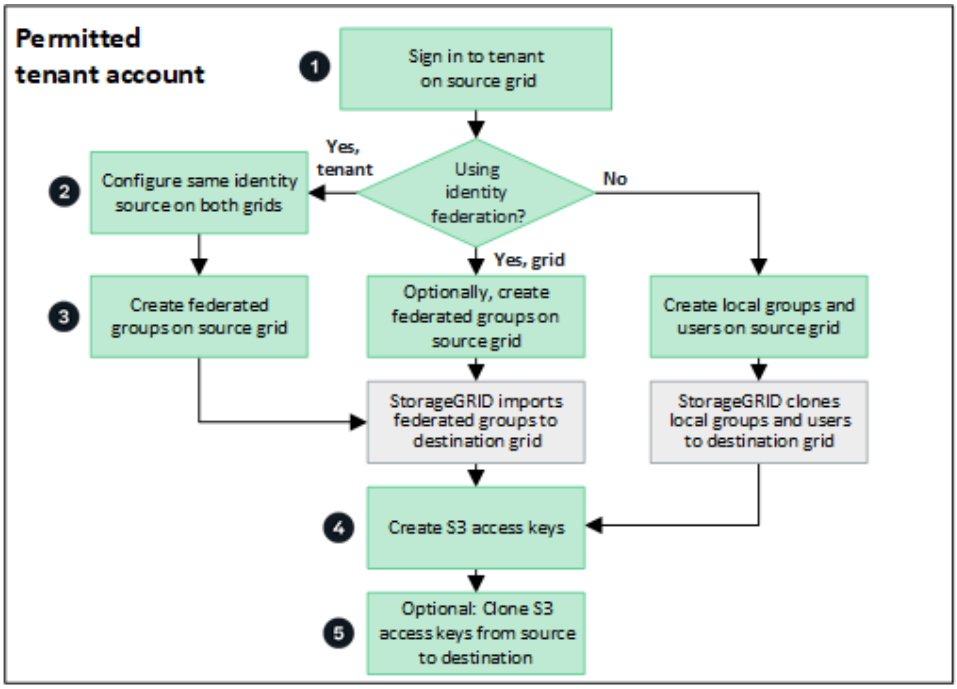
Si se creó o editó un inquilino para utilizar una conexión de federación de grid, ese inquilino se replica desde un sistema StorageGRID (el inquilino de origen) a otro sistema StorageGRID (el inquilino de réplica). Una vez que el inquilino se ha replicado, todos los grupos y usuarios agregados al inquilino de origen se clonan en el inquilino de réplica.

El sistema StorageGRID donde se crea originalmente el inquilino es *source grid* del inquilino. El sistema StorageGRID donde se replica el inquilino es el *grid de destino* del inquilino. Ambas cuentas de inquilino tienen el mismo ID de cuenta, nombre, descripción, cuota de almacenamiento y permisos asignados. pero el inquilino de destino no tiene inicialmente una contraseña de usuario raíz. Para obtener más información, consulte "Qué es el clon de cuenta" y.. "Gestionar inquilinos permitidos".

Se requiere la clonado de la información de la cuenta de inquilino para "replicación entre grid" de objetos de cubo. Tener los mismos grupos de arrendatarios y usuarios en ambas cuadrículas garantiza que pueda acceder a los bloques y objetos correspondientes en cualquiera de las cuadrículas.

Flujo de trabajo de inquilino para el clon de cuenta

Si su cuenta de inquilino tiene el permiso **Use grid federation connection**, revise el diagrama de flujo de trabajo para ver los pasos que realizará para clonar grupos, usuarios y claves de acceso S3.



Estos son los pasos principales del flujo de trabajo:

1 Inicie sesión en el inquilino

Inicie sesión en la cuenta de inquilino en la cuadrícula de origen (la cuadrícula donde se creó inicialmente el inquilino).

2 Opcionalmente, configure la federación de identidades

Si su cuenta de inquilino tiene el permiso **Usar origen de identidad propio** para usar grupos y usuarios federados, configure el mismo origen de identidad (con la misma configuración) tanto para las cuentas de inquilino de origen como de destino. Los grupos y usuarios federados no se pueden clonar a menos que ambas cuadrículas utilicen el mismo origen de identidad. Para ver instrucciones, consulte "Usar la federación de identidades".

3 Crear grupos y usuarios

Al crear grupos y usuarios, comience siempre desde la cuadrícula de origen del inquilino. Cuando se agrega un grupo nuevo, StorageGRID lo clona automáticamente en la cuadrícula de destino.

- Si la federación de identidades está configurada para todo el sistema de StorageGRID o para su cuenta de inquilino, "crear nuevos grupos de arrendatarios" importando grupos federados desde el origen de identidad.
- Si no está utilizando la federación de identidades, "crear nuevos grupos locales" y después "crear usuarios locales".

4 Crear claves de acceso S3

Puede hacerlo "cree sus propias claves de acceso" o hasta "crear claves de acceso de otro usuario" en la

cuadrícula de origen o en la de destino para acceder a los depósitos de dicha cuadrícula.

5 **Opcionalmente, clone las claves de acceso S3**

Si necesita acceder a los depósitos con las mismas claves de acceso en ambas cuadrículas, cree las claves de acceso en la cuadrícula de origen y, a continuación, utilice la API del administrador de inquilinos para clonarlas manualmente en la cuadrícula de destino. Para ver instrucciones, consulte "Clone las claves de acceso S3 mediante la API".

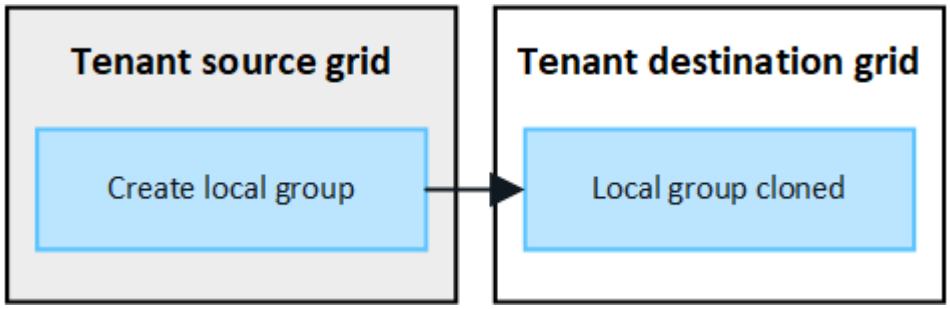
¿Cómo se clonan los grupos, los usuarios y las claves de acceso de S3?

Revise esta sección para entender cómo se clonan los grupos, los usuarios y las claves de acceso S3 entre la cuadrícula de origen de inquilino y el grid de destino de inquilino.

Los grupos locales creados en la cuadrícula de origen se clonan

Después de crear una cuenta de inquilino y replicarla en el grid de destino, StorageGRID clona automáticamente los grupos locales que se agregan a la cuadrícula de origen del inquilino en el grid de destino del inquilino.

Tanto el grupo original como su clon tienen el mismo modo de acceso, permisos de grupo y política de grupos S3. Para ver instrucciones, consulte "Cree grupos para el inquilino de S3".

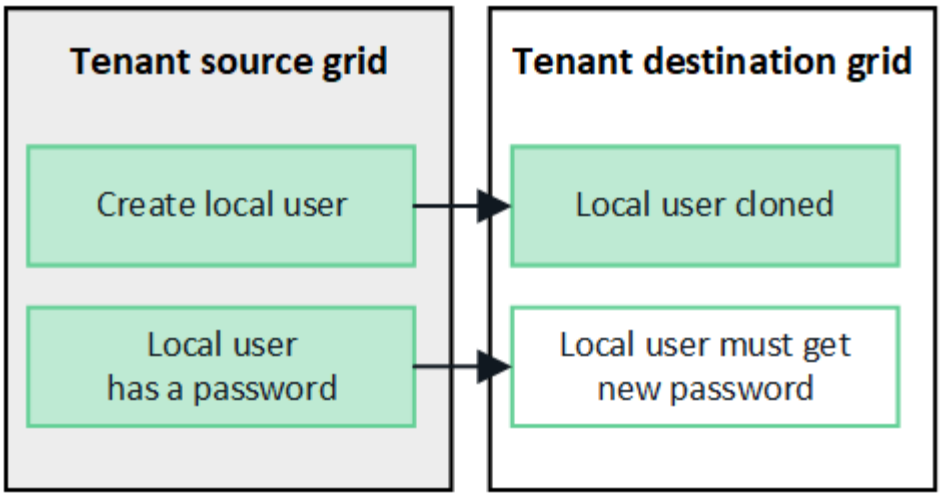


Los usuarios que seleccione al crear un grupo local en la cuadrícula de origen no se incluyen cuando el grupo se clona en la cuadrícula de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Los usuarios locales creados en la cuadrícula de origen se clonan

Cuando se crea un usuario local nuevo en el grid de origen, StorageGRID clona automáticamente ese usuario en el grid de destino. Tanto el usuario original como su clon tienen la misma configuración de nombre completo, nombre de usuario y **Denegar acceso**. Ambos usuarios también pertenecen a los mismos grupos. Para ver instrucciones, consulte "Gestionar usuarios locales".

Por motivos de seguridad, las contraseñas de usuario local no se clonan en el grid de destino. Si un usuario local necesita acceder a Tenant Manager en la cuadrícula de destino, el usuario raíz de la cuenta de inquilino debe agregar una contraseña para ese usuario en la cuadrícula de destino. Para ver instrucciones, consulte "Gestionar usuarios locales".

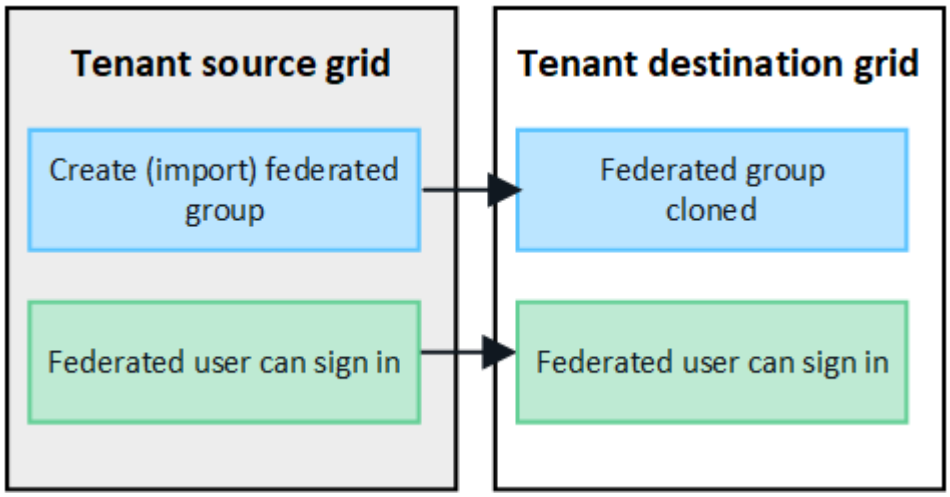


Los grupos federados creados en la cuadrícula de origen se clonan

Suponiendo los requisitos para utilizar el clon de cuenta con "inicio de sesión único" y.. "federación de identidades" se han cumplido, los grupos federados que se crean (se importan) para el inquilino en la cuadrícula de origen se clonan automáticamente en el inquilino en la cuadrícula de destino.

Ambos grupos tienen el mismo modo de acceso, permisos de grupo y política de grupos S3.

Una vez que se crean grupos federados para el inquilino de origen y se clonan en el inquilino de destino, los usuarios federados pueden iniciar sesión en el inquilino en cualquier grid.

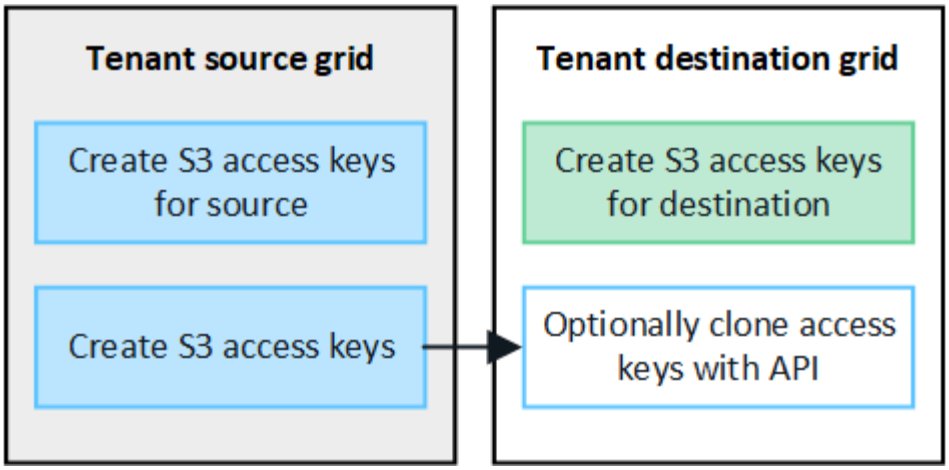


Las claves de acceso S3 se pueden clonar manualmente

StorageGRID no clona automáticamente claves de acceso S3, ya que la seguridad mejora al disponer de diferentes claves en cada grid.

Para gestionar las claves de acceso en las dos cuadrículas, puede realizar una de las siguientes acciones:

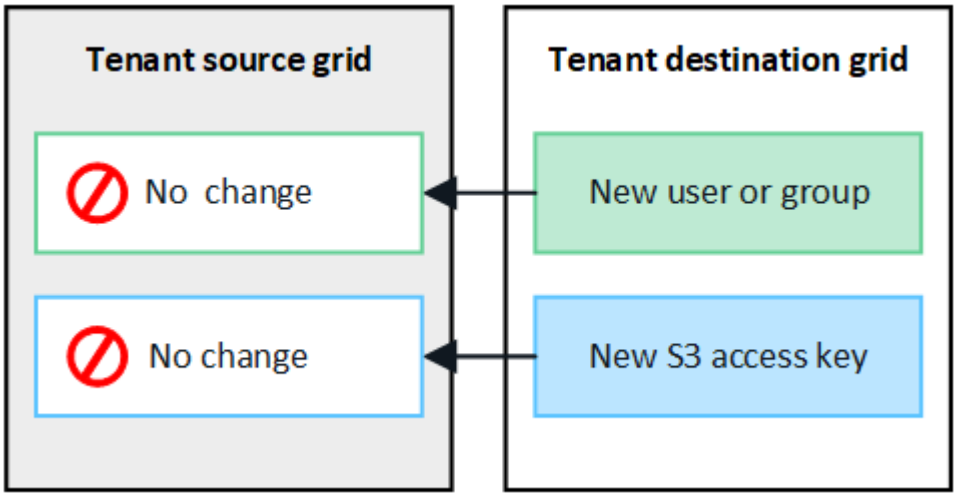
- Si no necesita utilizar las mismas claves para cada cuadrícula, puede hacerlo "cree sus propias claves de acceso" o. "crear claves de acceso de otro usuario" en cada cuadrícula.
- Si necesita utilizar las mismas claves en ambas cuadrículas, puede crear claves en la cuadrícula de origen y, a continuación, utilizar la API del gestor de inquilinos para manualmente "clonar las claves" a la cuadrícula de destino.



Cuando se clonan las claves de acceso S3 para un usuario federado, tanto el usuario como las claves de acceso S3 se clonan en el inquilino de destino.

Los grupos y usuarios que se agregan al grid de destino no se clonan

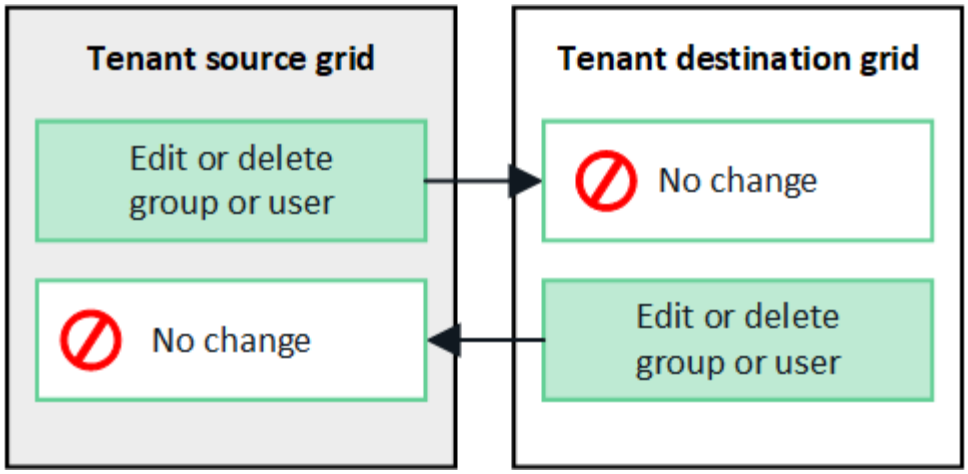
La clonación solo se produce desde la cuadrícula de origen del inquilino al grid de destino del inquilino. Si crea o importa grupos y usuarios en la cuadrícula de destino del inquilino, StorageGRID no clonará estos elementos de vuelta a la cuadrícula de origen del inquilino.



Los grupos, usuarios y claves de acceso editados o eliminados no se clonan

La clonación solo se produce cuando se crean nuevos grupos y usuarios.

Si edita o elimina grupos, usuarios o claves de acceso en cualquiera de las cuadrículas, los cambios no se clonarán en la otra cuadrícula.



Clone las claves de acceso S3 mediante la API

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, puede usar la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la cuadrícula de origen al inquilino en la cuadrícula de destino.

Antes de empezar

- La cuenta de inquilino tiene el permiso **Use grid federation connection**.
- La conexión de federación de red tiene un **estado de conexión** de **Conectado**.
- Ha iniciado sesión en el gestor de inquilinos en la cuadrícula de origen del inquilino mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Administre sus propias credenciales de S3 o permiso de acceso raíz".
- Si clona claves de acceso para un usuario local, el usuario ya existe en ambas cuadrículas.

> Cuando se clonan las claves de acceso S3 para un usuario federado, se agregan al inquilino de destino las claves de acceso S3 y el usuario.

Clone sus propias claves de acceso

Puede clonar sus propias claves de acceso si necesita acceder a los mismos depósitos en ambas cuadrículas.

Pasos

1. Mediante el administrador de inquilinos en la cuadrícula de origen, "cree sus propias claves de acceso" y descargue el `.csv` archivo.
2. En la parte superior del Administrador de inquilinos, selecciona el icono de ayuda y selecciona **Documentación de API**.
3. En la sección **S3**, seleccione el siguiente punto final:

```
POST /org/users/current-user/replicate-s3-access-key
```

4. Seleccione **probar**.
5. En el cuadro de texto **body**, reemplace las entradas de ejemplo de **accessKey** y **secretAccessKey** con los valores del archivo **.csv** que descargó.

   Asegúrese de conservar las comillas dobles alrededor de cada cadena.

6. Si la clave caduca, reemplace la entrada de ejemplo para **Expires** con la fecha y hora de vencimiento como una cadena en formato de datos-tiempo ISO 8601 (por ejemplo, `2024-02-28T22:46:33-08:00`). Si la clave no caduca, introduzca **null** como valor para la entrada **Expires** (o elimine la línea **Expires** y la coma anterior).
7. Seleccione **Ejecutar**.
8. Confirme que el código de respuesta del servidor es **204**, lo que indica que la clave se clonó correctamente en la cuadrícula de destino.

Clonar las claves de acceso de otro usuario

Puede clonar las claves de acceso de otro usuario si necesita acceder a los mismos depósitos en ambas cuadrículas.

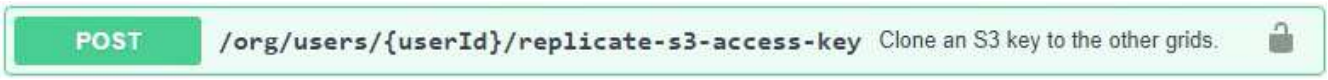
Pasos

1. Mediante el administrador de inquilinos en la cuadrícula de origen, "Cree las claves de acceso S3 del otro usuario" y descargue el `.csv` archivo.
2. En la parte superior del Administrador de inquilinos, selecciona el icono de ayuda y selecciona **Documentación de API**.
3. Obtenga el ID de usuario. Necesitará este valor para clonar las claves de acceso del otro usuario.
   a. En la sección **users**, selecciona el siguiente punto final:

      `GET /org/users`

   b. Seleccione **probar**.
   c. Especifique los parámetros que desee utilizar al buscar usuarios.
   d. Seleccione **Ejecutar**.
   e. Busque el usuario cuyas claves desea clonar y copie el número en el campo **id**.
4. En la sección **S3**, seleccione el siguiente punto final:

   `POST /org/users/{userId}/replicate-s3-access-key`



5. Seleccione **probar**.
6. En el cuadro de texto **UserId**, pega el ID de usuario que copiaste.
7. En el cuadro de texto **body**, reemplace las entradas de ejemplo de **example access key** y **secret access key** con los valores del archivo **.csv** para ese usuario.

   Asegúrese de conservar las comillas dobles alrededor de la cadena.

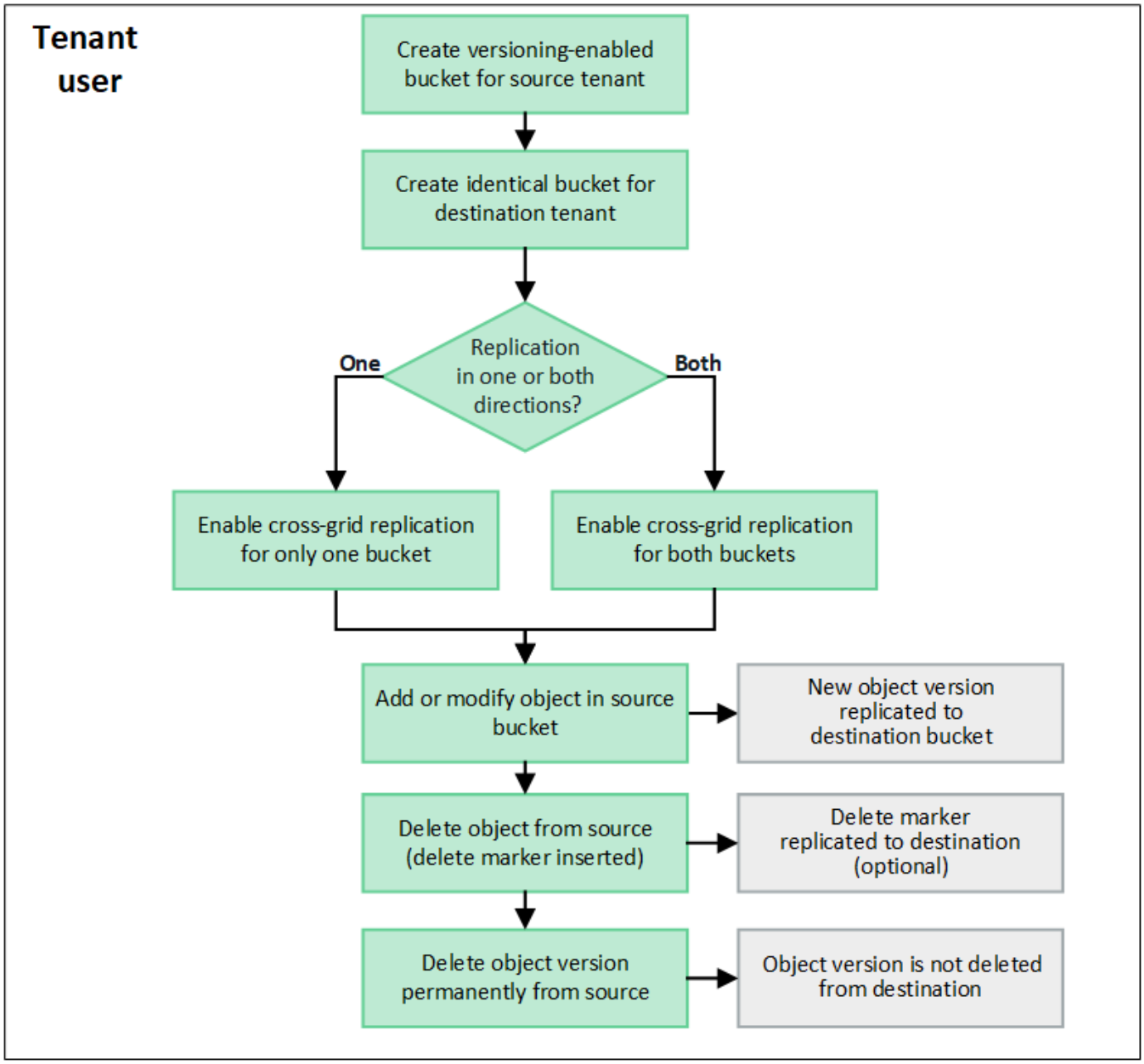
8. Si la clave caduca, reemplace la entrada de ejemplo para **Expires** con la fecha y hora de vencimiento como una cadena en formato de datos-tiempo ISO 8601 (por ejemplo, `2023-02-28T22:46:33-08:00`). Si la clave no caduca, introduzca **null** como valor para la entrada **Expires** (o elimine la línea **Expires** y la coma anterior).
9. Seleccione **Ejecutar**.
10. Confirme que el código de respuesta del servidor es **204**, lo que indica que la clave se clonó correctamente en la cuadrícula de destino.

Gestionar la replicación entre grid

Si a su cuenta de inquilino se le asignó el permiso **Usar conexión de federación de grid** cuando se creó, puede utilizar la replicación entre grid para replicar automáticamente objetos entre buckets en la cuadrícula de origen del inquilino y depósitos en la cuadrícula de destino del inquilino. La replicación entre grid puede producirse en una o en ambas direcciones.

Flujo de trabajo de replicación entre grid

El diagrama de flujo de trabajo resume los pasos que realizará para configurar la replicación entre bloques en dos cuadrículas. Estos pasos se describen con más detalle a continuación.



Configurar la replicación entre grid

Para poder utilizar la replicación entre grid, debe iniciar sesión en las cuentas de tenant correspondientes en cada grid y crear buckets idénticos. A continuación, puede activar la replicación entre grid en cualquiera de los dos bloques o en ambos.

Antes de empezar

- Ha revisado los requisitos para la replicación entre grid. Consulte "Qué es la replicación entre grid".
- Está utilizando un "navegador web compatible".
- La cuenta de inquilino tiene el permiso **Use grid federation connection** y existen cuentas de inquilino idénticas en ambas cuadrículas. Consulte "Gestione los inquilinos permitidos para la conexión de federación de grid".
- El usuario de inquilino al que se conectará como ya existe en ambas cuadrículas y pertenece a un grupo de usuarios que tiene "Permiso de acceso raíz".

- Si va a iniciar sesión en la cuadrícula de destino del inquilino como un usuario local, el usuario raíz de la cuenta de inquilino ha establecido una contraseña para su cuenta de usuario en ese grid.

Cree dos cubos idénticos

Como primer paso, inicie sesión en las cuentas de arrendatario correspondientes en cada cuadrícula y cree cubos idénticos.

Pasos

1. A partir de cualquier cuadrícula de la conexión de federación de grid, cree un nuevo bucket:
   a. Inicie sesión en la cuenta de inquilino con las credenciales de un usuario de inquilino que existe en ambas cuadrículas.

      Si no puede iniciar sesión en la cuadrícula de destino del inquilino como usuario local, confirme que el usuario raíz de la cuenta de inquilino ha establecido una contraseña para su cuenta de usuario.

   b. Siga las instrucciones a. "Cree un bucket de S3".
   c. En la pestaña **Administrar configuración de objetos**, selecciona **Activar control de versiones de objetos**.
   d. Si el bloqueo de objetos S3 está activado para el sistema StorageGRID, no habilite el bloqueo de objetos S3 para el depósito.
   e. Seleccione **Crear cucharón**.
   f. Seleccione **Finalizar**.
2. Repita estos pasos para crear un depósito idéntico para la misma cuenta de inquilino en el otro grid de la conexión de federación de grid.

