Utilice una cuenta de inquilino

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Utilice una cuenta de inquilino

Utilice una cuenta de inquilino

Una cuenta de inquilino le permite utilizar la API REST de Simple Storage Service (S3) o la API 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 federados o locales, usuarios, depósitos S3 o contenedores Swift y objetos.

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

- **Caso de uso empresarial:** si el sistema StorageGRID se utiliza dentro de una empresa, el almacenamiento de objetos de la red podría estar segregado por los diferentes departamentos de la organización. Por ejemplo, podría haber cuentas de inquilinos para el departamento de Marketing, el departamento de Atención al Cliente, el departamento de Recursos Humanos, etc.

  > Si utiliza el protocolo de cliente S3, también puede usar depósitos S3 y políticas de depósitos para segregar objetos entre los departamentos de una empresa. No es necesario crear cuentas de inquilino separadas. Consulte las instrucciones para la implementación"Cubos S3 y políticas de cubos" Para más información.

- **Caso de uso de proveedor de servicios:** si un proveedor de servicios utiliza el sistema StorageGRID , el almacenamiento de objetos de la red puede estar segregado por las diferentes entidades que alquilan el almacenamiento. Por ejemplo, podría haber cuentas de inquilinos para la Empresa A, la Empresa B, la Empresa C, etc.

Cómo crear una cuenta de inquilino

Las cuentas de inquilinos son creadas por un"Administrador de red StorageGRID que utiliza el Administrador de red" . Al crear una cuenta de inquilino, el administrador de la red especifica lo siguiente:

- Información básica que incluye el nombre del inquilino, el tipo de cliente (S3) y la cuota de almacenamiento opcional.
- Permisos para la cuenta de inquilino, como si la cuenta de inquilino puede usar servicios de la plataforma S3, configurar su propia fuente de identidad, usar S3 Select o usar una conexión de federación de red.
- El acceso raíz inicial para el inquilino, en función de si el sistema StorageGRID utiliza grupos y usuarios locales, federación de identidad o inicio de sesión único (SSO).

Además, los administradores de la red pueden habilitar la configuración de Bloqueo de objetos S3 para el sistema StorageGRID si las cuentas de inquilinos S3 necesitan cumplir con los requisitos reglamentarios. Cuando el bloqueo de objetos S3 está habilitado, todas las cuentas de inquilinos de S3 pueden crear y administrar depósitos compatibles.

Configurar inquilinos de S3

Después de un"Se crea una cuenta de inquilino S3" , puede acceder al Administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidad (a menos que la fuente de identidad se comparta con la red)
- Administrar grupos y usuarios
- Utilice la federación de red para la clonación de cuentas y la replicación entre redes
- Administrar claves de acceso S3
- Crear y administrar depósitos S3
- Utilice los servicios de la plataforma S3
- Utilice S3 Select
- Monitorear el uso del almacenamiento

Si bien puede crear y administrar depósitos S3 con el Administrador de inquilinos, debe usar un"Cliente S3" o"Consola S3" para ingerir y gestionar objetos.

Cómo iniciar y cerrar sesión

Sign in en el Administrador de inquilinos

Puede acceder al Administrador de inquilinos ingresando la URL del inquilino en la barra de direcciones de un"navegador web compatible" .

Antes de empezar

- Tienes tus credenciales de inicio de sesión.
- Tiene una URL para acceder al Administrador de inquilinos, proporcionada por su administrador de red. La URL se verá como 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 podría incluir un número de puerto, el ID de la cuenta del inquilino de 20 dígitos o ambos.

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

Pasos

1. Lanzar un"navegador web compatible" .
2. En la barra de direcciones del navegador, ingrese la URL para acceder al Administrador de inquilinos.
3. Si aparece una alerta de seguridad, instale el certificado utilizando el asistente de instalación del navegador.

4. Sign in en el Administrador de inquilinos.