   Según sea necesario, cada cubo puede utilizar una región diferente.

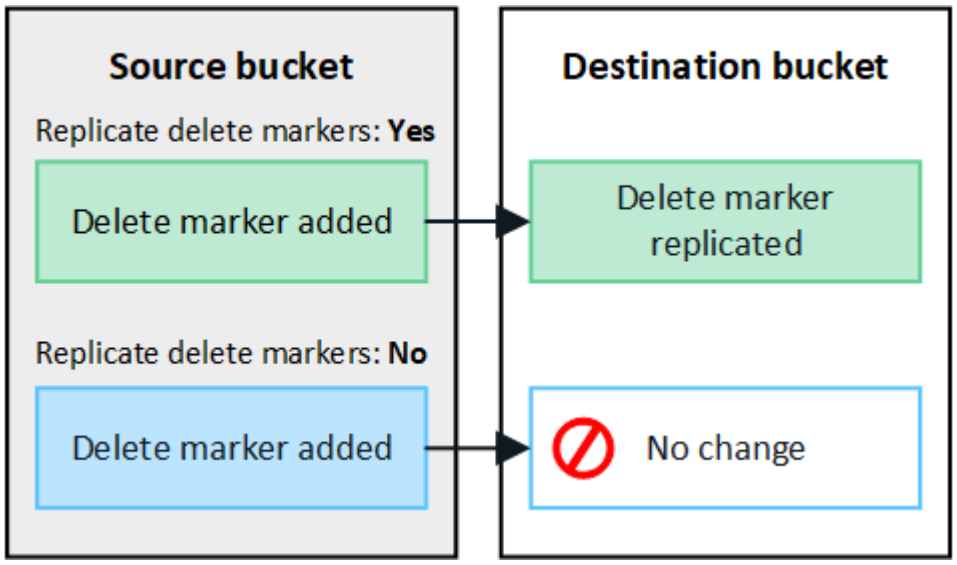
Habilite la replicación entre grid

Debe realizar estos pasos antes de agregar cualquier objeto a cada bloque.

Pasos

1. A partir de una cuadrícula cuyos objetos desea replicar, active "replicación entre grid en una dirección":
   a. Inicie sesión en la cuenta de inquilino del bloque.
   b. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
   c. Seleccione el nombre del cubo de la tabla para acceder a la página de detalles del cubo.
   d. Seleccione la pestaña **Replicación de cuadrícula**.
   e. Seleccione **Activar** y revise la lista de requisitos.
   f. Si se han cumplido todos los requisitos, seleccione la conexión de federación de grid que desea utilizar.
   g. Opcionalmente, cambie la configuración de **replicar marcadores de eliminación** para determinar qué sucede en la cuadrícula de destino si un cliente S3 emite una solicitud de eliminación a la cuadrícula de origen que no incluye un ID de versión:

- **Sí** (por defecto): Se agrega un marcador de borrado al depósito de origen y se replica en el cubo de destino.
- **No**: Se agrega un marcador de borrado al cubo de origen pero no se replica en el cubo de destino.



> Si la solicitud de eliminación incluye un ID de versión, esa versión de objeto se elimina permanentemente del depósito de origen. StorageGRID no replica las solicitudes de eliminación que incluyen un identificador de versión, por lo que la misma versión de objeto no se elimina del destino.

Consulte "Qué es la replicación entre grid" para obtener más detalles.

a. Opcionalmente, cambie la configuración de la categoría de auditoría **Replicación de cuadrícula** para administrar el volumen de los mensajes de auditoría:
   - **Error** (por defecto): Solo se incluyen solicitudes fallidas de replicación entre redes en la salida de la auditoría.
   - **Normal**: Se incluyen todas las solicitudes de replicación entre redes, lo que aumenta significativamente el volumen de la salida de auditoría.
b. Revise las selecciones. No puede cambiar esta configuración a menos que ambos cubos estén vacíos.
c. Seleccione **Habilitar y probar**.

   Después de unos momentos, aparece un mensaje de éxito. Los objetos agregados a este depósito ahora se replicarán automáticamente en la otra cuadrícula. **La replicación de cuadrícula cruzada** se muestra como una característica habilitada en la página de detalles del cubo.

2. Opcionalmente, vaya al cucharón correspondiente en la otra cuadrícula y. "permita la replicación entre grid en ambas direcciones".

Probar la replicación entre grids

Si se habilita la replicación entre grid para un bloque, es posible que deba comprobar que la conexión y la replicación entre grid funcionan correctamente y que los buckets de origen y de destino siguen cumpliendo todos los requisitos (por ejemplo, las versiones siguen activadas).

Antes de empezar

- Está utilizando un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Pasos

1. Inicie sesión en la cuenta de inquilino del bloque.
2. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
3. Seleccione el nombre del cubo de la tabla para acceder a la página de detalles del cubo.
4. Seleccione la pestaña **Replicación de cuadrícula**.
5. Seleccione **probar conexión**.

   Si la conexión es correcta, aparece el banner Correcta. De lo contrario, se muestra un mensaje de error que usted y el administrador de grid pueden utilizar para resolver el problema. Para obtener más información, consulte "Solucionar errores de federación de grid".

6. Si la replicación entre redes está configurada para que ocurra en ambas direcciones, vaya al depósito correspondiente en la otra cuadrícula y seleccione **Probar conexión** para verificar que la replicación entre redes funcione en la otra dirección.

Desactive la replicación entre grid

Puede detener de forma permanente la replicación entre grid si ya no desea copiar objetos en la otra grid.

Antes de deshabilitar la replicación entre grid, tenga en cuenta lo siguiente:

- Al desactivar la replicación entre grid no se elimina ningún objeto que ya se haya copiado entre grid. Por ejemplo, los objetos de `my-bucket` En la cuadrícula 1 en la que se ha copiado `my-bucket` En Grid 2 no se eliminan si deshabilita la replicación entre grid para ese bloque. Si desea eliminar estos objetos, debe eliminarlos manualmente.
- Si se activó la replicación entre grid para cada uno de los buckets (es decir, si la replicación se produce en ambas direcciones), puede deshabilitar la replicación entre grid para uno o ambos buckets. Por ejemplo, puede que desee desactivar la replicación de objetos de `my-bucket` En la cuadrícula 1 a. `my-bucket` En Grid 2, mientras continúa replicando objetos desde `my-bucket` En la cuadrícula 2 a. `my-bucket` En la cuadrícula 1.
- Debe deshabilitar la replicación entre grid para poder quitar el permiso de un inquilino para utilizar la conexión de federación de grid. Consulte "Gestionar inquilinos permitidos".
- Si deshabilita la replicación entre grid para un bucket que contiene objetos, no podrá volver a habilitar la replicación entre grid a menos que elimine todos los objetos de los buckets de origen y de destino.

  > ⚠ No puede volver a activar la replicación a menos que ambos buckets estén vacíos.

Antes de empezar

- Está utilizando un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Pasos

1. A partir de la cuadrícula cuyos objetos ya no desea replicar, detenga la replicación entre grid del bloque:
   a. Inicie sesión en la cuenta de inquilino del bloque.
   b. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.

c. Seleccione el nombre del cubo de la tabla para acceder a la página de detalles del cubo.

d. Seleccione la pestaña **Replicación de cuadrícula**.

e. Seleccione **Desactivar replicación**.

f. Si está seguro de que desea deshabilitar la replicación entre redes para este depósito, escriba **Sí** en el cuadro de texto y seleccione **Desactivar**.

   Después de unos momentos, aparece un mensaje de éxito. Los nuevos objetos agregados a este depósito ya no se pueden replicar automáticamente en el otro grid. **La replicación entre redes** ya no se muestra como una característica habilitada en la página Buckets.

2. Si la replicación entre grid se configuró para que se produzca en ambas direcciones, vaya al bucket correspondiente en la otra grid y detenga la replicación entre grid en la otra dirección.

Ver conexiones de federación de grid

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, puede ver las conexiones permitidas.

Antes de empezar

- La cuenta de inquilino tiene el permiso **Use grid federation connection**.
- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Pasos

1. Selecciona **STORAGE (S3)** > **Grid federation connections**.

   Aparece la página de conexión de Grid federation e incluye una tabla que resume la siguiente información:

Columna	Descripción
Nombre de conexión	Las conexiones de federación de grid que este inquilino tiene permiso para utilizar.
Buckets con replicación entre grid	Para cada conexión de federación de grid, los buckets de inquilinos que tienen habilitada la replicación entre grid. Los objetos agregados a estos cubos se replicarán en la otra cuadrícula de la conexión.
Último error	Para cada conexión de federación de grid, se produce el error más reciente, si lo hay, cuando los datos se están replicando en la otra cuadrícula. Consulte Borre el último error.

2. Si lo desea, seleccione un nombre de cubo a. "ver detalles del período".

Borrar el último error

Un error puede aparecer en la columna **last error** por uno de estos motivos:

- No se ha encontrado la versión del objeto de origen.
- No se ha encontrado el depósito de origen.

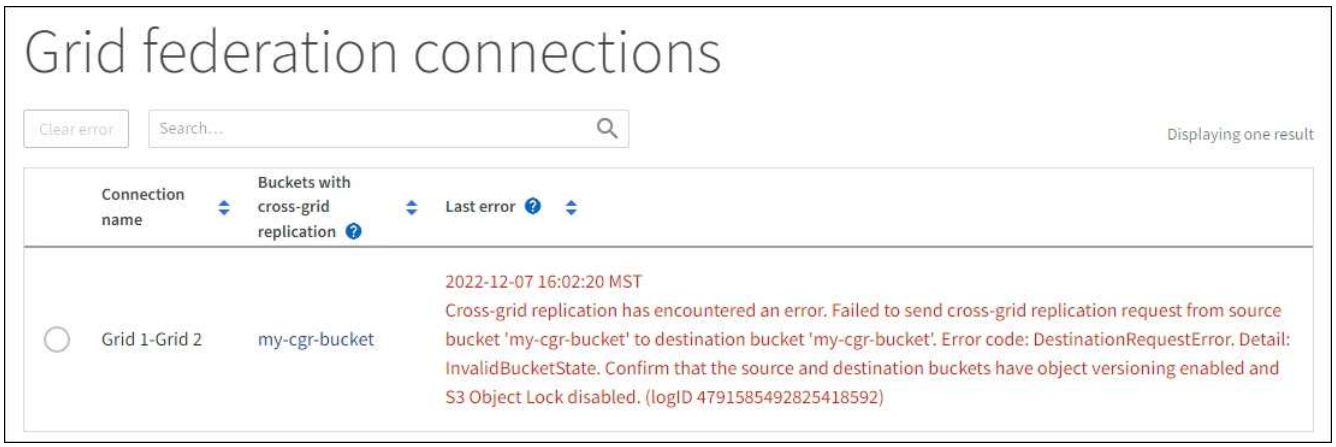
- Se ha suprimido el depósito de destino.
- Una cuenta diferente ha vuelto a crear el bloque de destino.
- Se ha suspendido el control de versiones del bloque de destino.
- La misma cuenta ha vuelto a crear el depósito de destino, pero ahora no tiene versiones.

> Esta columna solo muestra el último error de replicación entre cuadrículas que se produce; no se mostrarán los errores anteriores que podrían haberse producido.

Pasos

1. Si aparece un mensaje en la columna **Último error**, vea el texto del mensaje.

   Por ejemplo, este error indica que el depósito de destino para la replicación entre grid estaba en un estado no válido, posiblemente porque el control de versiones estaba suspendido o porque se activó el bloqueo de objetos S3.



2. Realice las acciones recomendadas. Por ejemplo, si se suspendió el control de versiones en el bloque de destino para la replicación entre grid, vuelva a habilitar el control de versiones para ese bloque.
3. Seleccione la conexión de la tabla.
4. Seleccione **Borrar error**.
5. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espere 5-6 minutos e incorpore un objeto nuevo en el bloque. Confirme que el mensaje de error no vuelve a aparecer.

   > Para asegurarse de que el mensaje de error se borra, espere al menos 5 minutos después de la marca de tiempo del mensaje antes de introducir un nuevo objeto.

7. Para determinar si se ha producido un error en la replicación de algún objeto debido al error de depósito, consulte "Identifique y vuelva a intentar operaciones de replicación fallidas".

Gestionar grupos y usuarios

Usar la federación de identidades

El uso de la federación de identidades agiliza la configuración de usuarios y grupos de inquilinos, y permite a los usuarios de inquilinos iniciar sesión en la cuenta de inquilinos

utilizando credenciales conocidas.

Configurar la federación de identidades para el Administrador de inquilinos

Puede configurar la federación de identidades para el administrador de inquilinos si desea que los grupos de inquilinos y los usuarios se gestionen en otro sistema como Active Directory, Azure Active Directory (Azure AD), OpenLDAP u Oracle Directory Server.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Se utiliza Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidades.

> Si desea utilizar un servicio LDAP v3 que no esté en la lista, póngase en contacto con el soporte técnico.

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Consulte Instrucciones para configurar el servidor OpenLDAP.
- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades debe usar TLS 1.2 o 1.3. Consulte "Cifrados compatibles para conexiones TLS salientes".

Acerca de esta tarea

Si puede configurar un servicio de federación de identidades para su inquilino depende de cómo se haya configurado su cuenta de inquilino. Es posible que el inquilino comparta el servicio de federación de identidades configurado para Grid Manager. Si ve este mensaje cuando accede a la página Identity Federation, no puede configurar un origen de identidad federado independiente para este arrendatario.

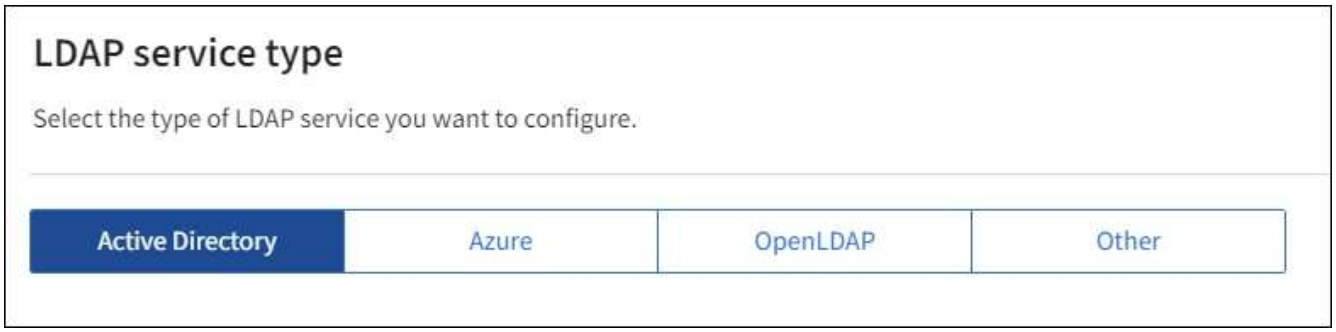
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Introducir configuración

Al configurar Identify federation, proporciona los valores que StorageGRID necesita para conectarse a un servicio LDAP.

Pasos

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



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

4. Si ha seleccionado **otros**, complete los campos de la sección atributos LDAP . De lo contrario, vaya al paso siguiente.
   - **Nombre único de usuario**: 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 va a configurar Oracle Directory Server, introduzca `uid`.
   - **UUID de usuario**: 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 va a configurar Oracle Directory Server, introduzca `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**: 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 va a configurar Oracle Directory Server, introduzca `cn`.
   - **UUID de grupo**: 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 va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
5. Para todos los tipos de servicio LDAP, introduzca la información de servidor LDAP y conexión de red necesaria en la sección Configure LDAP Server.
   - **Hostname**: El nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
   - **Puerto**: El puerto utilizado para conectarse al servidor LDAP.

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

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

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

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

     - `sAMAccountName` o. `uid`

- `objectGUID`, `entryUUID`, o. `nsuniqueid`
- `cn`
- `memberOf` o. `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, y. `userPrincipalName`
- **Azure**: `accountEnabled` y.. `userPrincipalName`

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

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

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

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

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

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

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

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

Introduzca uno de estos patrones:

- **Patrón UserPrincipalName (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 completo**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

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

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.
   ◦ **Use STARTTLS**: Utilice STARTTLS para asegurar 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.
   ◦ **Use LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Azure.
   ◦ **No utilice TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Azure.

El uso de la opción **no usar TLS** no es compatible si el servidor de Active Directory aplica la firma LDAP. Debe usar STARTTLS o LDAPS.

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

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

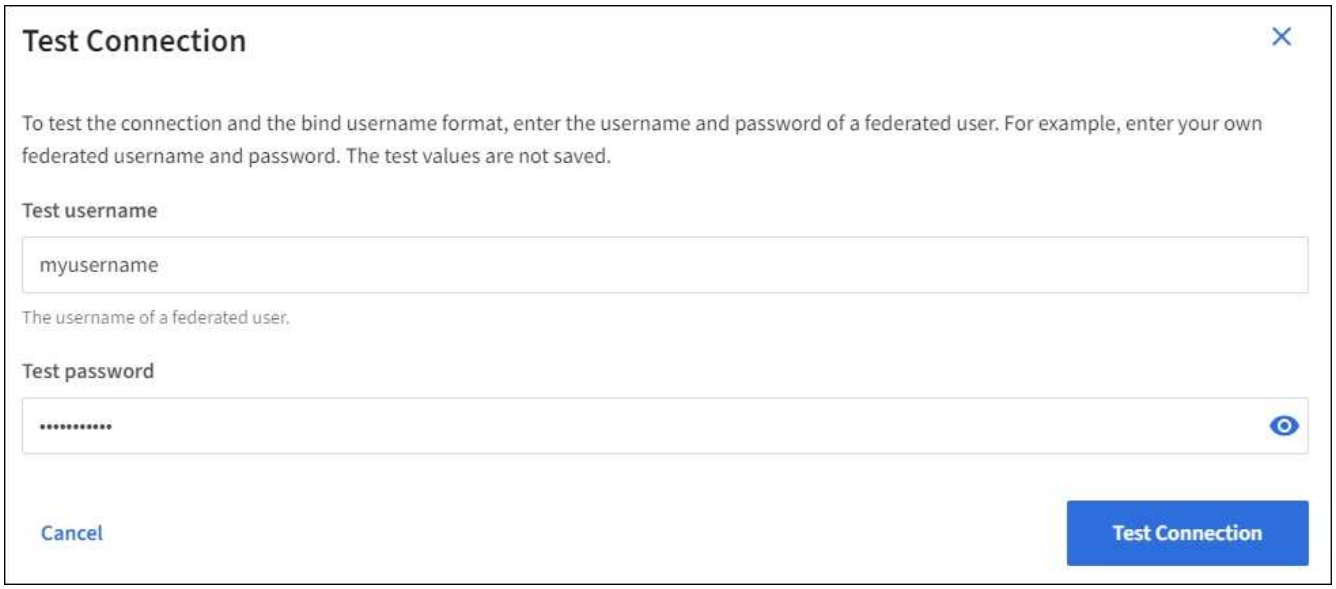
Pruebe la conexión y guarde la configuración

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

Pasos

1. Seleccione **probar conexión**.
2. Si no se proporciona un formato de nombre de usuario de enlace:
   - Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.
   - Si la configuración de conexión no es válida, aparecerá un mensaje que indica que no se ha podido establecer la conexión de prueba. Seleccione **Cerrar**. Luego, resuelva cualquier problema y vuelva a probar la conexión.
3. Si proporcionó un formato de nombre de usuario de enlace, introduzca el nombre de usuario y la contraseña de un usuario federado válido.

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



   - Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.

- Aparecerá un mensaje de error si las opciones de conexión, el formato de nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva los problemas y vuelva a probar la conexión.

Forzar la sincronización con el origen de identidades

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

Pasos

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

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

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

Deshabilitar la federación de identidades

Puede deshabilitar temporalmente o de forma permanente la federación de identidades para grupos y usuarios. Cuando la federación de identidades está deshabilitada, no existe comunicación entre StorageGRID y el origen de identidades. Sin embargo, cualquier configuración que haya configurado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidades en el futuro.

Acerca de esta tarea

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

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que hayan iniciado sesión en ese momento, retendrán el acceso al sistema StorageGRID hasta que caduque la sesión, pero no podrán iniciar sesión después de que caduque la sesión.
- No se realizará la sincronización entre el sistema StorageGRID y el origen de identidad, y no se realizarán alertas ni alarmas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Habilitar federación de identidad** está desactivada si el inicio de sesión único (SSO) está configurado en **enabled** o **Sandbox Mode**. El estado de SSO de la página Single Sign-On debe ser **Desactivado** antes de poder deshabilitar la federación de identidades. Consulte "Desactive el inicio de sesión único".

Pasos

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

Instrucciones para configurar el servidor OpenLDAP

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

En el caso de fuentes de identidad que no sean ActiveDirectory ni Azure, StorageGRID no bloqueará automáticamente el acceso S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine cualquier clave S3 para el usuario o elimine al usuario de todos los grupos.

Revestimientos memberOf y reft

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

Indización

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

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

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

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

Gestionar grupos de inquilinos

Cree grupos para un inquilino de S3

Es posible gestionar permisos para grupos de usuarios S3 importando grupos federados o creando grupos locales.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si planea importar un grupo federado, tiene "federación de identidades configurada", y el grupo federado ya existe en el origen de identidad configurado.
- Si su cuenta de inquilino tiene el permiso **Use grid federation connection**, ha revisado el flujo de trabajo y las consideraciones para "clonación de usuarios y grupos de inquilinos", y ha iniciado sesión en la cuadrícula de origen del inquilino.

Acceda al asistente Crear grupo

Como primer paso, acceda al asistente de creación de grupos.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, confirme que aparece un

banner azul, indicando que los nuevos grupos creados en esta cuadrícula se clonarán en el mismo inquilino en la otra cuadrícula de la conexión. Si este banner no aparece, puede que haya iniciado sesión en la cuadrícula de destino del inquilino.

3. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

1. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

2. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.

     Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, se producirá un error de clonación si el mismo **nombre único** ya existe para el inquilino en la cuadrícula de destino.

   - **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.
3. Seleccione **continuar**.

Administrar permisos de grupo

Los permisos de grupo controlan las tareas que los usuarios pueden realizar en el gestor de inquilinos y en la API de gestión de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:
   - **Read-write** (por defecto): Los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden hacer ningún cambio ni realizar ninguna operación en el administrador de inquilinos o la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

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

2. Seleccione uno o más permisos para este grupo.

   Consulte "Permisos de gestión de inquilinos".

3. Seleccione **continuar**.

Establezca la política de grupo S3

La política de grupo determina qué permisos de acceso S3 tendrán los usuarios.

Pasos

1. Seleccione la política que desea usar para este grupo.

Política de grupo	Descripción
Sin acceso S3	Predeterminado. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que el acceso se conceda con una política de bloque. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3.
Acceso de sólo lectura	Los usuarios de este grupo tienen acceso de solo lectura a los recursos de S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puede editar esta cadena.
Acceso total	Los usuarios de este grupo tienen acceso completo a recursos de S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena.

Política de grupo	Descripción
Mitigación del ransomware	Esta política de ejemplo se aplica a todos los depósitos de este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden suprimir de forma permanente objetos de los bloques que tienen activado el control de versiones de objetos. Los usuarios del administrador de inquilinos que tienen el permiso **Administrar todos los cubos** pueden anular esta política de grupo. Limite el permiso Gestionar todos los buckets a usuarios de confianza y use la autenticación multifactor (MFA) cuando esté disponible.
Personalizado	A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

2. Si ha seleccionado **personalizado**, introduzca la directiva de grupo. Cada política de grupo tiene un límite de tamaño de 5,120 bytes. Debe introducir una cadena con formato JSON válida.

   Para obtener información detallada sobre las políticas de grupo, incluida la sintaxis del idioma y los ejemplos, consulte "Ejemplo de políticas de grupo".

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

Añadir usuarios (sólo grupos locales)

Puede guardar el grupo sin agregar usuarios o, opcionalmente, puede agregar cualquier usuario local que ya exista.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, los usuarios que seleccione al crear un grupo local en la cuadrícula de origen no se incluyen cuando el grupo se clona en la cuadrícula de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Pasos

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.
2. Seleccione **Crear grupo** y **Finalizar**.

   El grupo creado aparece en la lista de grupos.

   Si su cuenta de inquilino tiene el permiso **Use grid federation connection** y usted está en la cuadrícula de origen del inquilino, el nuevo grupo se clona en la cuadrícula de destino del inquilino. **Success** aparece como **Cloning status** en la sección Overview de la página de detalles del grupo.

Cree grupos para un inquilino de Swift

Es posible gestionar los permisos de acceso para una cuenta de inquilino de Swift mediante la importación de grupos federados o la creación de grupos locales. Al menos un grupo debe tener el permiso de administrador de Swift, que se requiere para gestionar los contenedores y los objetos de una cuenta de inquilino de Swift.

Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si planea importar un grupo federado, tiene "federación de identidades configurada", y el grupo federado ya existe en el origen de identidad configurado.

Acceda al asistente Crear grupo

Pasos

Como primer paso, acceda al asistente de creación de grupos.

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

1. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

2. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.
   - **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.
3. Seleccione **continuar**.

Administrar permisos de grupo

Los permisos de grupo controlan las tareas que los usuarios pueden realizar en el gestor de inquilinos y en la API de gestión de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:
   - **Read-write** (por defecto): Los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden hacer ningún cambio ni realizar ninguna operación en el administrador de inquilinos o la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

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

2. Seleccione la casilla de verificación **acceso raíz** si los usuarios del grupo necesitan iniciar sesión en el Administrador de inquilinos o en la API de administración de inquilinos.
3. Seleccione **continuar**.

Configure la política de grupo de Swift

Los usuarios de Swift necesitan permiso de administrador para autenticarse en la API REST DE Swift para crear contenedores e ingerir objetos.

1. Seleccione la casilla de verificación **Swift administrator** si los usuarios del grupo necesitan usar la API REST DE Swift para administrar contenedores y objetos.
2. Si está creando un grupo local, seleccione **continuar**. Si está creando un grupo federado, seleccione **Crear grupo** y **Finalizar**.

Añadir usuarios (sólo grupos locales)

Puede guardar el grupo sin agregar usuarios o, opcionalmente, puede agregar cualquier usuario local que ya exista.

Pasos

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

   Si aún no ha creado usuarios locales, puede agregar este grupo al usuario en la página Usuarios. Consulte "Gestionar usuarios locales".

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

   El grupo creado aparece en la lista de grupos.

Permisos de gestión de inquilinos

Antes de crear un grupo de arrendatarios, tenga en cuenta qué permisos desea asignar a ese grupo. Los permisos de administración de inquilinos determinan qué tareas pueden realizar los usuarios con el Administrador de inquilinos o la API de gestión de inquilinos. Un usuario puede pertenecer a uno o más grupos. Los permisos son acumulativos si un usuario pertenece a varios grupos.

Para iniciar sesión en el Administrador de arrendatarios o utilizar la API de administración de arrendatarios, los usuarios deben pertenecer a un grupo que tenga al menos un permiso. Todos los usuarios que puedan iniciar sesión pueden realizar las siguientes tareas:

- Vea la consola
- Cambiar su propia contraseña (para usuarios locales)

Para todos los permisos, la configuración del modo de acceso del grupo determina si los usuarios pueden cambiar la configuración y realizar operaciones o si sólo pueden ver la configuración y las características relacionadas.

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

Puede asignar los siguientes permisos a un grupo. Tenga en cuenta que los inquilinos de S3 y los inquilinos de Swift tienen diferentes permisos de grupo.

Permiso	Descripción	Detalles
Acceso raíz	Proporciona acceso completo al administrador de inquilinos y a la API de gestión de inquilinos.	Los usuarios de Swift deben tener permiso de acceso raíz para iniciar sesión en la cuenta de inquilino.
Administrador	Solo para inquilinos Swift. Proporciona acceso completo a los contenedores y objetos de Swift para esta cuenta de inquilino	Los usuarios de Swift deben contar con el permiso de administrador de Swift para realizar cualquier operación con la API REST DE Swift.
Gestione sus propias credenciales de S3	Permite a los usuarios crear y eliminar sus propias claves de acceso S3.	Los usuarios que no tienen este permiso no ven la opción de menú **STORAGE (S3)** > **My S3 access keys**.
Ver todos los cubos	**S3 inquilinos**: Permite a los usuarios ver todas las configuraciones de cubos y cubos. • Inquilinos Swift*: Permite a los usuarios de Swift ver todos los contenedores y configuraciones de contenedores utilizando la API de administración de inquilinos.	Los usuarios que no tienen el permiso Ver todos los cubos o Gestionar todos los cubos no ven la opción de menú **Buckets**. Este permiso se sustituye por el permiso Gestionar todos los cubos. No afecta a las políticas de grupo o bloque S3 utilizadas por los clientes S3 o la consola S3. Solo puede asignar este permiso a grupos de Swift desde la API de gestión de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.
Gestionar todos los cucharones	**S3 inquilinos**: Permite a los usuarios utilizar el Administrador de inquilinos y la API de administración de inquilinos para crear y eliminar buckets S3 y para administrar la configuración de todos los S3 buckets en la cuenta de inquilino, independientemente de las políticas de buckets o grupos S3. • Inquilinos Swift*: Permite a los usuarios Swift controlar la consistencia de los contenedores Swift mediante la API de administración de inquilinos.	Los usuarios que no tienen el permiso Ver todos los cubos o Gestionar todos los cubos no ven la opción de menú **Buckets**. Este permiso sustituye al permiso Ver todos los cubos. No afecta a las políticas de grupo o bloque S3 utilizadas por los clientes S3 o la consola S3. Solo puede asignar este permiso a grupos de Swift desde la API de gestión de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.

Permiso	Descripción	Detalles
Gestionar puntos finales	Permite a los usuarios utilizar el Gestor de inquilinos o la API de gestión de inquilinos para crear o editar puntos finales de servicio de plataforma, que se utilizan como destino para los servicios de plataforma de StorageGRID.	Los usuarios que no tienen este permiso no ven la opción de menú **Platform services endpoints**.
Utilice la pestaña Consola de S3	Cuando se combina con el permiso Ver todos los cubos o Gestionar todos los cubos, permite a los usuarios ver y gestionar objetos desde la pestaña Consola de S3 en la página de detalles de un bloque.	

Gestionar grupos

Gestione los grupos de arrendatarios según sea necesario para ver, editar o duplicar un grupo y mucho más.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Ver o editar grupo

Puede ver y editar la información básica y los detalles de cada grupo.

Pasos

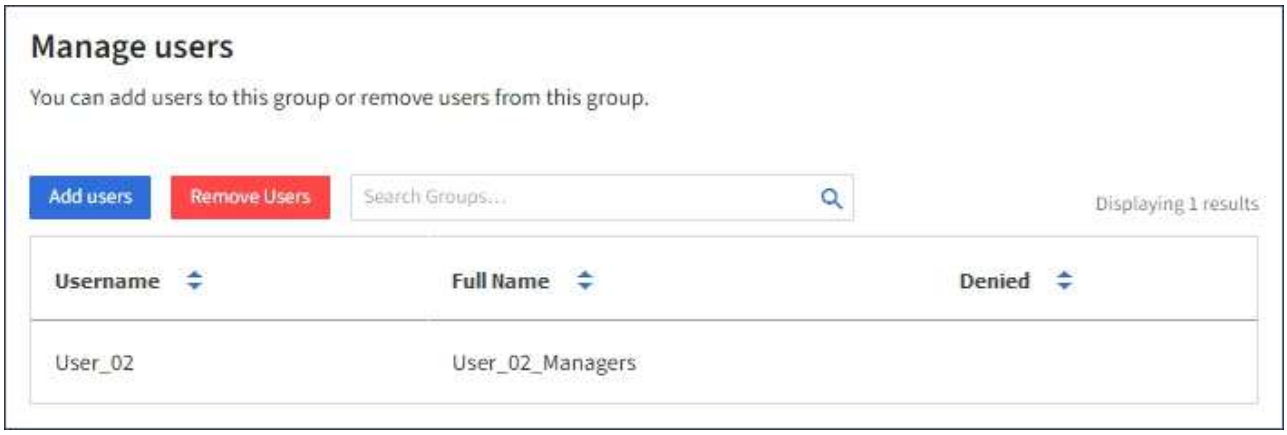
1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Revise la información proporcionada en la página Grupos, que muestra información básica de todos los grupos locales y federados de esta cuenta de arrendatario.

   Si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo grupos en la cuadrícula de origen del inquilino:

   - Un mensaje de banner indica que si edita o elimina un grupo, los cambios no se sincronizarán con la otra cuadrícula.
   - Según sea necesario, un mensaje de banner indica si los grupos no se clonaron en el inquilino en la cuadrícula de destino. Puede hacerlo volver a intentar un clon de grupo eso falló.
3. Si desea cambiar el nombre del grupo:
   a. Seleccione la casilla de verificación para el grupo.
   b. Selecciona **Acciones** > **Editar nombre de grupo**.
   c. Introduzca el nuevo nombre.
   d. Selecciona **Guardar cambios.**
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre del grupo.

- Selecciona la casilla de verificación del grupo y selecciona **Acciones** > **Ver detalles del grupo**.

5. Revise la sección Visión General, que muestra la siguiente información para cada grupo:
   - Nombre para mostrar
   - Nombre exclusivo
   - Tipo
   - Modo de acceso
   - Permisos
   - S3 Política
   - Número de usuarios en este grupo
   - Campos adicionales si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo el grupo en la cuadrícula de origen del inquilino:
     - Estado de clonación, ya sea **Success** o **Failure**
     - Un banner azul que indica que si edita o elimina este grupo, los cambios no se sincronizarán con la otra cuadrícula.
6. Edite la configuración del grupo según sea necesario. Consulte "Cree grupos para un inquilino de S3" y.. "Cree grupos para un inquilino de Swift" para obtener más información acerca de lo que se debe introducir.
   a. En la sección Descripción general, cambie el nombre mostrado seleccionando el nombre o el icono de edición .
   b. En la pestaña **Permisos de grupo**, actualice los permisos y seleccione **Guardar cambios**.
   c. En la pestaña **Política de grupo**, realice los cambios y seleccione **Guardar cambios**.
      - Si está editando un grupo S3, seleccione opcionalmente una política de grupo S3 diferente o introduzca la cadena JSON de una política personalizada, según corresponda.
      - Si está editando un grupo Swift, opcionalmente seleccione o desactive la casilla de verificación **Swift Administrator**.
7. Para añadir uno o varios usuarios locales existentes al grupo:
   a. Seleccione la ficha Usuarios.



   b. Selecciona **Añadir usuarios**.
   c. Seleccione los usuarios existentes que desea agregar y seleccione **Agregar usuarios**.

      Aparece un mensaje de éxito en la parte superior derecha.

8. Para eliminar usuarios locales del grupo:
   a. Seleccione la ficha Usuarios.
   b. Selecciona **Eliminar usuarios**.
   c. Seleccione los usuarios que desea eliminar y seleccione **Eliminar usuarios**.

      Aparece un mensaje de éxito en la parte superior derecha.

9. Confirma que has seleccionado **Guardar cambios** para cada sección que cambiaste.

Grupo duplicado

Puede duplicar un grupo existente para crear nuevos grupos más rápidamente.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y duplica un grupo de la cuadrícula de origen del inquilino, el grupo duplicado se clonará en la cuadrícula de destino del inquilino.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de control del grupo que desea duplicar.
3. Seleccione **acciones** > **Duplicar grupo**.
4. Consulte "Cree grupos para un inquilino de S3" o. "Cree grupos para un inquilino de Swift" para obtener más información acerca de lo que se debe introducir.
5. Seleccione **Crear grupo**.

Vuelva a intentar clonar el grupo

Para volver a intentar un clon que generó errores:

1. Seleccione cada grupo que indique *(Error de clonación)* debajo del nombre del grupo.
2. Selecciona **Acciones** > **Clonar grupos**.
3. Vea el estado de la operación de clonación desde la página de detalles de cada grupo que está clonando.

Para obtener más información, consulte "Clone los usuarios y los grupos de inquilinos".

Elimine uno o más grupos

Puede eliminar uno o varios grupos. Cualquier usuario que pertenezca únicamente a un grupo que se haya eliminado ya no podrá iniciar sesión en el gestor de inquilinos ni utilizar la cuenta de inquilino.

> Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y eliminas un grupo, StorageGRID no eliminará el grupo correspondiente en la otra cuadrícula. Si necesita mantener esta información sincronizada, debe eliminar el mismo grupo de ambas cuadrículas.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de verificación para cada grupo que desee eliminar.
3. Selecciona **Acciones** > **Eliminar grupo** o **Acciones** > **Eliminar grupos**.

Se muestra un cuadro de diálogo de confirmación.

4. Selecciona **Borrar grupo** o **Eliminar grupos**.

Gestionar usuarios locales

Puede crear usuarios locales y asignarles grupos locales para determinar las funciones a las que pueden acceder estos usuarios. El gestor de inquilinos incluye un usuario local predefinido, denominado «root». Aunque puede agregar y eliminar usuarios locales, no puede eliminar el usuario root.

> Si el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el gestor de inquilinos o en la API de gestión de inquilinos, aunque pueden utilizar aplicaciones cliente para acceder a los recursos del inquilino, según los permisos del grupo.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si su cuenta de inquilino tiene el permiso **Use grid federation connection**, ha revisado el flujo de trabajo y las consideraciones para "clonación de usuarios y grupos de inquilinos", y ha iniciado sesión en la cuadrícula de origen del inquilino.

Cree un usuario local

Puede crear un usuario local y asignarlos a uno o varios grupos locales para controlar sus permisos de acceso.

Los usuarios de S3 que no pertenecen a ningún grupo no tienen permisos de administración ni se les aplican S3 políticas de grupo. Es posible que estos usuarios tengan acceso a bloques de S3 otorgado a través de una política de bloques.

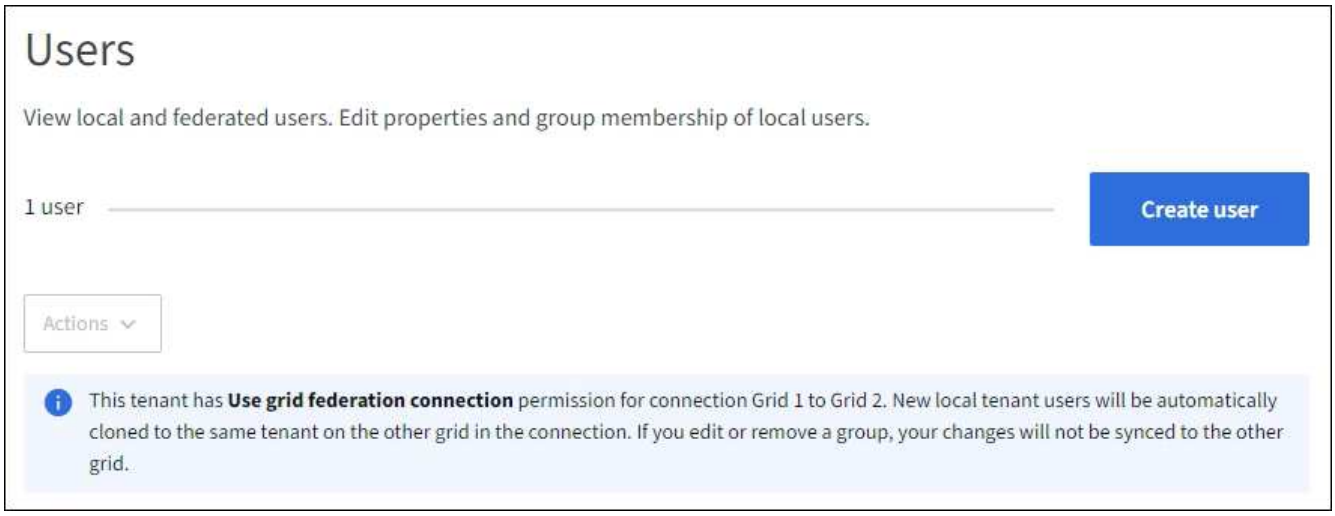
Los usuarios de Swift que no pertenezcan a ningún grupo no tienen permisos de administración ni acceso a contenedor Swift.

Acceda al asistente Crear usuario

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.

   Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, un banner azul indica que esta es la cuadrícula de origen del inquilino. Todos los usuarios locales que cree en esta cuadrícula se clonarán en la otra cuadrícula de la conexión.



2. Seleccione **Crear usuario**.

Introduzca las credenciales

Pasos

1. Para el paso **Introducir credenciales de usuario**, complete los siguientes campos.

Campo	Descripción
Nombre completo	El nombre completo de este usuario, por ejemplo, el nombre y apellidos de una persona o el nombre de una aplicación.
Nombre de usuario	Nombre que utilizará este usuario para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar. **Nota**: Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, se producirá un error de clonación si el mismo **Nombre de usuario** ya existe para el inquilino en la cuadrícula de destino.
Contraseña y confirme la contraseña	La contraseña que el usuario utilizará inicialmente al iniciar sesión.
Denegar el acceso	Seleccione **Sí** para evitar que este usuario inicie sesión en la cuenta de inquilino, aunque todavía pertenezca a uno o más grupos. Por ejemplo, selecciona **Sí** para suspender temporalmente la capacidad de un usuario para iniciar sesión.

2. Seleccione **continuar**.

Asignar a grupos

Pasos

1. Asigne el usuario a uno o más grupos locales para determinar qué tareas se pueden realizar.

   La asignación de un usuario a grupos es opcional. Si lo prefiere, puede seleccionar usuarios al crear o editar grupos.

Los usuarios que no pertenezcan a ningún grupo no tendrán permisos de administración. Los permisos son acumulativos. Los usuarios tendrán todos los permisos para todos los grupos a los que pertenezcan. Consulte "Permisos de gestión de inquilinos".

2. Seleccione **Crear usuario**.

   Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y usted está en la cuadrícula de origen del inquilino, el nuevo usuario local se clona en la cuadrícula de destino del inquilino. **Success** aparece como **Cloning status** en la sección Overview de la página de detalles del usuario.

3. Seleccione **Finalizar** para volver a la página Usuarios.

Ver o editar usuario local

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Revise la información proporcionada en la página Usuarios, que muestra información básica para todos los usuarios locales y federados de esta cuenta de arrendatario.

   Si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo al usuario en la cuadrícula de origen del inquilino:

   - Un mensaje de banner indica que si edita o elimina un usuario, los cambios no se sincronizarán con la otra cuadrícula.
   - Según sea necesario, un mensaje de banner indica si los usuarios no se clonaron en el inquilino en la cuadrícula de destino. Puede hacerlo vuelva a intentar un clon de usuario que haya fallado.
3. Si desea cambiar el nombre completo del usuario:
   a. Seleccione la casilla de control para el usuario.
   b. Selecciona **Acciones** > **Editar nombre completo**.
   c. Introduzca el nuevo nombre.
   d. Selecciona **Guardar cambios.**
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre de usuario.
   - Selecciona la casilla de verificación para el usuario y selecciona **Acciones** > **Ver detalles de usuario**.
5. Revise la sección Visión General, que muestra la siguiente información para cada usuario:
   - Nombre completo
   - Nombre de usuario
   - Tipo de usuario
   - Acceso denegado
   - Modo de acceso
   - Pertenencia a grupos
   - Campos adicionales si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo al usuario en la cuadrícula de origen del inquilino:
     - Estado de clonación, ya sea **Success** o **Failure**
     - Un banner azul que indica que si edita este usuario, los cambios no se sincronizarán con la otra

cuadrícula.

6. Edite la configuración del usuario según sea necesario. Consulte Crear usuario local para obtener más información acerca de lo que se debe introducir.
   a. En la sección Descripción general, cambie el nombre completo seleccionando el nombre o el icono de edición .

      No puede cambiar el nombre de usuario.

   b. En la pestaña **Contraseña**, cambie la contraseña del usuario y seleccione **Guardar cambios**.
   c. En la pestaña **Acceso**, selecciona **No** para permitir que el usuario inicie sesión o selecciona **Sí** para evitar que el usuario inicie sesión. Luego, selecciona **Guardar cambios**.
   d. En la pestaña **Teclas de acceso**, selecciona **Crear clave** y sigue las instrucciones para "Creando las claves de acceso S3 de otro usuario".
   e. En la pestaña **Grupos**, selecciona **Editar grupos** para agregar el usuario a los grupos o eliminar al usuario de los grupos. Luego, selecciona **Guardar cambios**.
7. Confirma que has seleccionado **Guardar cambios** para cada sección que cambiaste.

Usuario local duplicado

Puede duplicar un usuario local para crear un usuario nuevo más rápidamente.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y duplica un usuario de la cuadrícula de origen del inquilino, el usuario duplicado se clonará en la cuadrícula de destino del inquilino.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Seleccione la casilla de control para el usuario que desea duplicar.
3. Selecciona **Acciones** > **Usuario duplicado**.
4. Consulte Crear usuario local para obtener más información acerca de lo que se debe introducir.
5. Seleccione **Crear usuario**.

Reintente clonar el usuario

Para volver a intentar un clon que generó errores:

1. Seleccione cada usuario que indique *(Error de clonación)* debajo del nombre de usuario.
2. Selecciona **Acciones** > **Clonar usuarios**.
3. Vea el estado de la operación de clonación desde la página de detalles de cada usuario que está clonando.

Para obtener más información, consulte "Clone los usuarios y los grupos de inquilinos".

Elimine uno o varios usuarios locales

Puede eliminar de forma permanente uno o varios usuarios locales que ya no necesiten acceder a la cuenta de inquilino de StorageGRID.

Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y eliminas a un usuario local, StorageGRID no eliminará al usuario correspondiente en la otra cuadrícula. Si necesita mantener esta información sincronizada, debe eliminar el mismo usuario de ambas cuadrículas.

Debe utilizar el origen de identidad federado para eliminar usuarios federados.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Seleccione la casilla de verificación para cada usuario que desee eliminar.
3. Selecciona **Acciones** > **Eliminar usuario** o **Acciones** > **Eliminar usuarios**.

   Se muestra un cuadro de diálogo de confirmación.

4. Seleccione **Eliminar usuario** o **Eliminar usuarios**.

Gestión de claves de acceso de S3

Gestionar claves de acceso S3: Descripción general

Cada usuario de una cuenta de inquilino de S3 debe tener una clave de acceso para almacenar y recuperar objetos en el sistema StorageGRID. Una clave de acceso consta de un ID de clave de acceso y una clave de acceso secreta.

Las claves de acceso S3 se pueden gestionar de la siguiente manera:

- Los usuarios que tienen el permiso **Administrar sus propias credenciales de S3** pueden crear o eliminar sus propias claves de acceso de S3.
- Los usuarios que tienen el permiso **root access** pueden administrar las claves de acceso para la cuenta root de S3 y todos los demás usuarios. Las claves de acceso raíz proporcionan acceso completo a todos los bloques y objetos para el inquilino, a menos que se deshabilite explícitamente mediante una política de bloque.

StorageGRID admite la autenticación Signature versión 2 y Signature versión 4. No se permite el acceso de cuenta cruzada a menos que una política de bloque lo habilite explícitamente.

Cree sus propias claves de acceso S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede crear sus propias claves de acceso S3. Debe tener una clave de acceso para acceder a los cubos y objetos.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Administre sus propias credenciales de S3 o permiso de acceso raíz".

Acerca de esta tarea

Puede crear una o varias claves de acceso S3 que le permiten crear y gestionar bloques para su cuenta de

inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con su nuevo ID de clave de acceso y clave de acceso secreta. Por seguridad, no cree más claves de las que necesita, y elimine las claves que no está utilizando. Si sólo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la antigua y, a continuación, elimine la anterior.

Cada clave puede tener un tiempo de caducidad específico o no puede caducar. Siga estas directrices para el tiempo de caducidad:

- Establezca un tiempo de caducidad para sus llaves para limitar su acceso a un período de tiempo determinado. Establecer un tiempo de caducidad corto puede ayudar a reducir el riesgo si el ID de clave de acceso y la clave de acceso secreta están expuestos accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo de seguridad en su entorno es bajo y no necesita crear periódicamente claves nuevas, no tiene que establecer un tiempo de caducidad para las claves. Si decide más tarde crear claves nuevas, elimine manualmente las claves antiguas.

> Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.

   Aparecerá la página Mis claves de acceso y mostrará una lista de las claves de acceso existentes.

2. Seleccione **Crear clave**.
3. Debe realizar una de las siguientes acciones:
   - Seleccione **no establezca un tiempo de caducidad** para crear una clave que no caducará. (Predeterminado)
   - Seleccione **establecer un tiempo de caducidad** y establezca la fecha y la hora de caducidad.

     > La fecha de caducidad puede ser un máximo de cinco años a partir de la fecha actual. El tiempo de caducidad puede ser un mínimo de un minuto desde la hora actual.

4. Seleccione **Crear clave de acceso**.

   Aparece el cuadro de diálogo Descargar clave de acceso, en el que se enumeran el ID de clave de acceso y la clave de acceso secreta.

5. 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 clave de acceso y la clave de acceso secreta.

   > No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No puede copiar ni descargar claves después de cerrar el cuadro de diálogo.

6. Seleccione **Finalizar**.

   La nueva clave aparece en la página Mis claves de acceso.

7. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, utilice opcionalmente la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la cuadrícula de origen al inquilino en la cuadrícula de destino. Consulte "Clone las claves de acceso S3 mediante la API".

Consulte las claves de acceso de S3

Si está utilizando un inquilino de S3 y tiene el "permiso apropiado", Puede ver una lista de sus S3 teclas de acceso. Puede ordenar la lista por tiempo de caducidad, de modo que puede determinar qué claves caducarán pronto. Según sea necesario, puedes "crear nuevas claves" o. "teclas de eliminación" que ya no utiliza.

> Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene las credenciales Administrar sus propias credenciales S3 "permiso".

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.
2. Desde la página Mis claves de acceso, ordene las claves de acceso existentes por **Tiempo de caducidad** o **ID de clave de acceso**.
3. Según sea necesario, cree nuevas claves o elimine las claves que ya no esté utilizando.

   Si crea claves nuevas antes de que caduquen las claves existentes, puede empezar a utilizar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

   Las claves caducadas se eliminan automáticamente.

Elimine sus propias claves de acceso de S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede eliminar sus propias claves de acceso S3. Cuando se elimina una clave de acceso, ya no se puede utilizar para acceder a los objetos y los bloques de la cuenta de inquilino.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Usted tiene la "Administre sus propios permisos de credenciales de S3".

Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.
2. En la página Mis claves de acceso, seleccione la casilla de verificación de cada clave de acceso que desee eliminar.
3. Seleccione **tecla Eliminar**.
4. En el cuadro de diálogo de confirmación, seleccione **Tecla Eliminar**.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página.

Cree las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene el permiso apropiado, puede crear claves de acceso S3 para otros usuarios, como las aplicaciones que necesitan acceso a bloques y objetos.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Acerca de esta tarea

Puede crear una o varias claves de acceso de S3 para otros usuarios, de modo que puedan crear y gestionar bloques para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con el nuevo ID de clave de acceso y la clave de acceso secreta. Por seguridad, no cree más claves de las que necesita el usuario y elimine las claves que no se están utilizando. Si sólo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la antigua y, a continuación, elimine la anterior.

Cada clave puede tener un tiempo de caducidad específico o no puede caducar. Siga estas directrices para el tiempo de caducidad:

- Establezca un tiempo de caducidad para que las claves limiten el acceso del usuario a un determinado período de tiempo. Establecer un tiempo de caducidad corto puede ayudar a reducir el riesgo si el ID de clave de acceso y la clave de acceso secreta se exponen accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo de seguridad de su entorno es bajo y no es necesario crear periódicamente claves nuevas, no es necesario establecer un tiempo de caducidad de las claves. Si decide más tarde crear claves nuevas, elimine manualmente las claves antiguas.

Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Seleccione el usuario cuyas claves de acceso de S3 desee gestionar.

   Aparece la página de detalles del usuario.

3. Seleccione **teclas de acceso** y, a continuación, seleccione **tecla de creación**.
4. Debe realizar una de las siguientes acciones:
   - Selecciona **No establecer un tiempo de caducidad** para crear una clave que no caduque. (Predeterminado)
   - Seleccione **establecer un tiempo de caducidad** y establezca la fecha y la hora de caducidad.

     La fecha de caducidad puede ser un máximo de cinco años a partir de la fecha actual. El tiempo de caducidad puede ser un mínimo de un minuto desde la hora actual.

5. Seleccione **Crear clave de acceso**.

   Se muestra el cuadro de diálogo Descargar clave de acceso, en el que se enumeran el ID de clave de acceso y la clave de acceso secreta.

6. 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 clave de acceso y la clave de acceso secreta.

   No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No puede copiar ni descargar claves después de cerrar el cuadro de diálogo.

7. Seleccione **Finalizar**.

   La nueva clave aparece en la ficha teclas de acceso de la página de detalles del usuario.

8. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, utilice opcionalmente la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la cuadrícula de origen al inquilino en la cuadrícula de destino. Consulte "Clone las claves de acceso S3 mediante la API".

Ver las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene los permisos adecuados, puede ver las claves de acceso S3 de otro usuario. Puede ordenar la lista por tiempo de caducidad para que pueda determinar qué claves caducarán pronto. Según sea necesario, puede crear nuevas claves y eliminar claves que ya no estén en uso.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. En la página Usuarios, seleccione el usuario cuyas S3 claves de acceso desea ver.
3. En la página Detalles del usuario, selecciona **Teclas de acceso**.
4. Ordene las teclas por **tiempo de caducidad** o **ID de clave de acceso**.
5. Según sea necesario, cree nuevas claves y elimine manualmente las que ya no estén en uso.

   Si crea claves nuevas antes de que caduquen las claves existentes, el usuario podrá empezar a utilizar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

   Las claves caducadas se eliminan automáticamente.

Información relacionada

"Cree las claves de acceso S3 de otro usuario"

"Elimine las claves de acceso S3 de otro usuario"

Elimine las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene los permisos adecuados, puede eliminar las claves de acceso S3 de otro usuario. Cuando se elimina una clave de acceso, ya no se puede utilizar para acceder a los objetos y los bloques de la cuenta de inquilino.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. En la página Usuarios, seleccione el usuario cuyas S3 claves de acceso desea administrar.
3. En la página Detalles del usuario, selecciona **Teclas de acceso** y, a continuación, selecciona la casilla de verificación para cada clave de acceso desea eliminar.
4. Seleccione **acciones** > **Borrar clave seleccionada**.
5. En el cuadro de diálogo de confirmación, seleccione **Tecla Eliminar**.

Aparecerá un mensaje de confirmación en la esquina superior derecha de la página.

Gestión de bloques S3

Cree un bloque de S3

Puede usar el administrador de inquilinos para crear bloques S3 para los datos de objetos.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene acceso raíz o Gestionar todos los bloques "permiso". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

> Los permisos para establecer o modificar las propiedades de Object Lock de grupos o objetos de S3 pueden ser concedidos por "política de bloques o política de grupo".

- Si tiene previsto habilitar el bloqueo de objetos de S3 para un depósito, un administrador de grid ha habilitado la configuración global de bloqueo de objetos de S3 para el sistema StorageGRID y ha revisado los requisitos para los bloques y objetos de bloqueo de objetos de S3. Consulte "Utilice Bloqueo de objetos S3 para retener objetos".

Acceda al asistente

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione **Crear cucharón**.

Introduzca los detalles

Pasos

1. Introduzca los detalles del cucharón.

Campo	Descripción
Nombre del bloque	Un nombre para el depósito que cumple con estas reglas: • Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino). • Debe ser compatible con DNS. • Debe incluir al menos 3 y no más de 63 caracteres. • Cada etiqueta debe comenzar y terminar con una letra minúscula o un número y solo puede utilizar letras minúsculas, números y guiones. • No debe utilizar periodos en solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor. Para obtener más información, consulte "Documentación de Amazon Web Services (AWS) sobre reglas de nomenclatura de bloques". **Nota**: No puedes cambiar el nombre del cubo después de crear el cubo.
Región	La región del cubo. El administrador de StorageGRID gestiona las regiones disponibles. La región de un bloque puede afectar la política de protección de datos aplicada a los objetos. De forma predeterminada, todos los bloques se crean en la `us-east-1` región. **Nota**: No puedes cambiar la región después de crear el cubo.

2. Seleccione **continuar**.

Gestionar la configuración del objeto

Pasos

1. Opcionalmente, habilite el control de versiones del objeto para el bloque.

   Habilite el control de versiones de objetos si desea almacenar cada versión de cada objeto en este bloque. A continuación, puede recuperar versiones anteriores de un objeto según sea necesario. Debe habilitar el control de versiones de objetos si el bloque se va a utilizar para la replicación entre grid.

2. Si la opción Bloqueo de objetos S3 global está habilitada, habilite opcionalmente Bloqueo de objetos S3 para que el depósito almacene objetos utilizando un modelo WORM.

   Habilite el bloqueo de objetos S3 para un depósito solo si necesita mantener objetos durante un tiempo fijo, por ejemplo, para cumplir con ciertos requisitos normativos. S3 Object Lock es una configuración permanente que le ayuda a evitar que los objetos se eliminen o sobrescriban durante un período de tiempo fijo o indefinidamente.

   > Una vez que se habilita la configuración Bloqueo de objetos S3 para un depósito, no se puede desactivar. Cualquier persona con los permisos correctos puede agregar objetos a este depósito que no se pueden cambiar. Es posible que no pueda eliminar estos objetos o el cubo en sí.

Si habilita S3 Object Lock para un bloque, el control de versiones de bloques se habilita automáticamente.

3. Si seleccionó **Habilitar bloqueo de objetos S3**, opcionalmente habilite **Retención predeterminada** para este depósito.

   Cuando se habilita **Retención predeterminada**, los nuevos objetos agregados al depósito se protegerán automáticamente de ser eliminados o sobrescritos. La configuración **default retention** no se aplica a los objetos que tienen sus propios periodos de retención.

   a. Si **Retención predeterminada** está habilitada, especifique un **Modo de retención predeterminado** para el depósito.

Modo de retención predeterminado	Descripción
Cumplimiento de normativas	• El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta. • La fecha de retención del objeto se puede aumentar, pero no se puede reducir. • No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.
Gobernanza	• Usuarios con `s3:BypassGovernanceRetention` el permiso puede utilizar el `x-amz-bypass-governance-retention: true` solicitar cabecera para omitir la configuración de retención. • Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

   b. Si **Retención predeterminada** está habilitada, especifique el **Período de retención predeterminado** para el depósito.

      El **período de retención predeterminado** indica cuánto tiempo deben conservarse los nuevos objetos agregados a este depósito, a partir del momento en que se ingieren. Especifique un valor entre 1 y 36.500 días o entre 1 y 100 años, ambos incluidos.

4. Seleccione **Crear cucharón**.

   El cucharón se crea y se agrega a la tabla de la página Cuches.

5. Opcionalmente, selecciona **Ir a la página de detalles del cubo** a. "ver detalles del período" y realizar la configuración adicional.

Ver detalles del período

Puede ver los depósitos en su cuenta de inquilino.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".

- Pertenece a un grupo de usuarios que tiene el "Acceso raíz, Gestionar todos los bloques o Ver todos los bloques". Estos permisos anulan la configuración de permisos en las políticas de grupo o bloque.

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.

   Aparecerá la página Buckets.

2. Revise la información de resumen de cada bloque.

   Según sea necesario, puede ordenar la información por cualquier columna o puede avanzar y retroceder por la lista.

   > Los valores de recuento de objetos y espacio utilizado que se muestran son estimaciones. Estas estimaciones se ven afectadas por el tiempo de los ingests, la conectividad de red y el estado del nodo. Si los bloques tienen habilitado el control de versiones, las versiones de objetos eliminados se incluyen en el recuento de objetos.

Columna	Descripción
Nombre	El nombre único del depósito, que no se puede cambiar.
Funciones activadas	Lista de funciones activadas para el depósito.
Bloqueo de objetos de S3	Si el bloqueo de objetos S3 está activado para el depósito. Esta columna sólo aparece si Bloqueo de objetos S3 está activado para la cuadrícula. Esta columna también muestra información para todos los segmentos compatibles anteriores.
Región	La región del cubo, que no se puede cambiar.
Recuento de objetos	Núm. De objetos en este depósito. Cuando se agregan o se eliminan objetos, es posible que este valor no se actualice de inmediato. Si los cubos tienen el control de versiones activado, se incluyen versiones de objetos no actuales en este valor.
Espacio utilizado	El tamaño lógico de todos los objetos del bloque. El tamaño lógico no incluye el espacio real necesario para las copias replicadas o con código de borrado o para los metadatos de objetos.
Fecha de creación	La fecha y la hora en la que se creó el bloque.

3. Para ver los detalles de un cubo específico, seleccione el nombre del cubo en la tabla.

   Aparece la página de detalles bucket. En esta página, puede realizar las siguientes tareas si tiene los permisos necesarios:

   - Configure y gestione las opciones de bloque:
     - "Etiquetas de políticas de ILM"

        - "Gestione la coherencia de los bloques"
        - "Últimas actualizaciones de hora de acceso"
        - "Control de versiones de objetos"
        - "Bloqueo de objetos de S3"
        - "Retención de cucharón por defecto"
    - Configurar el acceso al bloque, por ejemplo "Uso compartido de recursos de origen cruzado (CORS)"
    - "Gestione los servicios de la plataforma" (Si se permite para el inquilino), incluida la replicación de CloudMirror, las notificaciones de eventos y la integración de búsqueda
    - Habilite y. "gestionar la replicación entre grid" (Si se permite para el inquilino) replicar los objetos ingeridos en este bucket en otro sistema StorageGRID
    - Acceda a "S3 Consola" para gestionar los objetos del depósito
    - "Eliminar todos los objetos de un depósito"
    - "Eliminar un cubo" eso ya está vacío

Aplique una etiqueta de política de ILM a un bloque

Elija una etiqueta de política de ILM para aplicarla a un bloque en función de sus requisitos de almacenamiento de objetos.

La política de ILM controla dónde se almacenan los datos de objetos y si se eliminan después de un cierto período de tiempo. Su administrador de grid crea políticas de ILM y las asigna a las etiquetas de políticas de ILM cuando usa varias políticas activas.

> Evite reasignar con frecuencia la etiqueta de política de un bucket. De lo contrario, pueden producirse problemas de rendimiento.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Acceso raíz, Gestionar todos los bloques o Ver todos los bloques". Estos permisos anulan la configuración de permisos en las políticas de grupo o bloque.

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.

   Aparecerá la página Buckets. Según sea necesario, puede ordenar la información por cualquier columna o puede avanzar y retroceder por la lista.

2. Seleccione el nombre del bloque al que desea asignar una etiqueta de política de ILM.

   También puede cambiar la asignación de etiquetas de política de ILM de un bloque que ya tenga una etiqueta asignada.

   > Los valores de recuento de objetos y espacio utilizado que se muestran son estimaciones. Estas estimaciones se ven afectadas por el tiempo de los ingests, la conectividad de red y el estado del nodo. Si los bloques tienen habilitado el control de versiones, las versiones de objetos eliminados se incluyen en el recuento de objetos.

3. En la pestaña Bucket options, expanda el acordeón de etiqueta de política de ILM. Este acordeón solo aparece si el administrador de grid ha habilitado el uso de etiquetas de política personalizadas.
4. Lea la descripción de cada etiqueta de política para determinar qué etiqueta se debe aplicar al depósito.

> Si se cambia la etiqueta de política de ILM de un bloque, se activará la reevaluación de ILM de todos los objetos del bloque. Si la nueva política conserva los objetos durante un tiempo limitado, los objetos más antiguos se eliminarán.

5. Seleccione el botón de radio de la etiqueta que desea asignar al depósito.
6. Seleccione **Guardar cambios**. Se establecerá una nueva etiqueta de cubo S3 en el cucharón con la llave `NTAP-SG-ILM-BUCKET-TAG` Y el valor del nombre de etiqueta de la política de ILM.

> Asegúrese de que las aplicaciones S3 no anulen ni eliminen accidentalmente la nueva etiqueta de depósito. Si se omite esta etiqueta al aplicar un TagSet nuevo al bloque, los objetos del bloque se volverán a evaluar según la política de ILM predeterminada.

> Establezca y modifique las etiquetas de políticas de ILM mediante solo la API del administrador de inquilinos o del administrador de inquilinos donde se valida la etiqueta de política de ILM. No modifique el `NTAP-SG-ILM-BUCKET-TAG` Etiqueta de política de gestión de la vida útil de la información mediante la API de PutBucketTagging de S3 o la API de DeleteBucketTagging de S3.

> El cambio de la etiqueta de política asignada a un bloque tiene un impacto temporal en el rendimiento mientras los objetos se reevalúan con la nueva política de ILM.

Gestione la coherencia de los bloques

Los valores de coherencia se pueden utilizar para especificar la disponibilidad de cambios de configuración de bloques, así como para proporcionar un equilibrio entre la disponibilidad de los objetos dentro de un bloque y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios. Puede cambiar los valores de coherencia para que sean diferentes de los valores predeterminados para que las aplicaciones cliente puedan satisfacer sus necesidades operativas.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Directrices de coherencia de bloques

La coherencia de bloques se utiliza para determinar la coherencia de las aplicaciones cliente que afectan a los objetos dentro de ese bloque S3. En general, debe utilizar la consistencia **Read-after-new-write** para sus cubos.

Cambie la consistencia del bloque

Si la consistencia de **Read-after-new-write** no cumple con los requisitos de la aplicación cliente, puede

cambiar la consistencia configurando la consistencia del depósito o utilizando el `Consistency-Control` encabezado. La `Consistency-Control` el cabezal anula la consistencia del cucharón.

> Cuando se cambia la consistencia de un depósito, sólo se garantiza que los objetos que se ingieren después del cambio cumplan con la configuración revisada.

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

3. En la pestaña **Opciones de cucharón**, selecciona el acordeón **.
4. Seleccione una coherencia para las operaciones realizadas en los objetos de este bloque.
   - **Todo**: Proporciona el más alto nivel de consistencia. Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.
   - **Strong-global**: Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes en todos los sitios.
   - **Strong-site**: Garantiza la consistencia de lectura después de escritura para todas las solicitudes de los clientes dentro de un sitio.
   - **Read-after-new-write** (por defecto): Proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
   - **Disponible**: Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.
5. Seleccione **Guardar cambios**.

Qué sucede cuando se cambia la configuración del bloque

Los cubos tienen varios ajustes que afectan al comportamiento de los cubos y los objetos dentro de esos cubos.

Los siguientes ajustes de cucharón utilizan la consistencia **strong** de forma predeterminada. Si no hay dos o más nodos de almacenamiento disponibles en ningún sitio, o si no hay un sitio disponible, es posible que no esté disponible ningún cambio en estos ajustes.

- "Eliminación de bloque vacío en segundo plano"
- "Hora del último acceso"
- "Ciclo de vida del cucharón"
- "Política de bloques"
- "Etiquetado de cucharones"
- "Control de versiones del cucharón"
- "Bloqueo de objetos de S3"
- "Cifrado de bloques"

El valor de coherencia para el control de versiones de bloque, el bloqueo de objetos de S3 y el cifrado de bloque no se puede establecer en un valor que no es muy consistente.

Los siguientes ajustes de cucharón no utilizan una gran consistencia y tienen una mayor disponibilidad para los cambios. Los cambios en estos ajustes pueden tardar algún tiempo antes de tener un efecto.

- "Configuración de servicios de plataforma: Notificación, replicación o integración de búsqueda"
- "Configuración de CORS"
- Cambie la consistencia del cucharón

Si la coherencia predeterminada que se utiliza al cambiar la configuración del bloque no cumple con los requisitos de la aplicación cliente, puede cambiar la coherencia mediante el `Consistency-Control` encabezado del "API REST DE S3" o mediante el `reducedConsistency` o. `force` de la "API de gestión de inquilinos".

Activar o desactivar las actualizaciones de la hora del último acceso

Cuando los administradores de grid crean las reglas de gestión del ciclo de vida de la información (ILM) para un sistema StorageGRID, puede especificar si desea mover ese objeto a una ubicación de almacenamiento diferente. Si usa un inquilino de S3, puede aprovechar esas reglas al habilitar actualizaciones en la última hora de acceso para los objetos de un bloque de S3.

Estas instrucciones solo se aplican a los sistemas StorageGRID que incluyen al menos una regla de ILM que utiliza la opción **last access time** como filtro avanzado o como tiempo de referencia. Puede ignorar estas instrucciones si el sistema StorageGRID no incluye dicha regla. Consulte "Utilice la última hora de acceso en las reglas de ILM" para obtener más detalles.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

El tiempo de último acceso es una de las opciones disponibles para la instrucción de colocación de **Tiempo de referencia** para una regla de ILM. Establecer el tiempo de referencia para una regla como el tiempo de último acceso permite a los administradores de grid especificar que los objetos se coloquen en determinadas ubicaciones de almacenamiento según la fecha en que se recuperaron por última vez esos objetos (se leyeron o vieron).

Por ejemplo, para asegurarse de que los objetos que se ven recientemente permanecen en un almacenamiento más rápido, el administrador de grid puede crear una regla de ILM que especifique lo siguiente:

- Los objetos que se han recuperado durante el último mes deben permanecer en los nodos de almacenamiento local.
- Los objetos que no se han recuperado en el último mes deben moverse a una ubicación externa.

De forma predeterminada, las actualizaciones de la hora del último acceso están desactivadas. Si su sistema StorageGRID incluye una regla de ILM que utiliza la opción **last access time** y desea que esta opción se

aplique a los objetos de este depósito, debe habilitar las actualizaciones a la última hora de acceso para los S3 buckets especificados en esa regla.

> La actualización del último tiempo de acceso cuando se recupera un objeto puede reducir el rendimiento de la StorageGRID, especialmente en objetos pequeños.

El impacto en el rendimiento se produce con las actualizaciones del último tiempo de acceso porque StorageGRID debe realizar estos pasos adicionales cada vez que se recuperan los objetos:

- Actualice los objetos con nuevas marcas de tiempo
- Añada los objetos a la cola de ILM para poder reevaluarlos según las reglas y políticas actuales de ILM

La tabla resume el comportamiento aplicado a todos los objetos del bloque cuando la hora de último acceso está desactivada o habilitada.

Tipo de solicitud	Comportamiento si la hora del último acceso está desactivada (valor predeterminado)		Comportamiento si la hora del último acceso está activada	
	¿Hora de último acceso actualizada?	¿Objeto añadido a la cola de evaluación de ILM?	¿Hora de último acceso actualizada?	¿Objeto añadido a la cola de evaluación de ILM?
Solicitud para recuperar un objeto, su lista de control de acceso o sus metadatos	No	No	Sí	Sí
Solicitud para actualizar los metadatos de un objeto	Sí	Sí	Sí	Sí
Solicite copiar un objeto de un bloque a otro	• No, para la copia de origen • Sí, para la copia de destino	• No, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

3. En la pestaña **Opciones de cubo**, selecciona el acordeón **Últimas actualizaciones de hora de acceso**.
4. Activar o desactivar las actualizaciones de hora del último acceso.
5. Seleccione **Guardar cambios**.

Cambiar el control de versiones del objeto para un bloque

Si utiliza un inquilino S3, puede cambiar el estado de control de versiones de los bloques S3.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.
- Todos los nodos de almacenamiento están disponibles.

Acerca de esta tarea

Puede habilitar o suspender el control de versiones de objetos de un bloque. Después de activar el control de versiones para un depósito, no puede volver a un estado sin versiones. Sin embargo, puede suspender el control de versiones del bloque.

- Desactivado: El control de versiones no se ha activado nunca
- Activado: El control de versiones está activado
- Suspendido: El control de versiones se ha habilitado anteriormente y se ha suspendido

Para obtener más información, consulte lo siguiente:

- "Control de versiones de objetos"
- "Reglas de ILM y políticas para objetos con versiones de S3 (ejemplo 4)"
- "Cómo se eliminan los objetos"

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

3. Desde la pestaña **Opciones de cubo**, selecciona el acordeón **Control de versiones de objeto**.
4. Seleccione un estado de control de versiones para los objetos de este bloque.

   El control de versiones de objetos debe permanecer habilitado para un bucket que se utiliza para la replicación entre grid. Si se habilita el bloqueo de objetos S3 o la compatibilidad con versiones heredadas, se desactivarán las opciones **versiones de objetos**.

Opción	Descripción
Habilite el control de versiones	Habilite el control de versiones de objetos si desea almacenar cada versión de cada objeto en este bloque. A continuación, puede recuperar versiones anteriores de un objeto según sea necesario. Los objetos que ya estaban en el bloque se versionarán cuando los modifique un usuario.
Suspender las versiones	Suspenda el control de versiones de objetos si ya no desea crear nuevas versiones de objetos. Aún puede recuperar cualquier versión de objeto existente.

5. Seleccione **Guardar cambios**.

Utilice Bloqueo de objetos S3 para retener objetos

Puede utilizar S3 Object Lock si los cubos y los objetos deben cumplir con los requisitos normativos de retención.

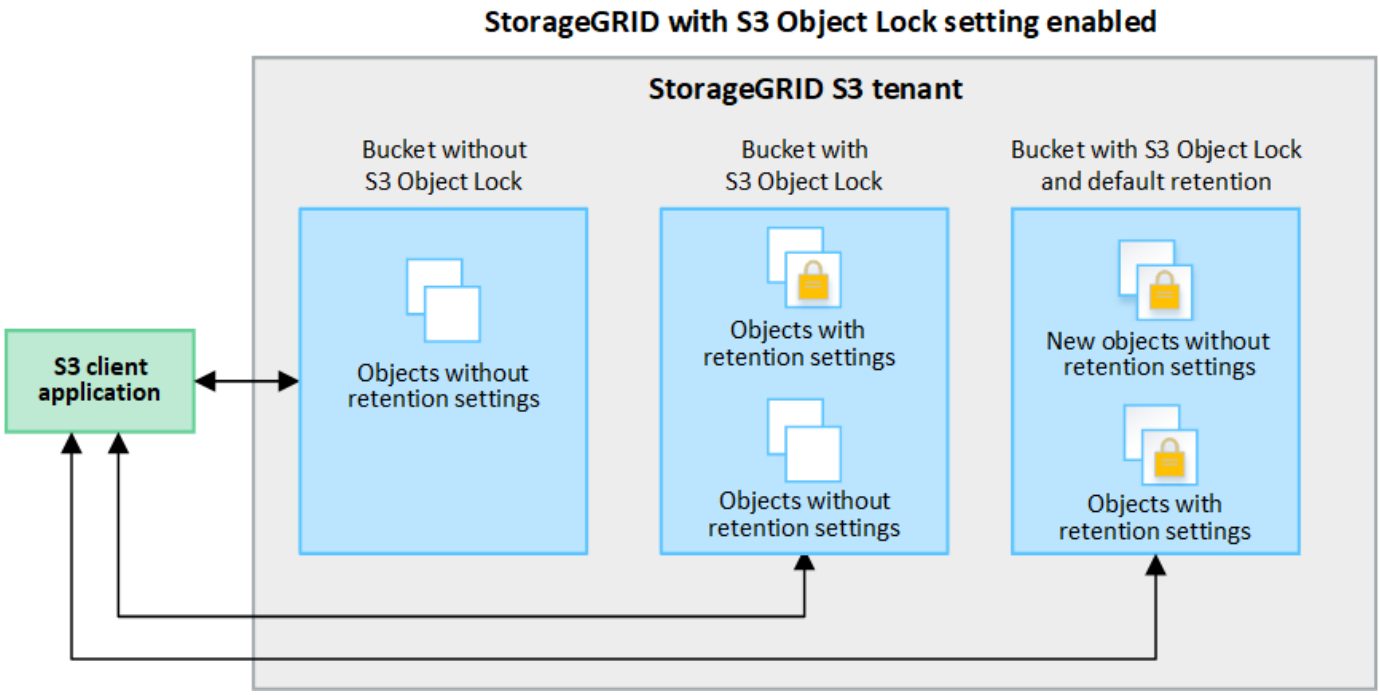
¿Qué es el bloqueo de objetos de S3?

La función StorageGRID S3 Object Lock es una solución de protección de objetos equivalente a S3 Object Lock en Amazon simple Storage Service (Amazon S3).

Tal y como se muestra en la figura, cuando se habilita la opción global de bloqueo de objetos de S3 para un sistema StorageGRID, una cuenta de inquilino de S3 puede crear bloques con o sin la función de bloqueo de objetos de S3 habilitada. Si un bucket tiene S3 Object Lock habilitado, se requiere el control de versiones de bucket y se habilita automáticamente.

Si un bucket tiene S3 Object Lock habilitado, las aplicaciones cliente S3 pueden especificar, de manera opcional, la configuración de retención para cualquier versión de objeto guardada en ese bucket.

Además, un bloque que tiene S3 Object Lock habilitado puede tener opcionalmente un modo de retención y un período de retención predeterminados. La configuración predeterminada se aplica solo a los objetos que se agregan al depósito sin su propia configuración de retención.



Modos de retención

La función de bloqueo de objetos 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 retención hasta.
  - La fecha de retención del objeto se puede aumentar, pero no se puede reducir.
  - No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.
- En modo de gobierno:
  - Los usuarios con permiso especial pueden utilizar un encabezado de omisión en las solicitudes para modificar ciertos valores de retención.
  - Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha.
  - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Configuración de retención para versiones de objetos

Si se crea un depósito con S3 Object Lock habilitado, los usuarios pueden utilizar la aplicación cliente S3 para especificar opcionalmente los siguientes valores de retención para cada objeto que se agregue al depósito:

- **Modo de retención**: Ya sea cumplimiento o gobierno.
- **Retain-until-date**: Si la fecha de retención de una versión de objeto está en el futuro, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal**: La aplicación de una retención legal a una versión de objeto bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesite poner una retención legal en un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, pero permanece en su lugar hasta que se elimina explícitamente. La retención legal es independiente de la retención hasta la fecha.

Si un objeto se encuentra bajo una conservación legal, nadie puede eliminarlo, independientemente de su modo de retención.

Para obtener más información sobre la configuración del objeto, consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".

Valor de retención predeterminado para los depósitos

Si se crea un depósito con S3 Object Lock habilitado, los usuarios pueden especificar opcionalmente los siguientes ajustes predeterminados para el bloque:

- **Modo de retención predeterminado**: Ya sea cumplimiento o gobierno.
- **Período de retención predeterminado**: Cuánto tiempo deben conservarse las nuevas versiones de objetos añadidas a este depósito, a partir del día en que se agregan.

La configuración de bloque predeterminada se aplica solo a objetos nuevos que no tienen su propia configuración de retención. Los objetos de cubo existentes no se ven afectados al agregar o cambiar estos valores predeterminados.

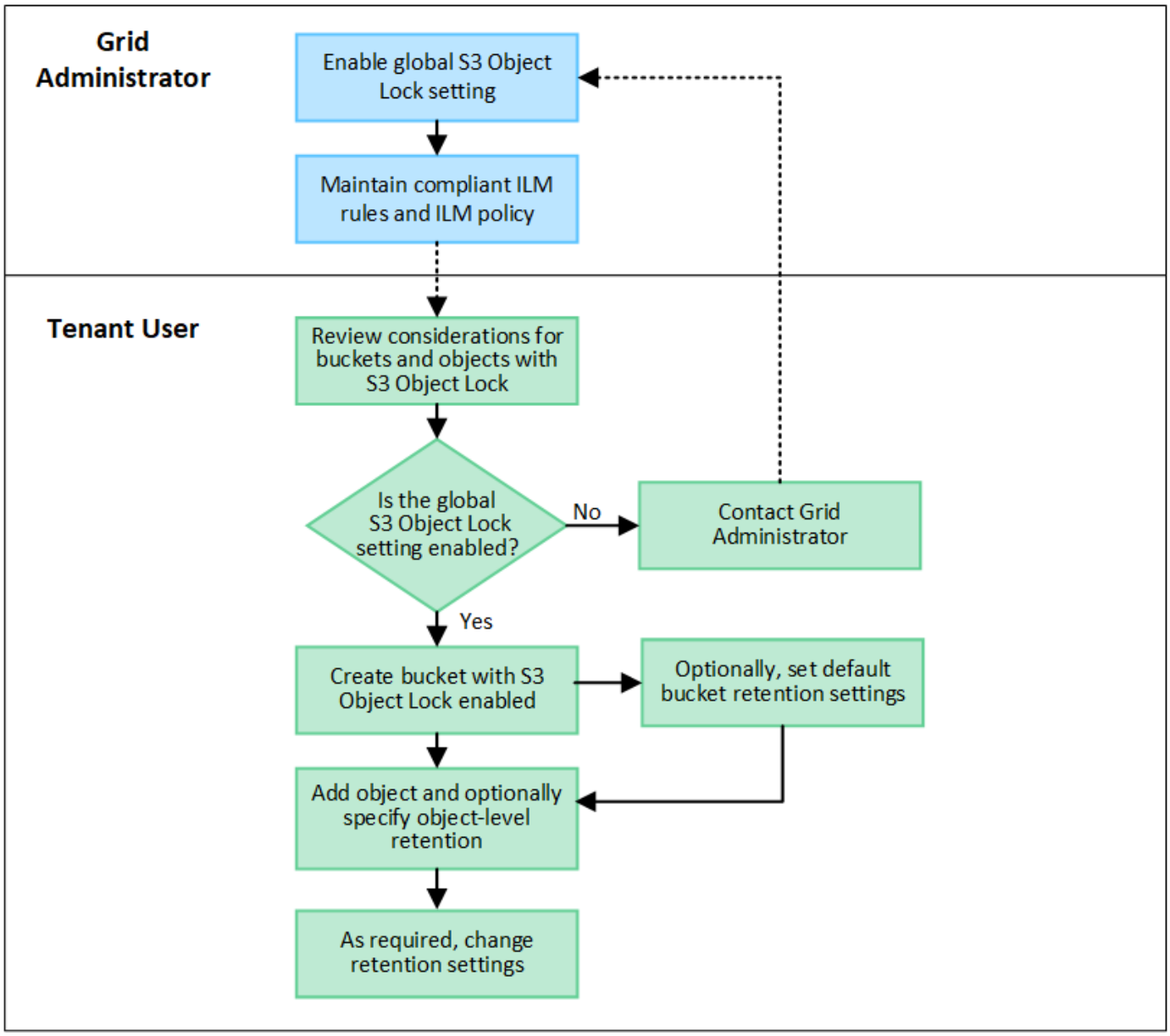
Consulte "Cree un bloque de S3" y.. "Actualizar S3 Retención predeterminada de bloqueo de objetos".

Flujo de trabajo de bloqueo de objetos de S3

En el diagrama de flujo de trabajo, se muestran los pasos de alto nivel para usar la función de bloqueo de objetos de S3 en StorageGRID.

Para poder crear bloques con el bloqueo de objetos S3 habilitado, el administrador de grid debe habilitar el valor global de bloqueo de objetos S3 para todo el sistema StorageGRID. El administrador de grid también debe asegurarse de que la política de gestión del ciclo de vida de la información (ILM) sea conforme; debe cumplir los requisitos de los buckets con bloqueo de objetos S3 habilitado. Para obtener más información, póngase en contacto con el administrador de grid o consulte las instrucciones para "Gestionar objetos con S3 Object Lock".

Después de habilitar la configuración global S3 Object Lock, puede crear buckets con S3 Object Lock habilitado y, opcionalmente, especificar la configuración de retención predeterminada para cada bucket. Además, puede utilizar la aplicación cliente S3 para especificar opcionalmente la configuración de retención para cada versión de objeto.



Requisitos para bloques con bloqueo de objetos de S3 habilitado

- Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, puede usar el administrador de inquilinos, la API de gestión de inquilinos o la API REST de S3 para crear bloques con el bloqueo de objetos S3 habilitado.
- Si planea utilizar el bloqueo de objetos S3, debe habilitar el bloqueo de objetos S3 al crear el bloque. No puede activar el bloqueo de objetos S3 para un depósito existente.
- Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque. No puede desactivar el bloqueo de objetos de S3 ni suspender el control de versiones del depósito.
- De manera opcional, puede especificar un modo de retención y un período de retención predeterminados para cada bloque mediante el administrador de inquilinos, la API de gestión de inquilinos o la API DE REST S3. La configuración de retención predeterminada del depósito se aplica solo a los nuevos objetos agregados al depósito que no tienen su propia configuración de retención. Puede anular esta configuración predeterminada especificando un modo de retención y Retain-until-date para cada versión del objeto cuando se cargue.

- Se admite la configuración de ciclo de vida de bloques para los bloques con S3 Object Lock habilitado.
- La replicación de CloudMirror no es compatible para bloques con el bloqueo de objetos S3 habilitado.

Requisitos para objetos en bloques con S3 Object Lock habilitado

- Para proteger una versión de objeto, puede especificar la configuración de retención predeterminada para el bloque, o bien puede especificar la configuración de retención para cada versión de objeto. La configuración de retención a nivel de objeto se puede especificar mediante la aplicación cliente S3 o la API DE REST S3.
- La configuración de retención se aplica a versiones individuales de objetos. Una versión de objeto puede tener una configuración de retención hasta fecha y una retención legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta fecha o de retención legal para un objeto, sólo se protege la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras que la versión anterior del objeto permanece bloqueada.

Ciclo de vida de los objetos en bloques con S3 Object Lock habilitado

Cada objeto que se guarda en un depósito con S3 Object Lock habilitado pasa por las siguientes etapas:

1. **Procesamiento de objetos**

   Cuando se agrega una versión de objeto al depósito que tiene S3 Object Lock habilitado, la configuración de retención se aplica de la siguiente manera:

   - Si se especifica la configuración de retención para el objeto, se aplica la configuración de nivel de objeto. Se ignoran todos los valores predeterminados de los depósitos.
   - Si no se especifica ninguna configuración de retención para el objeto, se aplica la configuración de bloque predeterminada, si existe.
   - Si no se especifica ninguna configuración de retención para el objeto o el depósito, el objeto no está protegido por S3 Object Lock.

   Si se aplica una configuración de retención, tanto el objeto como cualquier metadatos definidos por el usuario S3 se protegen.

2. **Retención y eliminación de objetos**

   StorageGRID almacena varias copias de cada objeto protegido durante el período de retención especificado. El número y el tipo exactos de copias de objetos y las ubicaciones de almacenamiento están determinados por las reglas conformes a la normativa de las políticas de ILM activas. Si se puede eliminar un objeto protegido antes de alcanzar su fecha de retención hasta la fecha, depende de su modo de retención.

   - Si un objeto se encuentra bajo una conservación legal, nadie puede eliminarlo, independientemente de su modo de retención.

¿Puedo seguir gestionando los depósitos compatibles heredados?

La función de bloqueo de objetos S3 sustituye la función Compliance disponible en versiones anteriores de StorageGRID. Si ha creado cubos compatibles con una versión anterior de StorageGRID, puede seguir gestionando la configuración de estos bloques; sin embargo, ya no puede crear nuevos bloques compatibles. Para ver instrucciones, consulte "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5".

Actualizar S3 Retención predeterminada de bloqueo de objetos

Si habilitó S3 Object Lock al crear el bucket, puede editar el bucket para cambiar la configuración de retención predeterminada. Puede habilitar (o deshabilitar) la retención predeterminada y establecer un modo de retención y un período de retención predeterminados.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.
- S3 Bloqueo de objetos está habilitado globalmente para su sistema StorageGRID, y usted habilitó S3 Bloqueo de objetos al crear el bucket. Consulte "Utilice Bloqueo de objetos S3 para retener objetos".

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

3. En la pestaña **Opciones de cubo**, selecciona el acordeón **S3 Object Lock**.
4. Opcionalmente, habilita o deshabilita **Retención predeterminada** para este depósito.

   Los cambios realizados en esta configuración no se aplican a objetos que ya estén en el depósito ni a objetos que puedan tener sus propios períodos de retención.

5. Si **Retención predeterminada** está habilitada, especifique un **Modo de retención predeterminado** para el depósito.

Modo de retención predeterminado	Descripción
Cumplimiento de normativas	• El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta. • La fecha de retención del objeto se puede aumentar, pero no se puede reducir. • No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.
Gobernanza	• Usuarios con `s3:BypassGovernanceRetention` el permiso puede utilizar el `x-amz-bypass-governance-retention: true` solicitar cabecera para omitir la configuración de retención. • Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

6. Si **Retención predeterminada** está habilitada, especifique el **Período de retención predeterminado**

para el depósito.

El **período de retención predeterminado** indica cuánto tiempo deben conservarse los nuevos objetos agregados a este depósito, a partir del momento en que se ingieren. Especifique un valor entre 1 y 36.500 días o entre 1 y 100 años, ambos incluidos.

7. Seleccione **Guardar cambios**.

Configurar el uso compartido de recursos de origen cruzado (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un depósito de S3 si desea que las aplicaciones web de otros dominios puedan acceder a ese depósito y a los objetos de ese depósito.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

El uso compartido de recursos de origen cruzado (CORS) es un mecanismo de seguridad que permite a las aplicaciones web de cliente de un dominio acceder a los recursos de un dominio diferente. Por ejemplo, supongamos que se utiliza un bloque de S3 llamado `Images` para almacenar gráficos. Configurando CORS para `Images` bloque, puede permitir que las imágenes de ese bloque se muestren en el sitio web `http://www.example.com`.

Activar CORS para un cucharón

Pasos

1. Utilice un editor de texto para crear el XML necesario.

   Este ejemplo muestra el XML utilizado para habilitar CORS para un bloque de S3. Este XML permite a cualquier dominio enviar solicitudes GET al bloque, pero sólo permite el `http://www.example.com` Dominio para enviar solicitudes DE PUBLICACIÓN Y ELIMINACIÓN. Se permiten todos los encabezados de las solicitudes.

```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

Para obtener más información acerca del XML de configuración de CORS, consulte "Documentación de Amazon Web Services (AWS): Guía para desarrolladores de Amazon simple Storage Service".

2. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
3. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

4. En la pestaña **Acceso a cubos**, selecciona el acordeón **Uso compartido de recursos de origen cruzado (CORS)**.
5. Seleccione la casilla de verificación **Activar CORS**.
6. Pegue el XML de configuración de CORS en el cuadro de texto.
7. Seleccione **Guardar cambios**.

Modificar el ajuste de CORS

Pasos

1. Actualice el XML de configuración de CORS en el cuadro de texto, o seleccione **Borrar** para empezar de nuevo.
2. Seleccione **Guardar cambios**.

Desactive el ajuste CORS

Pasos

1. Desactive la casilla de verificación **Activar CORS**.
2. Seleccione **Guardar cambios**.

Suprimir objetos del depósito

Puede utilizar el gestor de inquilinos para suprimir los objetos de uno o más depósitos.

Consideraciones y requisitos

Antes de realizar estos pasos, tenga en cuenta lo siguiente:

- Cuando elimina los objetos de un depósito, StorageGRID elimina de forma permanente todos los objetos y todas las versiones de objetos de cada bloque seleccionado de todos los nodos y sitios del sistema StorageGRID. StorageGRID también quita todos los metadatos de objetos relacionados. No podrá recuperar esta información.
- La eliminación de todos los objetos de un bloque puede demorar minutos, días o incluso semanas, según el número de objetos, copias de objetos y operaciones simultáneas.
- Si un cucharón tiene "S3 Bloqueo de objetos activado", Puede permanecer en el estado **Deleting objects: Read-only** para *Years*.

> Un depósito que utiliza S3 Object Lock permanecerá en el estado **Deleting objects: Read-only** hasta que se alcance la fecha de retención para todos los objetos y se eliminen las retenciones legales.

- Mientras los objetos se eliminan, el estado del depósito es **Eliminando objetos: Solo lectura**. En este estado, no puede agregar nuevos objetos al depósito.
- Cuando todos los objetos se han eliminado, el bloque permanece en su estado de solo lectura. Puede realizar una de las siguientes acciones:
  - Vuelva a colocar el depósito en modo de escritura y reutilícelo para objetos nuevos
  - Elimine el cucharón
  - Mantenga el bucket en modo de solo lectura para reservar su nombre para uso futuro
- Si un bloque tiene el control de versiones de objetos activado, los marcadores de eliminación que se crearon en StorageGRID 11,8 o posterior se pueden eliminar mediante la eliminación de objetos en las operaciones de bloque.
- Si un bloque tiene el control de versiones de objetos activado, la operación de supresión de objetos no eliminará los marcadores de supresión creados en StorageGRID 11,7 o anteriores. Consulte la información sobre la eliminación de objetos en un depósito en "Cómo se eliminan los objetos con versiones de S3".
- Si utiliza "replicación entre grid", tenga en cuenta lo siguiente:
  - El uso de esta opción no elimina ningún objeto del depósito en la otra cuadrícula.
  - Si selecciona esta opción para el depósito de origen, se activará la alerta **Fallo de replicación entre redes** si agrega objetos al depósito de destino en la otra cuadrícula. Si no puede garantizar que nadie agregará objetos al depósito de la otra cuadrícula, "desactive la replicación entre grid" para ese depósito antes de eliminar todos los objetos de cubo.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz". Este permiso anula la configuración de permisos en las políticas de grupo o bloque.

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.

   Aparece la página Buckets y muestra todos los bloques S3 existentes.

2. Utilice el menú **Acciones** o la página de detalles de un cubo específico.

Menú Actions

a. Seleccione la casilla de comprobación de cada bloque desde el que desea eliminar objetos.

b. Selecciona **Acciones** > **Eliminar objetos en el cubo**.

Detalles

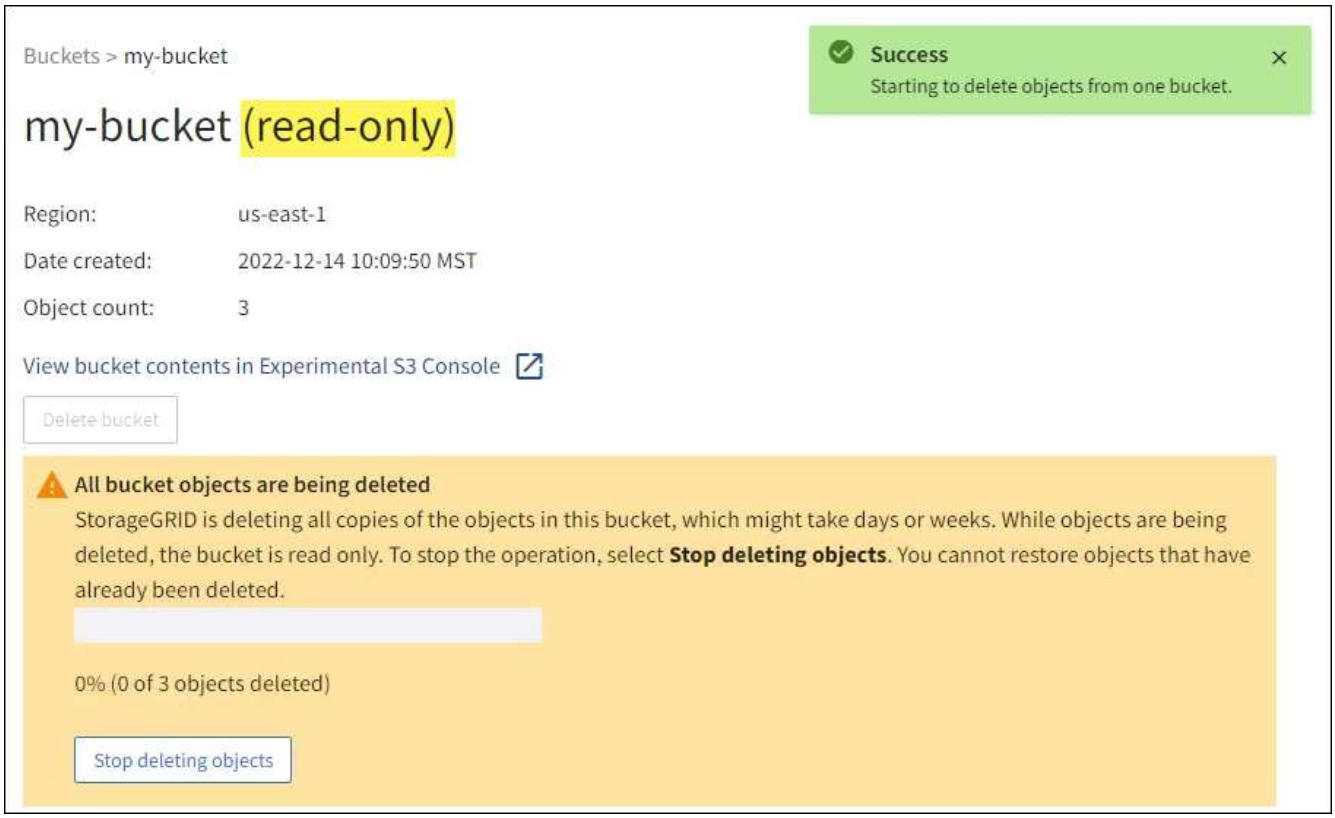
a. Seleccione un nombre de cubo para mostrar sus detalles.

b. Seleccione **Eliminar objetos en el cubo**.

3. Cuando aparezca el cuadro de diálogo de confirmación, revise los detalles, introduzca **Sí** y seleccione **Aceptar**.
4. Espere a que comience la operación de eliminación.

   Después de unos minutos:

   - Aparece un banner de estado amarillo en la página de detalles del depósito. La barra de progreso representa el porcentaje de objetos que se han suprimido.
   - **(solo lectura)** aparece después del nombre del cubo en la página de detalles del cubo.
   - **(Eliminación de objetos: Solo lectura)** aparece junto al nombre del cubo en la página Buckets.

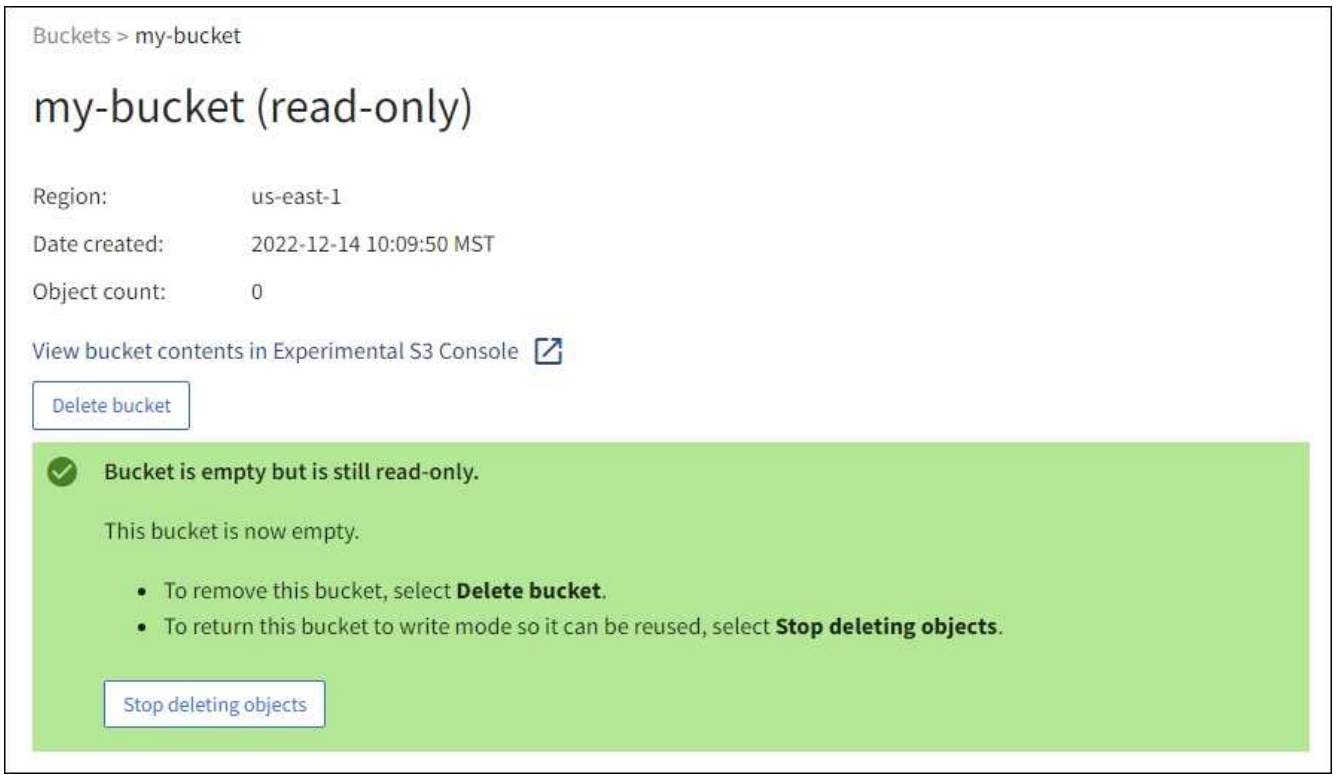


5. Según sea necesario mientras se ejecuta la operación, seleccione **Detener eliminación de objetos** para detener el proceso. Luego, opcionalmente, seleccione **Eliminar objetos en el cubo** para reanudar el proceso.

   Cuando selecciona **Dejar de eliminar objetos**, el depósito vuelve al modo de escritura; sin embargo, no puede acceder ni restaurar ningún objeto que se haya eliminado.

6. Espere a que se complete la operación.

   Cuando el depósito está vacío, se actualiza el banner de estado, pero el depósito permanece como de sólo lectura.



7. Debe realizar una de las siguientes acciones:
   - Salga de la página para mantener el depósito en modo de sólo lectura. Por ejemplo, puede mantener un depósito vacío en modo de solo lectura para reservar el nombre del depósito para uso futuro.
   - Eliminar el bloque. Puede seleccionar **Eliminar cubo** para eliminar un solo cubo o devolver la página Buckets y seleccionar **Acciones** > **Eliminar** cubos para eliminar más de un cubo.

     Si no puede suprimir un depósito con versiones después de eliminar todos los objetos, puede que permanezcan los marcadores de supresión. Para eliminar el cucharón, debe eliminar todos los marcadores de borrado restantes.

   - Vuelva a colocar el depósito en modo de escritura y, opcionalmente, reutilícelo para objetos nuevos. Puede seleccionar **Dejar de eliminar objetos** para un solo depósito o volver a la página Buckets y seleccionar **Acción** > **Dejar de eliminar objetos** para más de un depósito.

Eliminar bloque de S3

Puede usar el administrador de inquilinos para eliminar uno o varios bloques de S3 vacíos.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

- Los cucharones que desea eliminar están vacíos. Si los depósitos que desea suprimir están *NOT* vacíos, "suprimir objetos del depósito".

Acerca de esta tarea

Estas instrucciones describen cómo eliminar un bloque de S3 mediante el administrador de inquilinos. También se pueden eliminar bloques de S3 con el "API de gestión de inquilinos" o la "API REST DE S3".

No se puede eliminar un bucket de S3 si contiene objetos, versiones de objetos no actuales o marcadores de eliminación. Para obtener más información sobre cómo se eliminan los objetos con versiones S3, consulte "Cómo se eliminan los objetos".

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.

   Aparece la página Buckets y muestra todos los bloques S3 existentes.

2. Utilice el menú **Acciones** o la página de detalles de un cubo específico.

   Menú Actions

   a. Seleccione la casilla de verificación de cada bloque que desee eliminar.

   b. Selecciona **Acciones** > **Eliminar cubos**.

   Detalles

   a. Seleccione un nombre de cubo para mostrar sus detalles.

   b. Seleccione **Eliminar cubo**.

3. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí**.

   StorageGRID confirma que cada cucharón está vacío y, a continuación, elimina cada cucharón. Esta operación puede llevar algunos minutos.

   Si un segmento no está vacío, aparece un mensaje de error. Debe "elimine todos los objetos y cualquier marcador de borrado del depósito" antes de poder eliminar el depósito.

Utilice la consola S3

Puede utilizar S3 Console para ver y gestionar los objetos de un bucket de S3.

La consola S3 le permite:

- Cargar, descargar, renombrar, copiar, mover, y eliminar objetos
- Vea, revierta, descargue y elimine versiones de objetos
- Buscar objetos por prefijo
- Administrar etiquetas de objetos
- Ver los metadatos de objetos
- Ver, crear, cambiar nombre, copiar, mover, y elimine carpetas

S3 Console proporciona una experiencia de usuario mejorada para los casos más comunes. No está diseñado para sustituir las operaciones de la CLI o la API en todas las situaciones.

Si el uso de S3 Console provoca operaciones que tardan demasiado (por ejemplo, minutos u horas), considere:

- Reducción del número de objetos seleccionados
- Uso de métodos no gráficos (API o CLI) para acceder a los datos

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Si desea gestionar objetos, pertenece a un grupo de usuarios que tiene el permiso de acceso root. Como alternativa, pertenece a un grupo de usuarios que tiene el permiso Usar la pestaña Consola de S3 y el permiso Ver todos los cubos o Gestionar todos los cubos. Consulte "Permisos de gestión de inquilinos".
- Se ha configurado una política de grupo o bloque S3 para el usuario. Consulte "Utilice las políticas de acceso de bloques y grupos".
- Conoce el ID de clave de acceso del usuario y la clave de acceso secreta. Opcionalmente, usted tiene un `.csv` archivo que contiene esta información. Consulte "instrucciones para crear claves de acceso".

Pasos

1. Seleccione **STORAGE** > **Buckets** > ***bucket name***.
2. Seleccione la ficha Consola de S3.
3. Pegue el ID de clave de acceso y la clave de acceso secreta en los campos. De lo contrario, seleccione **cargar teclas de acceso** y seleccione el `.csv` archivo.
4. Seleccione **Iniciar sesión**.
5. Aparece la tabla de objetos de cubo. Puede gestionar objetos según sea necesario.

Información adicional

- **Buscar por prefijo**: La función de búsqueda de prefijo solo busca objetos que comiencen con una palabra específica relativa a la carpeta actual. La búsqueda no incluye objetos que contengan la palabra en otro lugar. Esta regla también se aplica a los objetos dentro de las carpetas. Por ejemplo, una búsqueda de `folder1/folder2/somefile-` devolvería objetos que se encuentran dentro de `folder1/folder2/` y empezar con la palabra `somefile-`.
- * Arrastre y suelte *: Puede arrastrar y soltar archivos desde el administrador de archivos de su computadora a S3 Console. Sin embargo, no puede cargar carpetas.
- **Operaciones en carpetas**: Cuando se mueve, copia o cambia el nombre de una carpeta, todos los objetos de la carpeta se actualizan de uno en uno, lo que puede llevar tiempo.
- **Eliminación permanente cuando el control de versiones del bucket está desactivado**: Cuando sobrescribe o elimina un objeto en un bucket con el control de versiones desactivado, la operación es permanente. Consulte "Cambiar el control de versiones del objeto para un bloque".

Gestione servicios de plataformas S3

Administrar servicios de plataforma: Descripción general

Los servicios de plataforma de StorageGRID pueden ayudarte a implementar una

estrategia de cloud híbrido permitiéndote enviar notificaciones de eventos y copias de objetos S3 y metadatos de objetos a destinos externos.

Si se permite el uso de servicios de plataforma para su cuenta de inquilino, puede configurar los siguientes servicios para cualquier bloque de S3:

Replicación de CloudMirror

Uso "Servicio de replicación CloudMirror de StorageGRID" Para reflejar objetos específicos de un bloque de StorageGRID en un destino externo especificado.

Por ejemplo, podría usar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y, a continuación, aprovechar los servicios de AWS para realizar análisis de los datos.

> La replicación de CloudMirror no es compatible si el bloque de origen tiene la función S3 Object Lock habilitada.

Notificaciones

Uso "notificaciones de eventos por bloque" Para enviar notificaciones sobre acciones específicas realizadas en objetos a un Amazon Simple Notification Service (Amazon SNS) externo especificado.

Por ejemplo, podría configurar que se envíen alertas a administradores acerca de cada objeto agregado a un bloque, donde los objetos representan los archivos de registro asociados a un evento crítico del sistema.

> Aunque la notificación de eventos se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluido el estado retener hasta fecha y retención legal) de los objetos no se incluirán en los mensajes de notificación.

Servicio de integración de búsqueda

Utilice la "servicio de integración de búsqueda" Para enviar metadatos de objetos S3 a un índice de Elasticsearch especificado donde se pueden buscar o analizar los metadatos mediante un servicio externo.

Por ejemplo, podría configurar sus bloques para que envíen metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, podría usar Elasticsearch para realizar búsquedas en los bloques y ejecutar análisis sofisticados de los patrones presentes en los metadatos de objetos.

> Aunque la integración de Elasticsearch se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos de S3 (incluidos los Estados Retain Until Date and Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

Puesto que la ubicación objetivo de los servicios de la plataforma suele ser externa a la puesta en marcha de StorageGRID, los servicios de plataforma le proporcionan la potencia y la flexibilidad que se obtiene al utilizar recursos de almacenamiento externo, servicios de notificación y servicios de búsqueda o análisis para sus datos.

Se puede configurar cualquier combinación de servicios de plataforma para un único bloque de S3. Por ejemplo, podría configurar el servicio CloudMirror y las notificaciones en un bloque de StorageGRID S3 de manera que pueda reflejar objetos específicos en Amazon simple Storage Service, al tiempo que envía una notificación sobre cada objeto de ese tipo a una aplicación de supervisión de terceros para ayudarle a realizar un seguimiento de los gastos de AWS.

Un administrador de StorageGRID debe habilitar el uso de servicios de plataforma para cada cuenta de inquilino mediante el Administrador de grid o la API de gestión de grid.

Cómo se configuran los servicios de plataforma

Los servicios de plataforma se comunican con los puntos finales externos que configure mediante "Administrador de inquilinos" o la "API de gestión de inquilinos". Cada extremo representa un destino externo, como un bloque de S3 de StorageGRID, un bloque de Amazon Web Services, un tema de Amazon SNS o un clúster de Elasticsearch alojado localmente, en AWS o en otro lugar.

Después de crear un punto final externo, puede activar un servicio de plataforma para un bloque agregando configuración XML al bloque. La configuración XML identifica los objetos en los que debe actuar el bloque, la acción que debe tomar el bloque y el extremo que el bloque debe utilizar para el servicio.

Debe agregar configuraciones XML independientes para cada servicio de plataforma que desee configurar. Por ejemplo:

- Si desea que todos los objetos con las claves comiencen `/images` Para replicarse en un bloque de Amazon S3, debe añadir una configuración de replicación al bloque de origen.
- Si también desea enviar notificaciones cuando estos objetos están almacenados en el bloque, debe añadir una configuración de notificaciones.
- Por último, si desea indexar los metadatos de estos objetos, debe agregar la configuración de notificación de metadatos que se utiliza para implementar la integración de búsquedas.

El formato de la configuración XML está regido por las API DE REST de S3 que se usan para implementar los servicios de plataforma StorageGRID:

Servicio de plataforma	API REST DE S3	Consulte
Replicación de CloudMirror	• GetBucketReplication • PutBucketReplication	• "Replicación de CloudMirror" • "Operaciones en bloques"
Notificaciones	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Notificaciones" • "Operaciones en bloques"
Integración de búsqueda	• OBTENGA la configuración de notificación de metadatos del bloque de datos • Configuración de notificaciones de metadatos de PUT Bucket	• "Integración de búsqueda" • "Operaciones personalizadas de StorageGRID"

Información relacionada

"Consideraciones sobre los servicios de plataforma"

Servicio de replicación de CloudMirror

Puede habilitar la replicación de CloudMirror para un bloque de S3 si desea que StorageGRID replique los objetos especificados que se añadan al bloque en uno o más bloques de destino.

La replicación de CloudMirror funciona independientemente de las políticas de gestión de la vida útil de la información activas del grid. El servicio CloudMirror replica los objetos cuando se almacenan en el bloque de origen y los envía al Lo antes posible. de bloque de destino. La entrega de objetos replicados se activa cuando la ingesta de objetos se realiza correctamente.

> La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre grid. Para obtener más información, consulte "Compare la replicación entre grid y la replicación de CloudMirror".

Si habilita la replicación de CloudMirror para un bloque existente, solo se replican los nuevos objetos agregados a ese bloque. Todos los objetos existentes del bloque no se replican. Para forzar la replicación de objetos existentes, puede actualizar los metadatos del objeto existente ejecutando una copia de objeto.

> Si utiliza la replicación de CloudMirror para copiar objetos a un destino de Amazon S3, tenga en cuenta que Amazon S3 limita el tamaño de los metadatos definidos por el usuario dentro de cada encabezado de solicitud PUT a 2 KB. Si un objeto tiene metadatos definidos por el usuario mayores de 2 KB, ese objeto no se replicará.

En StorageGRID, puede replicar los objetos de un solo bloque en varios bloques de destino. Para ello, especifique el destino de cada regla en el XML de configuración de replicación. No puede replicar un objeto en más de un bloque a la vez.

Además, puede configurar la replicación de CloudMirror en bloques con versiones o sin versiones, y puede especificar un bloque con versiones o sin versiones como destino. Puede utilizar cualquier combinación de cubos con versiones y sin versiones. Por ejemplo, puede especificar un bloque con versiones como destino para un bloque de origen sin versiones o viceversa. También puede replicar entre cubos sin versiones.

El comportamiento de eliminación del servicio de replicación CloudMirror es el mismo que el comportamiento de eliminación del servicio de replicación entre regiones (CRR) proporcionado por Amazon S3 — al eliminar un objeto de un bloque de origen nunca se elimina un objeto replicado en el destino. Si se van a crear versiones de los cubos de origen y de destino, se replica el marcador de borrado. Si el bloque de destino no tiene versiones, al eliminar un objeto del bloque de origen no se replicará el marcador DELETE en el bloque de destino ni se eliminará el objeto de destino.

A medida que los objetos se replican en el bloque de destino, StorageGRID los marca como «réplicas». Un bucket de StorageGRID de destino no replicará objetos marcados como réplicas de nuevo, lo que le protegerá de bucles de replicación accidentales. Este marcado de réplica es interno en StorageGRID y no le impide utilizar AWS CRR cuando se utiliza un bloque de Amazon S3 como destino.

> El encabezado personalizado utilizado para marcar una réplica es `x-ntap-sg-replica`. Esta Marca evita una duplicación en cascada. StorageGRID sí admite un CloudMirror bidireccional entre dos grids.

La singularidad y el orden de los eventos en el cubo de destino no están garantizados. Puede que más de una copia idéntica de un objeto de origen se proporcione en el destino como resultado de las operaciones realizadas para garantizar un éxito en la entrega. En raras ocasiones, cuando se actualiza el mismo objeto de forma simultánea desde dos o más sitios StorageGRID distintos, es posible que la ordenación de las

operaciones en el bloque de destino no coincida con la ordenación de eventos en el bloque de origen.

La replicación de CloudMirror suele configurarse para utilizar un bloque de S3 externo como destino. Sin embargo, también puede configurar la replicación para que utilice otra implementación de StorageGRID o cualquier servicio compatible con S3.

Comprender las notificaciones para bloques

Puede habilitar la notificación de eventos para un bucket de S3 si desea que StorageGRID envíe notificaciones sobre eventos especificados a un clúster Kafka de destino o a Amazon Simple Notification Service.

Puede hacerlo "configure las notificaciones de eventos" Asociando XML de configuración de notificación a un bloque de origen. El XML de configuración de notificaciones sigue las convenciones de S3 para configurar notificaciones de buckets, con el tema Kafka o Amazon SNS de destino especificado como URN de un punto final.

Las notificaciones de eventos se crean en el bloque de origen tal y como se especifica en la configuración de notificación y se envían al destino. Si un evento asociado con un objeto se realiza correctamente, se crea una notificación sobre ese evento y se pone en cola para su entrega.

La singularidad y el orden de las notificaciones no están garantizados. Como resultado de las operaciones realizadas para garantizar el éxito en la entrega, se podría enviar más de una notificación de un evento al destino. Además, como la entrega es asíncrona, no se garantiza que la ordenación del tiempo de las notificaciones en el destino coincida con la ordenación de eventos del bloque de origen, especialmente en las operaciones que se originan en diferentes sitios de StorageGRID. Puede utilizar el `sequencer` Introduzca el mensaje de evento para determinar el orden de los eventos de un objeto determinado, como se describe en la documentación de Amazon S3.

Notificaciones y mensajes compatibles

Las notificaciones de eventos de StorageGRID siguen la API de Amazon S3 con algunas limitaciones:

- Se admiten los siguientes tipos de evento:
  - S3:ObjetoCreado:*
  - S3:ObjectCreated:Put
  - S3:ObjectCreated:Post
  - S3:ObjectCreated:Copiar
  - S3:ObjectCreated:CompleteMultipartUpload
  - S3:ObjectRemoved:*
  - S3:ObjectRemoved:Eliminar
  - S3:ObjectRemoved:DeleteMarkerCreated
  - S3:ObjectRestore:Post
- Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar, pero no incluyen algunas claves ni utilizan valores específicos para otros, como se muestra en la tabla:

Nombre de clave	Valor de StorageGRID
EventSource	`sgws:s3`
AwsRegion	no incluido
x-amz-id-2	no incluido
arn	`urn:sgws:s3:::bucket_name`

Comprender el servicio de integración de búsquedas

Puede habilitar la integración de búsqueda para un bloque de S3 si desea usar un servicio de búsqueda y análisis de datos externo para sus metadatos de objetos.

El servicio de integración de búsqueda es un servicio StorageGRID personalizado que envía de forma automática y asíncrona los metadatos de objetos de S3 a un extremo de destino cada vez que se actualiza un objeto o sus metadatos. A continuación, puede usar herramientas sofisticadas de búsqueda, análisis de datos, visualización o aprendizaje automático que proporciona el servicio de destino para buscar, analizar y obtener información de sus datos de objetos.

Puede activar el servicio de integración de búsqueda para cualquier bloque con versiones o sin versiones. La integración de búsqueda se configura asociando el XML de configuración de notificación de metadatos al bloque que especifica los objetos en los que actuar y el destino de los metadatos del objeto.

Las notificaciones se generan en forma de un documento JSON denominado con el nombre del bloque, el nombre del objeto y el ID de versión, si los hubiera. Cada notificación de metadatos contiene un conjunto estándar de metadatos del sistema para el objeto, además de todas las etiquetas del objeto y los metadatos del usuario.

> Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para interpretar estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para la asignación dinámica de campos y para asignar formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Después de indexar un documento, no puede editar los tipos de campo del documento en el índice.

Las notificaciones se generan y se ponen en cola para su entrega siempre que:

- Se crea un objeto.
- Se elimina un objeto, incluso cuando se eliminan objetos como resultado del funcionamiento de la política de ILM de la cuadrícula.
- Los metadatos o las etiquetas de los objetos son añadidos, actualizados o eliminados. El conjunto completo de metadatos y etiquetas se envía siempre al momento de la actualización, no sólo los valores modificados.

Después de agregar XML de configuración de notificación de metadatos a un bloque, se envían notificaciones para los objetos nuevos que cree y para los objetos que modifique mediante la actualización de sus datos, metadatos de usuario o etiquetas. Sin embargo, no se envían notificaciones de ningún objeto que ya estuviera

en el bloque. Para garantizar que los metadatos de objeto de todos los objetos del bloque se envíen al destino, debe realizar una de las siguientes acciones:

- Configure el servicio de integración de búsqueda inmediatamente después de crear el bloque y antes de agregar ningún objeto.
- Realice una acción en todos los objetos que ya están en el bloque que activará un mensaje de notificación de metadatos que se enviará al destino.

El servicio de integración de búsqueda StorageGRID admite un clúster de Elasticsearch como destino. Al igual que con los demás servicios de plataforma, el destino se especifica en el extremo cuyo URN se utiliza en el XML de configuración del servicio. Utilice la "Herramienta de matriz de interoperabilidad de NetApp" Para determinar las versiones compatibles de Elasticsearch.

Información relacionada

"XML de configuración para la integración de búsqueda"

"Metadatos de objetos incluidos en las notificaciones de metadatos"

"JSON generado por el servicio de integración de búsqueda"

"Configure el servicio de integración de búsqueda"

Consideraciones sobre los servicios de plataforma

Antes de implementar los servicios de la plataforma, revise las recomendaciones y consideraciones sobre el uso de estos servicios.

Para obtener más información sobre S3, consulte "USE LA API DE REST DE S3".

Consideraciones sobre el uso de servicios de plataforma

Consideración	Detalles
Supervisión del extremo de destino	Debe supervisar la disponibilidad de cada extremo de destino. Si se pierde la conectividad con el extremo de destino durante un periodo de tiempo prolongado y existe una gran acumulación de solicitudes, se producirá un error en las solicitudes de cliente adicionales (como solicitudes PUT) a StorageGRID. Debe volver a intentar estas solicitudes con errores cuando se pueda acceder al extremo.

Consideración	Detalles
Limitación de punto final de destino	El software StorageGRID puede reducir las solicitudes entrantes de S3 para un bloque si la velocidad a la que se envían las solicitudes supera la velocidad a la que el extremo de destino puede recibir las solicitudes. La limitación sólo se produce cuando hay una acumulación de solicitudes que están a la espera de ser enviadas al extremo de destino. El único efecto visible es que las solicitudes entrantes de S3 tardarán más en ejecutarse. Si empieza a detectar un rendimiento significativamente más lento, debe reducir la tasa de procesamiento o utilizar un extremo con mayor capacidad. Si la acumulación de solicitudes sigue creciendo, las operaciones de S3 del cliente (como SOLICITUDES PUT) fallarán en el futuro. Las solicitudes de CloudMirror tienen más probabilidades de que se vean afectadas por el rendimiento del extremo de destino, ya que estas solicitudes suelen requerir más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.
Solicitud de garantías	StorageGRID garantiza la realización de pedidos de operaciones en un objeto dentro de un sitio. Siempre que todas las operaciones contra un objeto se encuentren en el mismo sitio, el estado del objeto final (para replicación) será siempre igual al estado en StorageGRID. StorageGRID hace todo un esfuerzo por intentar solicitar solicitudes cuando se realizan operaciones en todos los sitios de StorageGRID. Por ejemplo, si escribe un objeto inicialmente en el sitio A y después sobrescribe el mismo objeto en el sitio B, no se garantiza que el objeto final replicado por CloudMirror en el bloque de destino sea el más nuevo.
Eliminaciones de objetos condicionados por ILM	Para coincidir con el comportamiento de eliminación de AWS CRR y Amazon Simple Notification Service, CloudMirror y las solicitudes de notificación de eventos no se envían cuando se elimina un objeto del bloque de origen debido a las reglas de gestión de la vida útil de la información de StorageGRID. Por ejemplo, no se envían solicitudes de notificaciones de eventos o CloudMirror si una regla de ILM elimina un objeto después de 14 días. Por el contrario, las solicitudes de integración de búsqueda se envían cuando los objetos se eliminan debido a ILM.

Consideración	Detalles
Utilizando puntos finales Kafka	Para puntos finales Kafka, TLS mutuo no es compatible. Como resultado, si tiene `ssl.client.auth` establezca en `required` En su configuración de Kafka broker, puede causar problemas de configuración de punto final de Kafka. La autenticación de los puntos finales de Kafka utiliza los siguientes tipos de autenticación. Estos tipos son diferentes de los utilizados para la autenticación de otros puntos finales, como Amazon SNS, y requieren credenciales de nombre de usuario y contraseña. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Nota:** Los ajustes de proxy de almacenamiento configurados no se aplican a los endpoints de servicios de la plataforma Kafka.

Consideraciones sobre el uso del servicio de replicación de CloudMirror

Consideración	Detalles
Estado de replicación	StorageGRID no admite el `x-amz-replication-status` encabezado.
Tamaño del objeto	El tamaño máximo de los objetos que se pueden replicar en un bloque de destino mediante el servicio de replicación de CloudMirror es de 5 TIB, que es el mismo que el tamaño máximo de objeto *admitido*. **Nota**: El tamaño máximo *Recommended* para una sola operación PutObject es de 5 GiB (5.368.709.120 bytes). Si tiene objetos que sean mayores de 5 GIB, utilice la carga de varias partes en su lugar.
Versiones de bloques e ID de versión	Si el bloque de S3 de origen de StorageGRID tiene habilitado el control de versiones, también debe habilitar el control de versiones para el bloque de destino. Al usar el control de versiones, tenga en cuenta que el orden de las versiones de objetos en el bloque de destino es el mejor esfuerzo y no está garantizado por el servicio CloudMirror, debido a las limitaciones del protocolo S3. **Nota**: Los ID de versión para el depósito de origen en StorageGRID no están relacionados con los ID de versión para el depósito de destino.

Consideración	Detalles
Etiquetado para versiones de objetos	El servicio CloudMirror no replica ninguna solicitud PutObjectTagging o DeleteObjectTagging que proporcione un ID de versión, debido a las limitaciones del protocolo S3. Debido a que los ID de versión para el origen y el destino no están relacionados, no hay forma de garantizar que se replique una actualización de etiqueta para un ID de versión específico. Por el contrario, el servicio CloudMirror replica las solicitudes PutObjectTagging o las solicitudes DeleteObjectTagging que no especifican un ID de versión. Estas solicitudes actualizan las etiquetas de la clave más reciente (o la versión más reciente si el bloque está versionado). También se replican búsquedas normales con etiquetas (no actualizaciones de etiquetado).
Cargas en varias partes y. `ETag` valores	Cuando se crea un mirroring de objetos cargados con una carga de varias partes, el servicio CloudMirror no conserva las piezas. Como resultado, el `ETag` el valor del objeto reflejado será diferente al `ETag` valor del objeto original.
Objetos cifrados con SSE-C (cifrado en el lado del servidor con claves proporcionadas por el cliente)	El servicio CloudMirror no admite objetos cifrados con SSE-C. Si intenta procesar un objeto en el bloque de origen para la replicación de CloudMirror y la solicitud incluye los encabezados de solicitud de SSE-C, se produce un error en la operación.
Bloque con S3 Object Lock habilitado	Si el bucket S3 de destino para la replicación de CloudMirror tiene S3 Object Lock habilitado, el intento de configurar la replicación de bucket (PutBucketReplication) fallará con un error ACCESSDENIED.

Configure los extremos de servicios de la plataforma

Para poder configurar un servicio de plataforma para un bloque, debe configurar al menos un extremo para que sea el destino del servicio de plataforma.

El acceso a servicios de la plataforma está habilitado por inquilino por un administrador de StorageGRID. Para crear o utilizar un punto final de servicios de plataforma, debe ser un usuario inquilino con permiso de gestión de puntos finales o acceso raíz, en una cuadrícula cuya red se ha configurado para permitir que los nodos de almacenamiento accedan a recursos de punto final externo. Para un solo inquilino, puede configurar un máximo de 500 puntos finales de servicios de plataforma. Si desea obtener más información, póngase en contacto con el administrador de StorageGRID.

¿Qué es un extremo de servicios de plataforma?

Al crear un extremo de servicios de plataforma, se especifica la información que StorageGRID necesita para acceder al destino externo.

Por ejemplo, si desea replicar objetos de un bucket de StorageGRID en un bucket de Amazon S3, cree un punto final de servicios de plataforma que incluya la información y las credenciales que necesita StorageGRID para acceder al bucket de destino en Amazon.

Cada tipo de servicio de plataforma requiere su propio extremo, por lo que debe configurar al menos un extremo para cada servicio de plataforma que tenga previsto utilizar. Después de definir un extremo de servicios de plataforma, se utiliza URN del extremo como destino en el XML de configuración utilizado para

habilitar el servicio.

Puede utilizar el mismo extremo que el destino para más de un bloque de origen. Por ejemplo, se pueden configurar varios bloques de origen para que envíen metadatos de objetos al mismo extremo de integración de búsqueda, de modo que se puedan realizar búsquedas en varios bloques. También puede configurar un depósito de origen para que utilice más de un extremo como destino, lo que permite hacer cosas como enviar notificaciones sobre la creación de objetos a un tema de Amazon Simple Notification Service (Amazon SNS) y notificaciones sobre la eliminación de objetos a un segundo tema de Amazon SNS.

Extremos para la replicación de CloudMirror

StorageGRID admite extremos de replicación que representan bloques de S3. Estos bloques se pueden alojar en Amazon Web Services, la misma puesta en marcha de StorageGRID remota o en otro servicio.

Extremos para notificaciones

StorageGRID es compatible con los extremos Amazon SNS y Kafka. No se admiten el servicio de cola simple (SQS) ni los extremos de AWS Lambda.

Para puntos finales Kafka, TLS mutuo no es compatible. Como resultado, si tiene `ssl.client.auth` establezca en `required` En su configuración de Kafka broker, puede causar problemas de configuración de punto final de Kafka.

Extremos del servicio de integración de búsqueda

StorageGRID admite extremos de integración de búsqueda que representan clústeres de Elasticsearch. Estos clústeres de Elasticsearch pueden estar en un centro de datos local o alojados en un cloud de AWS o en otro lugar.

El extremo de integración de búsqueda hace referencia a un índice y un tipo específicos de Elasticsearch. Debe crear el índice en Elasticsearch antes de crear el extremo en StorageGRID o se producirá un error en la creación del extremo. No es necesario crear el tipo antes de crear el punto final. StorageGRID creará el tipo si es necesario al enviar metadatos de objetos al extremo.

Información relacionada

"Administre StorageGRID"

Especifique URN para el extremo de servicios de la plataforma

Al crear un extremo de servicios de plataforma, debe especificar un nombre de recurso único (URN). Utilizará el URN para hacer referencia al punto final cuando cree un XML de configuración para el servicio de plataforma. El URN de cada extremo debe ser único.

StorageGRID valida los extremos de los servicios de la plataforma a medida que se crean. Antes de crear un extremo de servicios de plataforma, confirme que el recurso especificado en el extremo existe y que se puede alcanzar.

URN elementos

El URN de un extremo de servicios de plataforma debe comenzar con cualquiera de los dos `arn:aws` o. `urn:mysite`, como se indica a continuación:

- Si el servicio está alojado en Amazon Web Services (AWS), utilice `arn:aws`

- Si el servicio está alojado en Google Cloud Platform (GCP), utilice `arn:aws`
- Si el servicio se aloja localmente, utilice `urn:mysite`

Por ejemplo, si especifica el URN para un extremo de CloudMirror alojado en StorageGRID, el URN podría comenzar con `urn:sgws`.

El siguiente elemento de URN especifica el tipo de servicio de plataforma, como se indica a continuación:

Servicio	Tipo
Replicación de CloudMirror	`s3`
Notificaciones	`sns` o. `kafka`
Integración de búsqueda	`es`

Por ejemplo, para seguir especificando URN para un extremo de CloudMirror alojado en StorageGRID, debería añadir `s3` para conseguirlo `urn:sgws:s3`.

El elemento final del URN identifica el recurso de destino específico en el URI de destino.

Servicio	Recurso específico
Replicación de CloudMirror	`bucket-name`
Notificaciones	`sns-topic-name` o. `kafka-topic-name`
Integración de búsqueda	`domain-name/index-name/type-name` **Nota:** Si el clúster Elasticsearch está **no** configurado para crear índices automáticamente, debe crear el índice manualmente antes de crear el punto final.

Urnas para servicios alojados en AWS y GCP

Para las entidades AWS y GCP, el URN completo es un AWS ARN válido. Por ejemplo:

- Replicación de CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notificaciones:

```
arn:aws:sns:region:account-id:topic-name
```

- Integración de búsqueda:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

Para un extremo de integración de búsqueda de AWS, la `domain-name` debe incluir la cadena literal `domain/`, como se muestra aquí.

Servicios alojados localmente

Al usar servicios alojados localmente en lugar de servicios de cloud, puede especificar el URN de cualquier forma que cree una URN válida y única, siempre y cuando URN incluya los elementos necesarios en la tercera y última posición. Puede dejar los elementos indicados por opcional en blanco o puede especificarlos de cualquier forma que le ayude a identificar el recurso y hacer que el URN sea único. Por ejemplo:

- Replicación de CloudMirror:

  ```
  urn:mysite:s3:optional:optional:bucket-name
  ```

  En el caso de un extremo de CloudMirror alojado en StorageGRID, es posible especificar una URN válida que comience por `urn:sgws`:

  ```
  urn:sgws:s3:optional:optional:bucket-name
  ```

- Notificaciones:

  Especifique un punto final de Amazon Simple Notification Service:

  ```
  urn:mysite:sns:optional:optional:sns-topic-name
  ```

  Especifique un punto final Kafka:

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-name
  ```

- Integración de búsqueda:

  ```
  urn:mysite:es:optional:optional:domain-name/index-name/type-name
  ```

  Para los extremos de integración de búsqueda alojados localmente, el `domain-name` Element puede ser cualquier cadena siempre que el URN del extremo sea único.

Cree un extremo de servicios de plataforma

Debe crear al menos un extremo del tipo correcto para poder habilitar un servicio de

plataforma.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".
- Se ha creado el recurso al que hace referencia el punto final de servicios de plataforma:
  - Replicación de CloudMirror: Bloque de S3
  - Notificación de eventos: Tema de Amazon Simple Notification Service (Amazon SNS) o Kafka
  - Notificación de búsqueda: Índice de Elasticsearch, si el clúster de destino no está configurado para crear índices automáticamente.
- Tiene la información sobre el recurso de destino:
  - Host y puerto para el Identificador uniforme de recursos (URI)

    Si piensa utilizar un bloque alojado en un sistema StorageGRID como extremo para la replicación de CloudMirror, póngase en contacto con el administrador de grid para determinar los valores que debe introducir.

  - Nombre del recurso único (URN)

    "Especifique URN para el extremo de servicios de la plataforma"

  - Credenciales de autenticación (si es necesario):

Extremos de integración de búsquedas de AWS

Para los extremos de integración de búsqueda de AWS, puede usar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave de acceso secreta
- Basic HTTP: Nombre de usuario y contraseña
- CAP (C2S Access Portal): URL de credenciales temporales, certificados de servidor y de cliente, claves de cliente y una contraseña de clave privada de cliente opcional.

Replicación de CloudMirror y extremos de Amazon SNS

Para la replicación de CloudMirror y los extremos de Amazon SNS, puede usar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave de acceso secreta
- CAP (C2S Access Portal): URL de credenciales temporales, certificados de servidor y de cliente, claves de cliente y una contraseña de clave privada de cliente opcional.

Puntos finales de Kafka

Para los puntos finales de Kafka, puede utilizar las siguientes credenciales:

- SASL/PLAIN: Nombre de usuario y contraseña
- SASL/SCRAM-SHA-256: Nombre de usuario y contraseña
- SASL/SCRAM-SHA-512: Nombre de usuario y contraseña

- Certificado de seguridad (si se utiliza un certificado de CA personalizado)

- Si las funciones de seguridad de Elasticsearch están activadas, tiene el privilegio de clúster de supervisión para las pruebas de conectividad y el privilegio WRITE INDEX o los privilegios INDEX y DELETE INDEX para las actualizaciones de documentos.

Pasos

1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**. Aparece la página de extremos de servicios de plataforma.
2. Seleccione **Crear punto final**.
3. Introduzca un nombre para mostrar para describir brevemente el extremo y su propósito.

   El tipo de servicio de plataforma que soporta el punto final se muestra junto al nombre del punto final cuando se muestra en la página de puntos finales, por lo que no es necesario incluir esa información en el nombre.

4. En el campo **URI**, especifique el Identificador de recursos único (URI) del extremo.

   Utilice uno de los siguientes formatos:

   ```
   https://host:port
   http://host:port
   ```

   Si no especifica un puerto, se utilizan los siguientes puertos predeterminados:

   - Puerto 443 para URI HTTPS y puerto 80 para URI HTTP (mayoría de extremos)
   - Puerto 9092 para URI HTTPS y HTTP (solo puntos finales Kafka)

   Por ejemplo, el URI para un bloque alojado en StorageGRID podría ser:

   ```
   https://s3.example.com:10443
   ```

   En este ejemplo: `s3.example.com` Representa la entrada DNS para la IP virtual (VIP) del grupo de alta disponibilidad (ha) de StorageGRID, y. `10443` representa el puerto definido en el extremo del equilibrador de carga.

   > Siempre que sea posible, debe conectarse a un grupo de alta disponibilidad de nodos de equilibrio de carga para evitar un único punto de error.

   Del mismo modo, el URI para un bloque alojado en AWS podría ser:

   ```
   https://s3-aws-region.amazonaws.com
   ```

   > Si el punto final se utiliza para el servicio de replicación de CloudMirror, no incluya el nombre del bloque en el URI. Incluye el nombre de bloque en el campo **URN**.

5. Introduzca el nombre de recurso único (URN) para el extremo.

No puede cambiar el URN de un punto final después de crear el punto final.

6. Seleccione **continuar**.
7. Seleccione un valor para **Tipo de autenticación**.

Extremos de integración de búsquedas de AWS

Introduzca o cargue las credenciales para un extremo de integración de búsqueda de AWS.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
Clave de acceso	Usa credenciales de estilo AWS para autenticar conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta
HTTP básico	Utiliza un nombre de usuario y una contraseña para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña
CAP (Portal de acceso C2S)	Usa certificados y claves para autenticar las conexiones al destino.	• URL de credenciales temporales • Certificado de CA de servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada de cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada no cifrado) • Contraseña de clave privada de cliente (opcional)

Replicación de CloudMirror o extremos de Amazon SNS

Introduzca o cargue las credenciales para una replicación de CloudMirror o un extremo de Amazon SNS.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
Clave de acceso	Usa credenciales de estilo AWS para autenticar conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta

Tipo de autenticación	Descripción	Credenciales
CAP (Portal de acceso C2S)	Usa certificados y claves para autenticar las conexiones al destino.	• URL de credenciales temporales • Certificado de CA de servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada de cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada no cifrado) • Contraseña de clave privada de cliente (opcional)

Puntos finales de Kafka

Introduzca o cargue las credenciales para un punto final de Kafka.

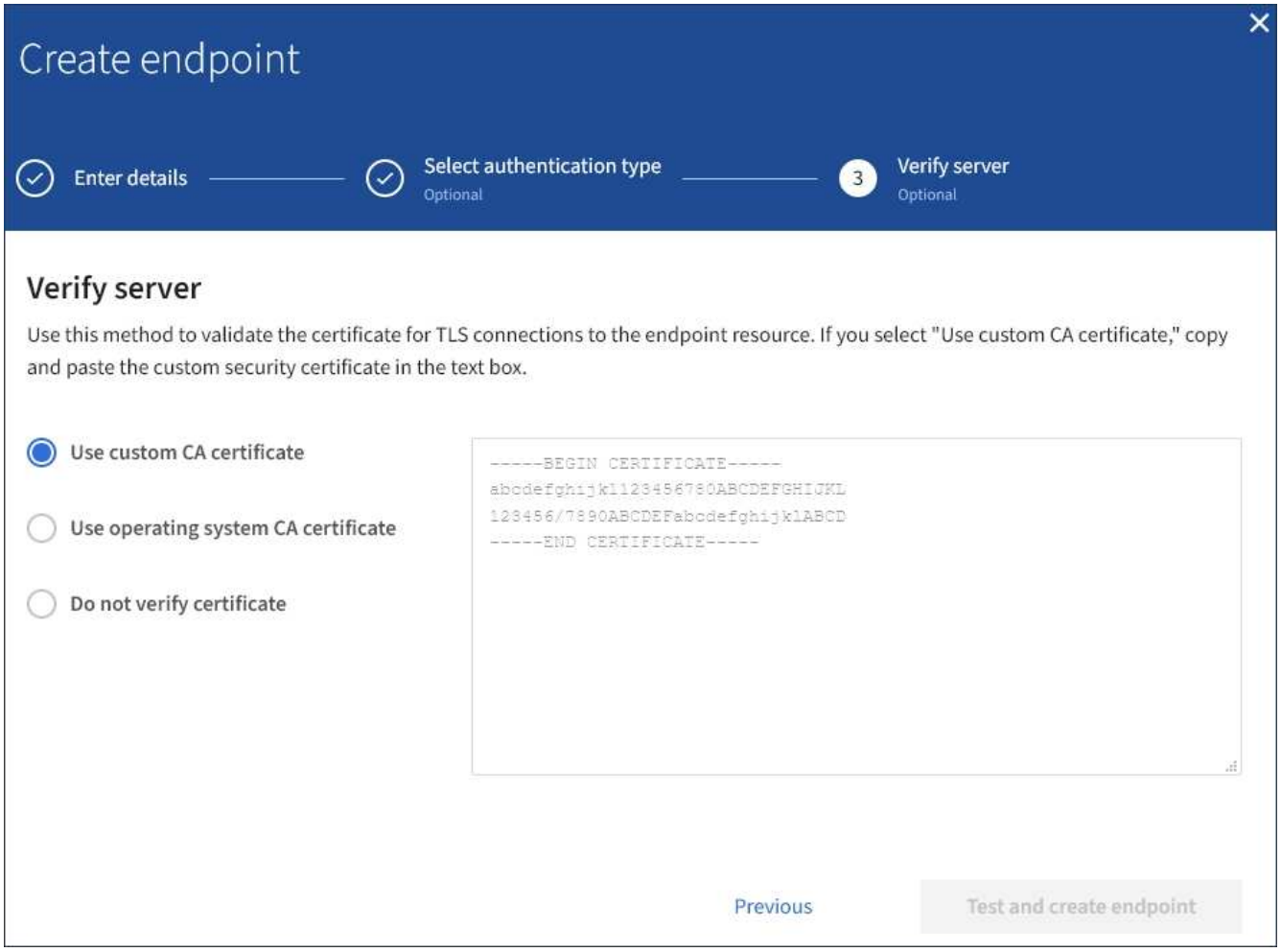
Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
SASL/PLAIN	Utiliza un nombre de usuario y una contraseña con texto sin formato para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña
SASL/SCRAM-SHA-256	Utiliza un nombre de usuario y una contraseña mediante un protocolo de respuesta de desafío y hash SHA-256 para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña
SASL/SCRAM-SHA-512	Utiliza un nombre de usuario y una contraseña mediante un protocolo de respuesta de desafío y hash SHA-512 para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña

Seleccione **Usar la autenticación de delegación tomada** si el nombre de usuario y la contraseña se derivan de un token de delegación que se obtuvo de un clúster de Kafka.

8. Seleccione **continuar**.
9. Seleccione un botón de opción para **verificar servidor** para elegir cómo se verifica la conexión TLS con el

extremo.



Tipo de verificación del certificado	Descripción
Utilizar certificado de CA personalizado	Usar un certificado de seguridad personalizado. Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto **Certificado CA**.
Utilizar certificado de CA del sistema operativo	Utilice el certificado de CA de cuadrícula predeterminado instalado en el sistema operativo para asegurar las conexiones.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica. Esta opción no es segura.

10. Seleccione **probar y crear punto final**.
    - Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión con el extremo se valida desde un nodo en cada sitio.
    - Aparece un mensaje de error si se produce un error en la validación del extremo. Si necesita modificar el punto final para corregir el error, seleccione **Volver a los detalles del punto final** y actualice la información. A continuación, seleccione **probar y crear punto final**.

La creación de punto final falla si los servicios de plataforma no están activados para su cuenta de inquilino. Póngase en contacto con el administrador de StorageGRID.

Una vez que haya configurado un extremo, puede utilizar su URN para configurar un servicio de plataforma.

Información relacionada

"Especifique URN para el extremo de servicios de la plataforma"

"Configure la replicación de CloudMirror"

"Configure las notificaciones de eventos"

"Configure el servicio de integración de búsqueda"

Probar la conexión para el extremo de servicios de la plataforma

Si la conexión a un servicio de plataforma ha cambiado, puede probar la conexión del extremo para validar que el recurso de destino existe y que se puede acceder a él utilizando las credenciales especificadas.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".

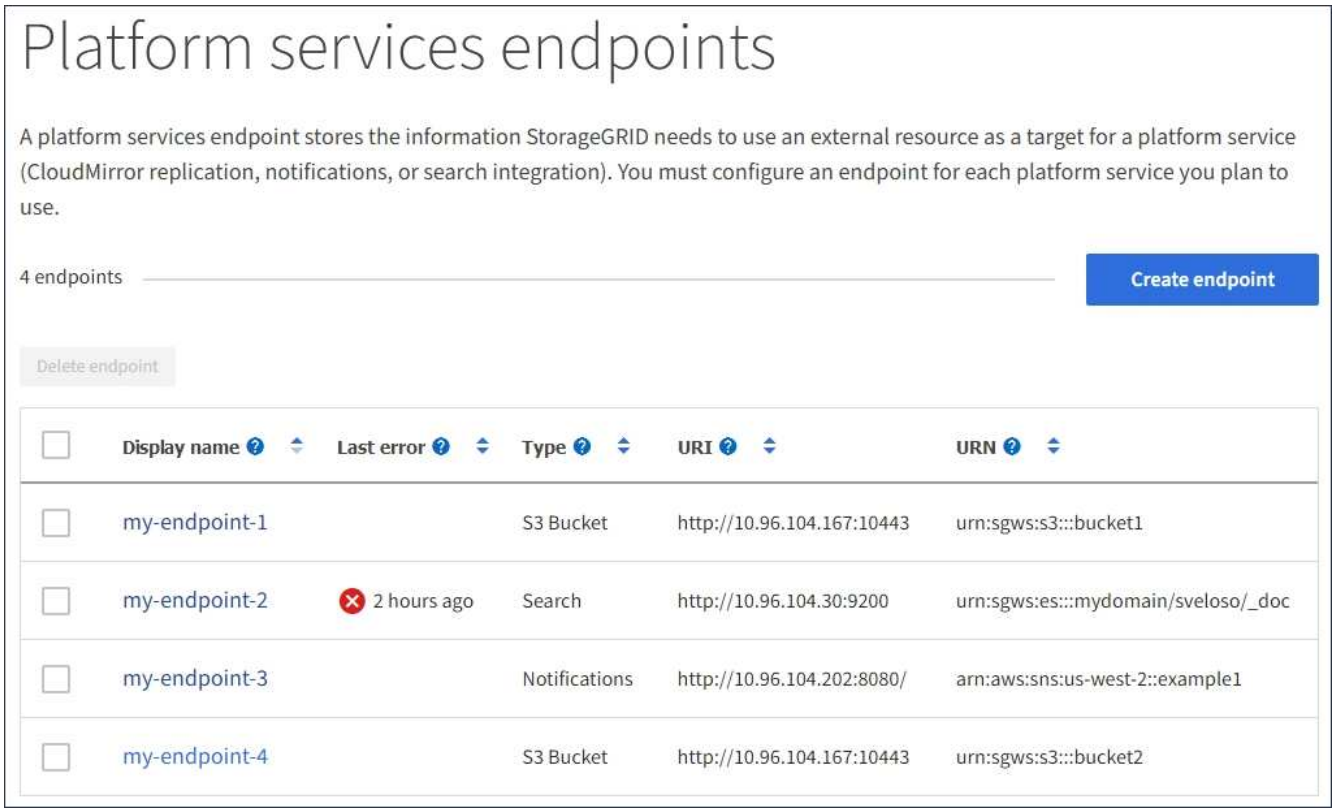
Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

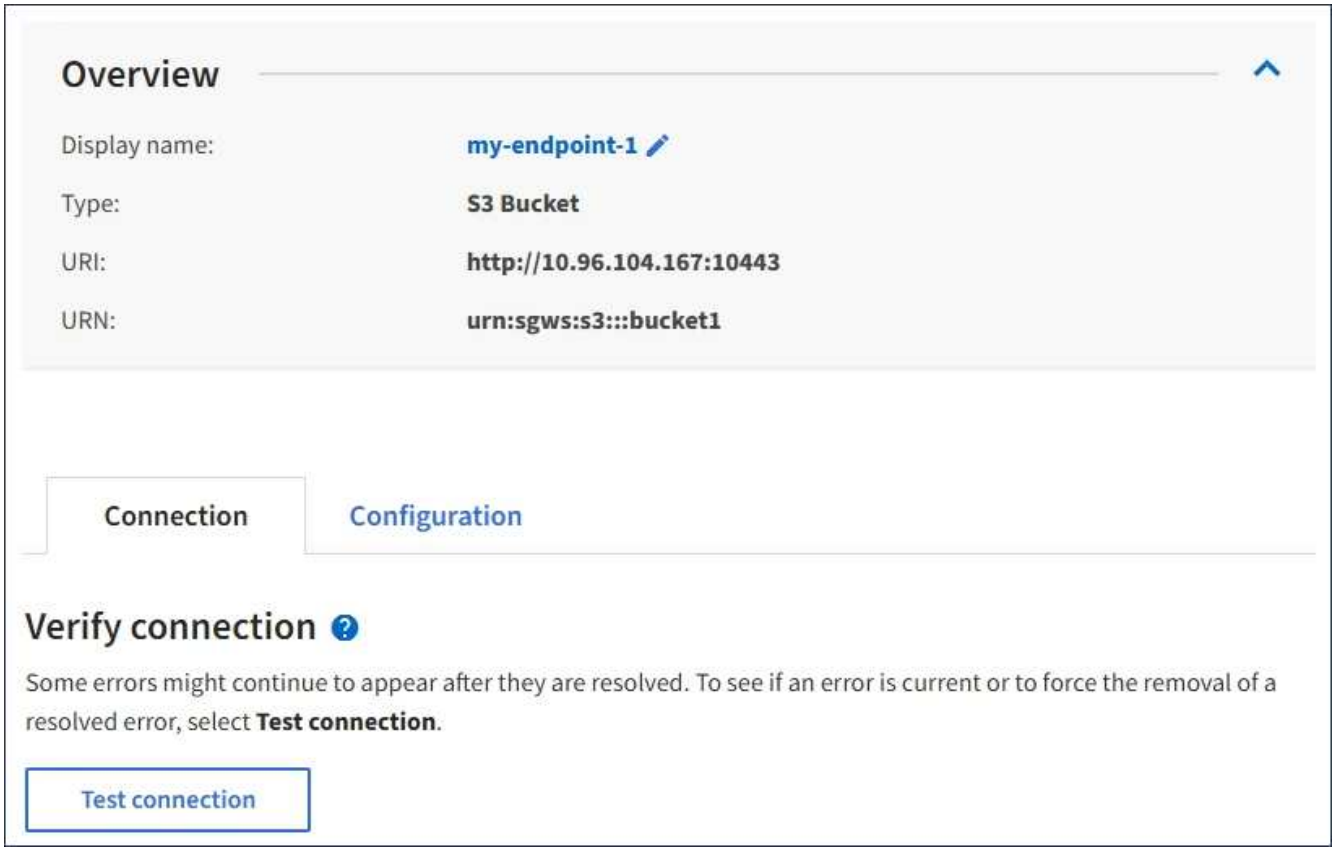
1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.



2. Seleccione el extremo cuya conexión desea probar.

   Aparece la página de detalles del extremo.



3. Seleccione **probar conexión**.

- Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión con el extremo se valida desde un nodo en cada sitio.
- Aparece un mensaje de error si se produce un error en la validación del extremo. Si necesita modificar el extremo para corregir el error, seleccione **Configuración** y actualice la información. A continuación, seleccione **probar y guardar los cambios**.

Editar extremo de servicios de plataforma

Puede editar la configuración de un extremo de servicios de plataforma para cambiar su nombre, URI u otros detalles. Por ejemplo, es posible que deba actualizar las credenciales caducadas o cambiar el URI para apuntar a un índice de Elasticsearch de backup para la conmutación por error. No puede cambiar el URN para un punto final de servicios de plataforma.

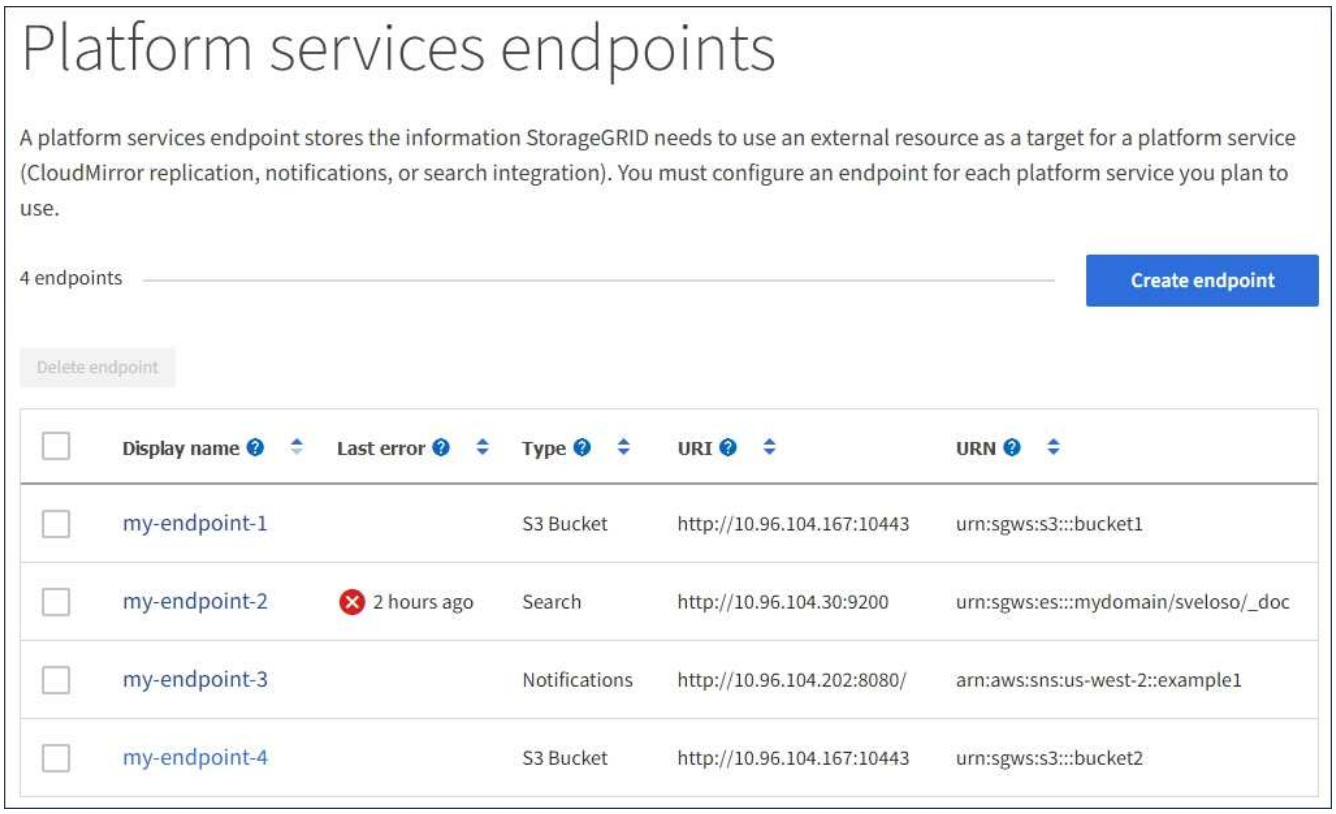
Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".

Pasos

1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.



2. Seleccione el extremo que desea editar.

   Aparece la página de detalles del extremo.

3. Seleccione **Configuración**.
4. Según sea necesario, cambie la configuración del extremo.

   No puede cambiar el URN de un punto final después de crear el punto final.

   a. Para cambiar el nombre para mostrar del extremo, seleccione el icono de edición .
   b. Según sea necesario, cambie el URI.
   c. Según sea necesario, cambie el tipo de autenticación.
      - Para la autenticación de la clave de acceso, cambie la clave según sea necesario seleccionando **Editar clave S3** y pegando un nuevo ID de clave de acceso y una clave de acceso secreta. Si necesita cancelar los cambios, seleccione **Revert S3 key EDIT**.
      - Para la autenticación CAP (C2S Access Portal), cambie la URL de las credenciales temporales o la frase de contraseña de la clave privada del cliente opcional y cargue nuevos archivos de certificado y claves según sea necesario.

        La clave privada del cliente debe estar en formato cifrado OpenSSL o en formato de clave privada no cifrada.

   d. Según sea necesario, cambie el método para verificar el servidor.
5. Seleccione **probar y guardar los cambios**.
   - Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión al extremo se verifica desde un nodo en cada sitio.
   - Aparece un mensaje de error si se produce un error en la validación del extremo. Modifique el extremo para corregir el error y, a continuación, seleccione **probar y guardar los cambios**.

Eliminar extremo de servicios de plataforma

Puede eliminar un extremo si ya no desea utilizar el servicio de plataforma asociado.

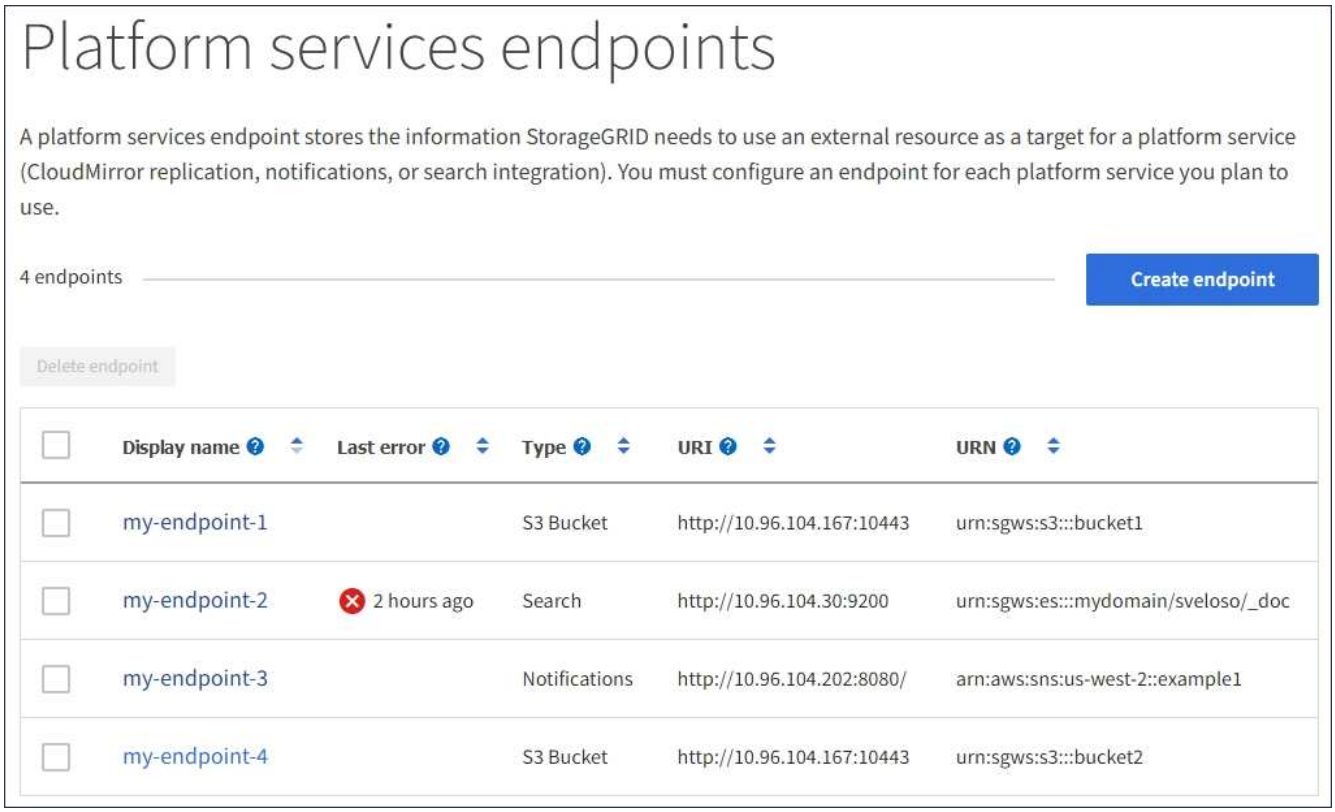
Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".

Pasos

1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.

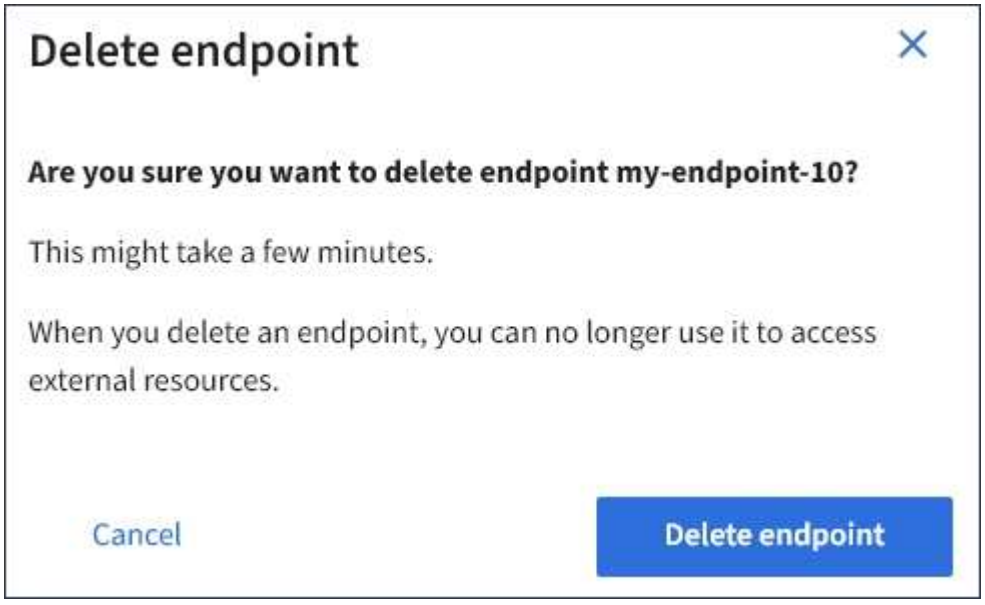


2. Seleccione la casilla de verificación de cada punto final que desee suprimir.

> Si elimina un extremo de servicios de plataforma que está en uso, el servicio de plataforma asociado se deshabilitará para todos los bloques que utilicen el extremo. Se descartarán las solicitudes que aún no se hayan completado. Se continuarán generando todas las solicitudes nuevas hasta que cambie la configuración de bloque para que ya no haga referencia a URN eliminado. StorageGRID informará de estas solicitudes como errores irrecuperables.

3. Seleccione **acciones** > **Eliminar punto final**.

   Aparecerá un mensaje de confirmación.



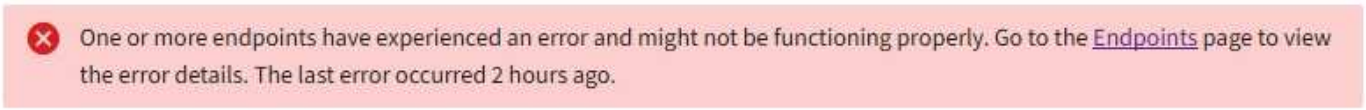
4. Seleccione **Eliminar punto final**.

Solucionar errores de extremos de servicios de plataforma

Si se produce un error cuando StorageGRID intenta comunicarse con un punto final de servicios de plataforma, se muestra un mensaje en el panel de control. En la página Platform Services Endpoints, la columna Last error indica durante cuánto tiempo se produjo el error. No se muestra ningún error si los permisos asociados con las credenciales de un extremo son incorrectos.

Determine si se ha producido un error

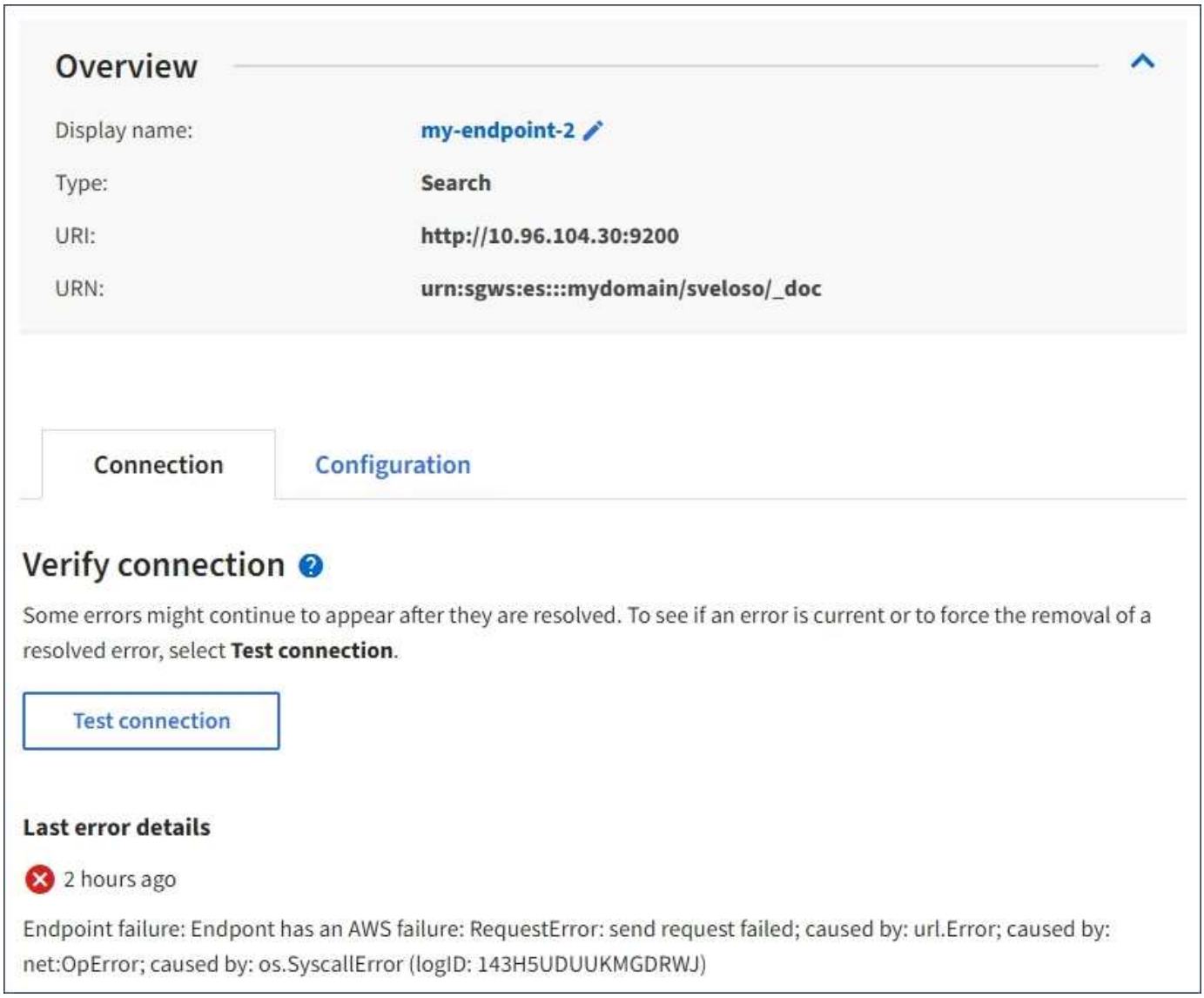
Si se ha producido algún error de punto final de servicios de plataforma en los últimos 7 días, el panel de control del gestor de inquilinos muestra un mensaje de alerta. Puede ir a la página de extremos de servicios de plataforma para ver más detalles sobre el error.



El mismo error que aparece en el panel de control también aparece en la parte superior de la página Puntos Finales de Servicios de Plataforma. Para ver un mensaje de error más detallado:

Pasos

1. En la lista de puntos finales, seleccione el extremo que tiene el error.
2. En la página de detalles del punto final, seleccione **Conexión**. Esta pestaña muestra sólo el error más reciente de un punto final e indica cuánto tiempo se produjo el error. Errores que incluyen el icono X rojo  ocurrió en los últimos 7 días.



Compruebe si el error sigue estando actualizado

Es posible que algunos errores sigan apareciendo en la columna **último error** incluso después de que se hayan resuelto. Para ver si un error es actual o para forzar la eliminación de un error resuelto de la tabla:

Pasos

1. Seleccione el extremo.

   Aparece la página de detalles del extremo.

2. Seleccione **Conexión** > **probar conexión**.

Al seleccionar **probar conexión**, StorageGRID valida que el extremo de servicios de la plataforma existe y que se puede alcanzar con las credenciales actuales. La conexión con el extremo se valida desde un nodo en cada sitio.

Resolver errores de punto final

Puede utilizar el mensaje **último error** de la página de detalles del punto final para ayudar a determinar qué está causando el error. Es posible que algunos errores requieran que edite el extremo para resolver el problema. Por ejemplo, se puede producir un error CloudMirroring si StorageGRID no puede acceder al

bloque de S3 de destino porque no tiene los permisos de acceso correctos o si la clave de acceso ha caducado. El mensaje es «Las credenciales del punto final o el acceso al destino deben actualizarse» y los detalles son «ACCESSDENIED» o «InvalidAccessKeyId».

Si necesita editar el extremo para resolver un error, al seleccionar **probar y guardar cambios** StorageGRID validará el extremo actualizado y confirmará que se puede alcanzar con las credenciales actuales. La conexión con el extremo se valida desde un nodo en cada sitio.

Pasos

1. Seleccione el extremo.
2. En la página de detalles del punto final, seleccione **Configuración**.
3. Edite la configuración del extremo según sea necesario.
4. Seleccione **Conexión** > **probar conexión**.

Credenciales de extremo con permisos insuficientes

Cuando StorageGRID valida un extremo de servicios de plataforma, confirma que las credenciales del extremo se pueden utilizar para ponerse en contacto con el recurso de destino y realiza una comprobación básica de permisos. Sin embargo, StorageGRID no valida todos los permisos necesarios para ciertas operaciones de servicios de plataforma. Por este motivo, si recibe un error al intentar utilizar un servicio de plataforma (como “403 Forbidden”), compruebe los permisos asociados con las credenciales del punto final.

Información relacionada

- **Administrar los servicios de plataforma de StorageGRID › Solucionar problemas**
- "Cree un extremo de servicios de plataforma"
- "Probar la conexión para el extremo de servicios de la plataforma"
- "Editar extremo de servicios de plataforma"

Configure la replicación de CloudMirror

La "Servicio de replicación de CloudMirror" Es uno de los tres servicios de plataforma de StorageGRID. Puede usar la replicación de CloudMirror para replicar automáticamente objetos en un bloque de S3 externo.

Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket que actúa como origen de replicación.
- El punto final que pretende utilizar como destino para la replicación de CloudMirror ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

La replicación de CloudMirror copia los objetos de un bloque de origen en un bloque de destino que se especifique en un extremo.

La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre grid. Para obtener más información, consulte "Compare la replicación entre grid y la replicación de CloudMirror".

Para habilitar la replicación de CloudMirror para un bucket, debe crear y aplicar un XML de configuración de replicación de bucket válido. El XML de configuración de replicación debe usar la URN de un extremo de bloque de S3 para cada destino.

La replicación no es compatible con buckets de origen o destino con el bloqueo de objetos S3 habilitado.

Para obtener información general sobre la replicación de bloques y cómo configurarla, consulte "Documentación de Amazon Simple Storage Service (S3): Replicación de objetos". Para obtener información sobre cómo StorageGRID implementa GetBucketReplication, DeleteBucketReplication y PutBucketReplication, consulte "Operaciones en bloques".

Si habilita la replicación de CloudMirror en un bloque que contiene objetos, se replican los nuevos objetos agregados al bloque, pero los objetos existentes del bloque no se replican. Debe actualizar los objetos existentes para activar la replicación.

Si se especifica una clase de almacenamiento en el XML de configuración de replicación, StorageGRID utiliza esa clase al realizar operaciones en el extremo de S3 de destino. El extremo de destino también debe admitir la clase de almacenamiento especificada. Asegúrese de seguir las recomendaciones que proporciona el proveedor del sistema de destino.

Pasos

1. Habilite la replicación para su bloque de origen:

   Utilice un editor de texto para crear el XML de configuración de replicación necesario para habilitar la replicación, tal y como se especifica en la API de replicación de S3. Al configurar XML:

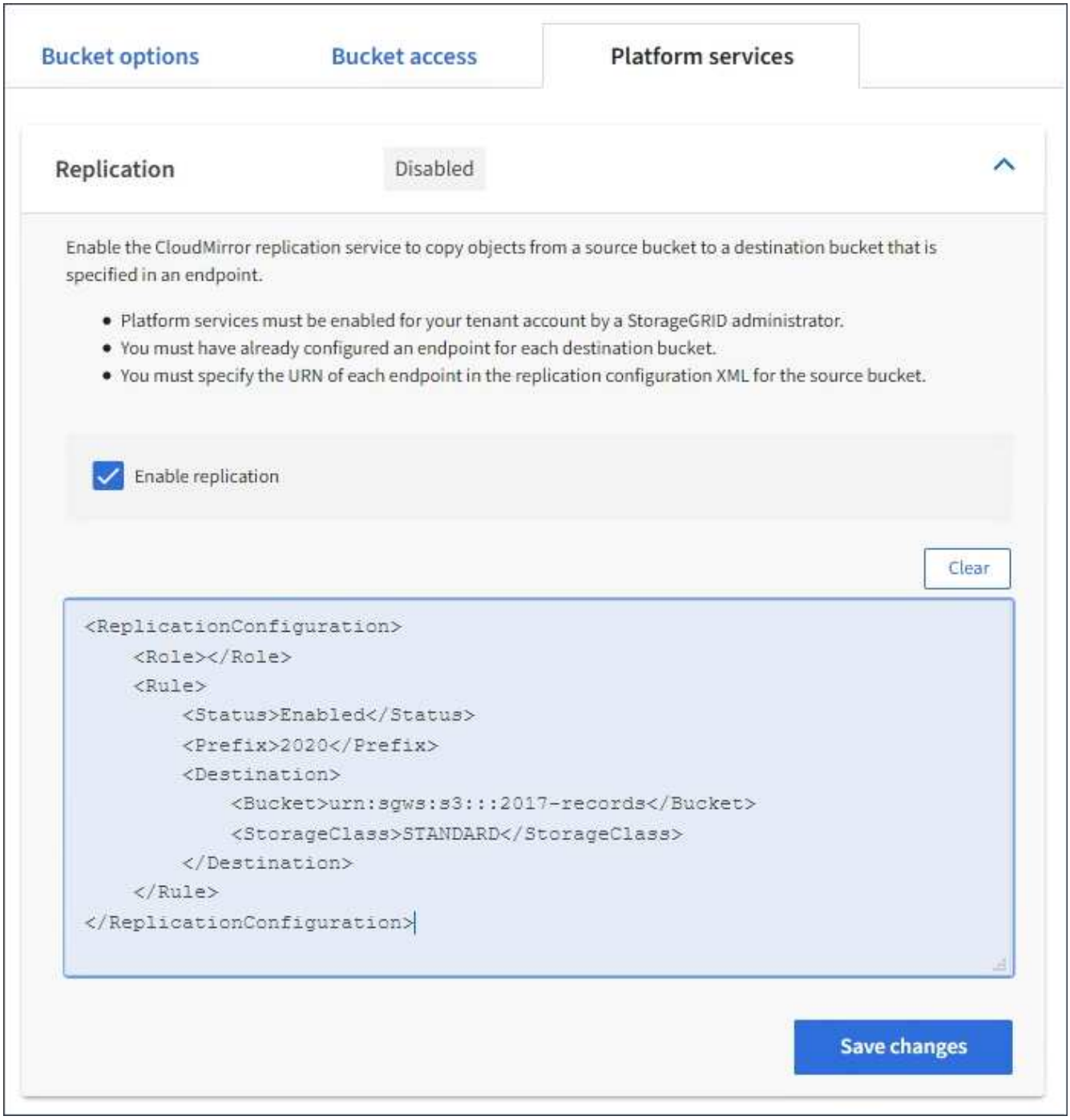
   - Tenga en cuenta que StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de `Filter` Elemento para reglas y sigue las convenciones V1 para eliminar versiones de objetos. Consulte la documentación de Amazon sobre la configuración de replicación para obtener más información.
   - Use el URN de un extremo de bloque de S3 como destino.
   - Si lo desea, puede agregar el `<StorageClass>` y especifique una de las siguientes opciones:
     - `STANDARD`: La clase de almacenamiento predeterminada. Si no especifica una clase de almacenamiento al cargar un objeto, el `STANDARD` se utiliza la clase de almacenamiento.
     - `STANDARD_IA`: (Estándar - acceso poco frecuente.) Utilice esta clase de almacenamiento para los datos a los que se accede con menor frecuencia; sin embargo, este proceso requiere un acceso rápido cuando sea necesario.
     - `REDUCED_REDUNDANCY`: Utilice esta clase de almacenamiento para datos no críticos y reproducibles que se pueden almacenar con menos redundancia que el `STANDARD` clase de almacenamiento.
   - Si especifica un `Role` En el XML de configuración se ignorará. StorageGRID no utiliza este valor.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
3. Seleccione el nombre del bloque de origen.

   Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma** > **replicación**.
5. Seleccione la casilla de verificación **Habilitar replicación**.
6. Pegue el XML de configuración de replicación en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión de grid. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que la replicación está configurada correctamente:
   a. Añada un objeto al bloque de origen que cumpla con los requisitos de replicación según se especifica en la configuración de replicación.

      En el ejemplo mostrado anteriormente, se replican los objetos que coincidan con el prefijo «2020».

   b. Confirme que el objeto se ha replicado en el bloque de destino.

En el caso de objetos pequeños, la replicación se realiza con rapidez.

Información relacionada

"Cree un extremo de servicios de plataforma"

Configure las notificaciones de eventos

El servicio de notificaciones es uno de los tres servicios de la plataforma StorageGRID. Puede habilitar las notificaciones de un depósito para enviar información sobre eventos especificados a un clúster Kafka de destino o servicio compatible con AWS Simple Notification Service (Amazon SNS).

Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya creó un bloque para que actúe como origen de notificaciones.
- El punto final que pretende utilizar como destino para las notificaciones de eventos ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar las notificaciones de eventos, cada vez que se produce un evento específico para un objeto en el depósito de origen, se genera una notificación y se envía al tema de Amazon SNS o Kafka utilizado como punto final de destino. Para habilitar las notificaciones para un bloque, debe crear y aplicar un XML de configuración de notificación válido. El XML de configuración de notificaciones debe usar el URN de un extremo de notificaciones de eventos para cada destino.

Para obtener información general sobre las notificaciones de eventos y cómo configurarlas, consulte la documentación de Amazon. Para obtener información sobre cómo StorageGRID implementa la API de configuración de notificación de bloques de S3, consulte la "Instrucciones para implementar aplicaciones cliente de S3".

Si habilita las notificaciones de eventos para un bloque que contiene objetos, las notificaciones se envían solo para las acciones que se realizan una vez guardada la configuración de notificación.

Pasos

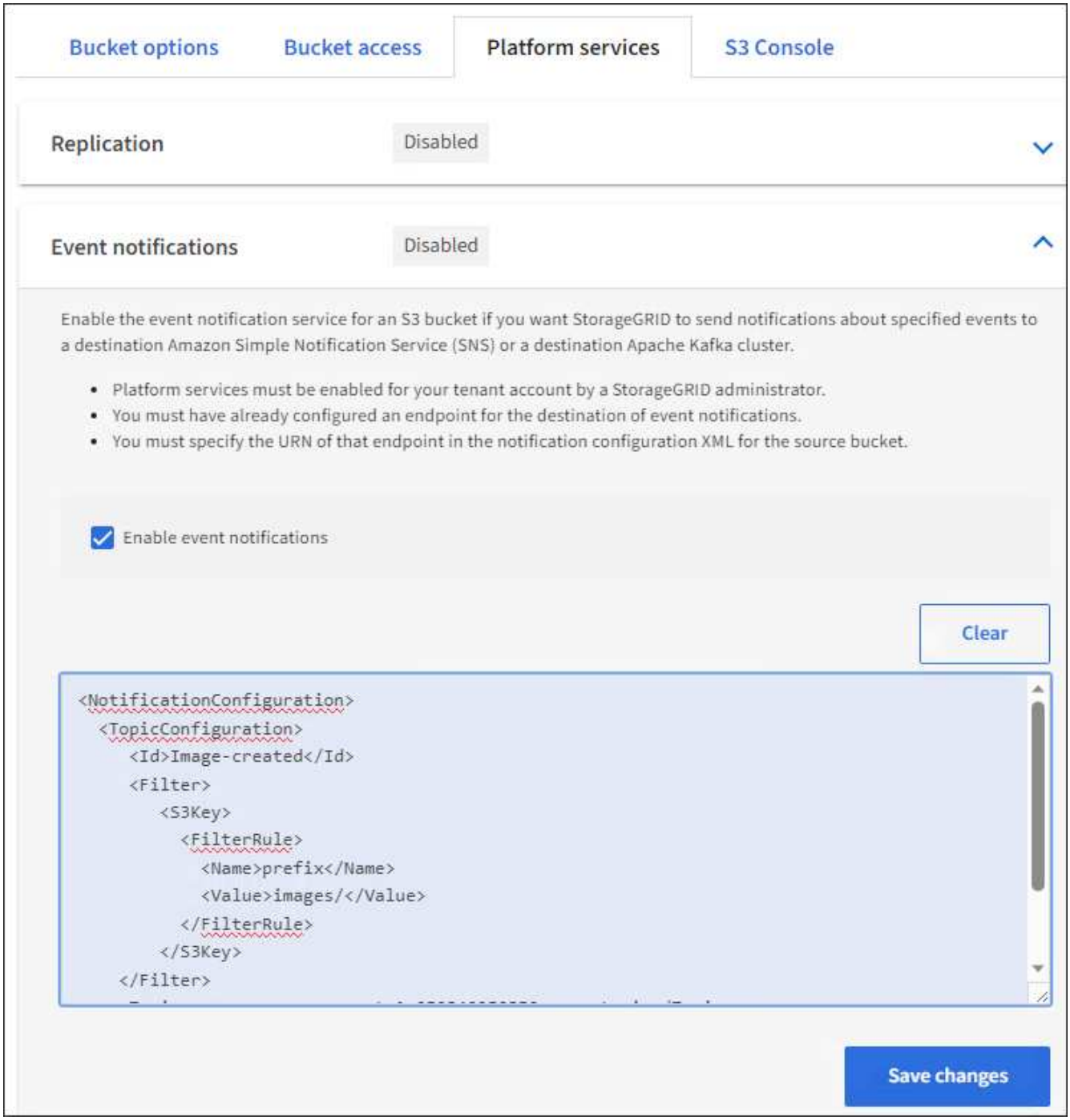
1. Habilite las notificaciones para su bloque de origen:
    - Use un editor de texto para crear el XML de configuración de notificaciones necesario para habilitar las notificaciones de eventos, como se especifica en la API de notificación de S3.
    - Al configurar XML, utilice URN de un extremo de notificaciones de eventos como tema de destino.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
3. Seleccione el nombre del bloque de origen.

   Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma** > **Notificaciones de eventos**.
5. Seleccione la casilla de verificación **Habilitar notificaciones de eventos**.
6. Pegue el XML de configuración de notificación en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión de grid. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que las notificaciones de eventos están configuradas correctamente:

   a. Realice una acción en un objeto del bloque de origen que cumpla los requisitos para activar una notificación tal y como se ha configurado en el XML de configuración.

      En el ejemplo, se envía una notificación de evento cada vez que se crea un objeto con el `images/` prefijo.

b. Confirme que se ha entregado una notificación al tema de destino de Amazon SNS o Kafka.

Por ejemplo, si el tema de destino está alojado en Amazon SNS, puede configurar el servicio para que le envíe un correo electrónico cuando se entregue la notificación.


```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


+ Si se recibe la notificación en el tema de destino, ha configurado correctamente el bloque de origen para las notificaciones StorageGRID.

Información relacionada

"Comprender las notificaciones para bloques"

"USE LA API DE REST DE S3"

"Cree un extremo de servicios de plataforma"

Utilice el servicio de integración de búsqueda

El servicio de integración de búsqueda es uno de los tres servicios de la plataforma StorageGRID. Este servicio puede habilitar el envío de metadatos de objetos a un índice de búsqueda de destino siempre que se cree, se elimine o actualice los metadatos o las etiquetas de un objeto.

Puede configurar la integración de búsqueda mediante el Administrador de inquilinos para aplicar XML de configuración de StorageGRID personalizado a un bloque.

> Debido a que el servicio de integración de búsqueda hace que los metadatos de objeto se envíen a un destino, su XML de configuración se denomina XML_ de configuración de notificación de metadatos. Este XML de configuración es diferente al *notification Configuration XML* utilizado para habilitar las notificaciones de eventos.

Consulte "Instrucciones para implementar aplicaciones cliente de S3" Para obtener detalles sobre las siguientes operaciones personalizadas de la API de REST de StorageGRID S3:

- DELETE bucket metadata notification Configuration
- OBTENGA la configuración de notificación de metadatos del bloque de datos
- Configuración de notificaciones de metadatos de PUT Bucket

Información relacionada

"XML de configuración para la integración de búsqueda"

"Metadatos de objetos incluidos en las notificaciones de metadatos"

"JSON generado por el servicio de integración de búsqueda"

"Configure el servicio de integración de búsqueda"

"USE LA API DE REST DE S3"

XML de configuración para la integración de búsqueda

El servicio de integración de búsqueda se configura mediante un conjunto de reglas contenidas en `<MetadataNotificationConfiguration>` y.. `</MetadataNotificationConfiguration>` etiquetas. Cada regla especifica los objetos a los que se aplica la regla y el destino al que StorageGRID debe enviar los metadatos de esos objetos.

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, puede enviar metadatos de los objetos con el prefijo `images` en un destino y los metadatos de los objetos con el prefijo `videos` a otro. Las configuraciones que tienen prefijos superpuestos no son válidas y se rechazan cuando se envían. Por ejemplo, una configuración que incluye una regla para objetos con el prefijo `test` y una segunda regla para

los objetos con el prefijo `test2` no está permitido.

Los destinos deben especificarse mediante el URN de un extremo de StorageGRID que se ha creado para el servicio de integración de búsqueda. Estos extremos se refieren a un índice y tipo definidos en un clúster de Elasticsearch.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

En la tabla se describen los elementos del XML de configuración de notificaciones de metadatos.

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos Regla.	Sí
Regla	Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Regla.	No

Nombre	Descripción	Obligatorio
Estado	El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas. Incluido en el elemento Regla.	Sí
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para hacer coincidir todos los objetos, especifique un prefijo vacío. Incluido en el elemento Regla.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Regla.	Sí
No	URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades: • `es` debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en el formulario `domain-name/myindex/mytype`. Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404. EL VALOR DE URN se incluye en el elemento Destination.	Sí

Utilice el XML de configuración de notificación de metadatos de ejemplo para aprender a crear su propio XML.

La configuración de notificaciones de metadatos se aplica a todos los objetos

En este ejemplo, los metadatos de objeto de todos los objetos se envían al mismo destino.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Configuración de notificaciones de metadatos con dos reglas

En este ejemplo, metadatos de objeto para objetos que coinciden con el prefijo `/images` se envía a un destino, mientras que los metadatos de objetos de los objetos que coinciden con el prefijo `/videos` se envía a un segundo destino.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Información relacionada

"USE LA API DE REST DE S3"

"Metadatos de objetos incluidos en las notificaciones de metadatos"

"JSON generado por el servicio de integración de búsqueda"

"Configure el servicio de integración de búsqueda"

Configure el servicio de integración de búsqueda

El servicio de integración de búsqueda envía metadatos de objetos a un índice de búsqueda de destino cada vez que se crea, se elimina o se actualizan sus metadatos o etiquetas.

Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket S3 cuyo contenido desea indexar.
- El punto final que pretende utilizar como destino para el servicio de integración de búsqueda ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar el servicio de integración de búsqueda para un bloque de origen, al crear un objeto o actualizar los metadatos o las etiquetas de un objeto se activan los metadatos de objeto que se enviarán al extremo de destino. Si habilita el servicio de integración de búsqueda para un depósito que ya contiene objetos, las notificaciones de metadatos no se envían automáticamente para los objetos existentes. Debe actualizar estos objetos existentes para asegurarse de que sus metadatos se agregan al índice de búsqueda de destino.

Pasos

1. Utilice un editor de texto para crear el XML de notificación de metadatos necesario para habilitar la integración de búsqueda.
   - Consulte la información sobre XML de configuración para la integración de búsquedas.
   - Al configurar XML, utilice URN de un extremo de integración de búsqueda como destino.

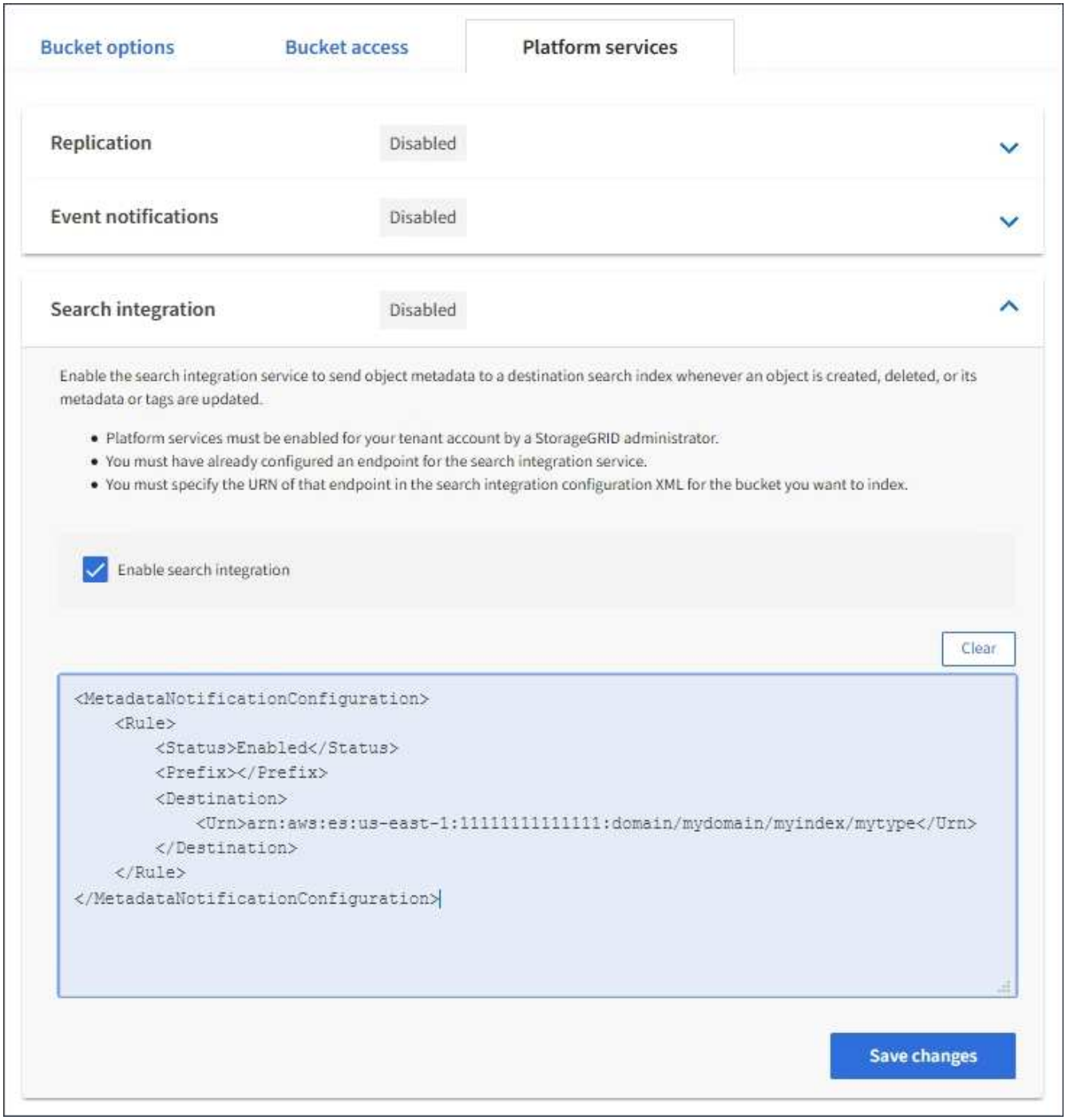
```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
3. Seleccione el nombre del bloque de origen.

   Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma** > **integración de búsqueda**
5. Seleccione la casilla de verificación **Habilitar integración de búsqueda**.

6. Pegue la configuración de notificación de metadatos en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que el servicio de integración de búsqueda está configurado correctamente:
   a. Añada un objeto al bloque de origen que cumpla los requisitos para activar una notificación de metadatos tal y como se especifica en el XML de configuración.

      En el ejemplo mostrado anteriormente, todos los objetos añadidos al bloque activan una notificación de metadatos.

b. Confirme que se ha agregado un documento JSON que contiene los metadatos y las etiquetas del objeto al índice de búsqueda especificado en el extremo.

Después de terminar

Según sea necesario, se puede deshabilitar la integración de búsqueda para un bloque con cualquiera de los siguientes métodos:

- Seleccione **STORAGE (S3)** > **Buckets** y desactive la casilla de verificación **Enable search integration**.
- Si utiliza la API de S3 directamente, utilice una solicitud de notificación DELETE Bucket. Consulte las instrucciones para implementar aplicaciones cliente de S3.

Información relacionada

"Comprender el servicio de integración de búsquedas"

"XML de configuración para la integración de búsqueda"

"USE LA API DE REST DE S3"

"Cree un extremo de servicios de plataforma"

JSON generado por el servicio de integración de búsqueda

Al habilitar el servicio de integración de búsqueda para un bloque, se genera un documento JSON y se envía al extremo de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas del objeto.

Este ejemplo muestra un ejemplo de JSON que se podría generar cuando un objeto con la clave `SGWS/Tagging.txt` se crea en un bloque llamado `test`. La `test` el bloque no tiene versiones, por lo que el `versionId` la etiqueta está vacía.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadatos de objetos incluidos en las notificaciones de metadatos

En la tabla se enumeran todos los campos que se incluyen en el documento JSON que se envían al extremo de destino cuando la integración de búsqueda está habilitada.

El nombre del documento incluye el nombre del bloque, el nombre del objeto y el ID de versión, si existe.

Tipo	Nombre y descripción del artículo
Información sobre bloques y objetos	`bucket`: Nombre del cubo
`key`: Nombre de clave de objeto	`versionID`: Versión de objeto, para objetos en cubos con versiones
`region`: Región de cucharón, por ejemplo `us-east-1`	Metadatos del sistema
`size`: Tamaño del objeto (en bytes) visible para un cliente HTTP	`md5`: Hash de objeto
Metadatos del usuario	`metadata`: Todos los metadatos de usuario del objeto, como pares clave-valor `key:value`
Etiquetas	`tags`: Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor `key:value`

Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para interpretar estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para la asignación dinámica de campos y para asignar formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Después de indexar un documento, no puede editar los tipos de campo del documento en el índice.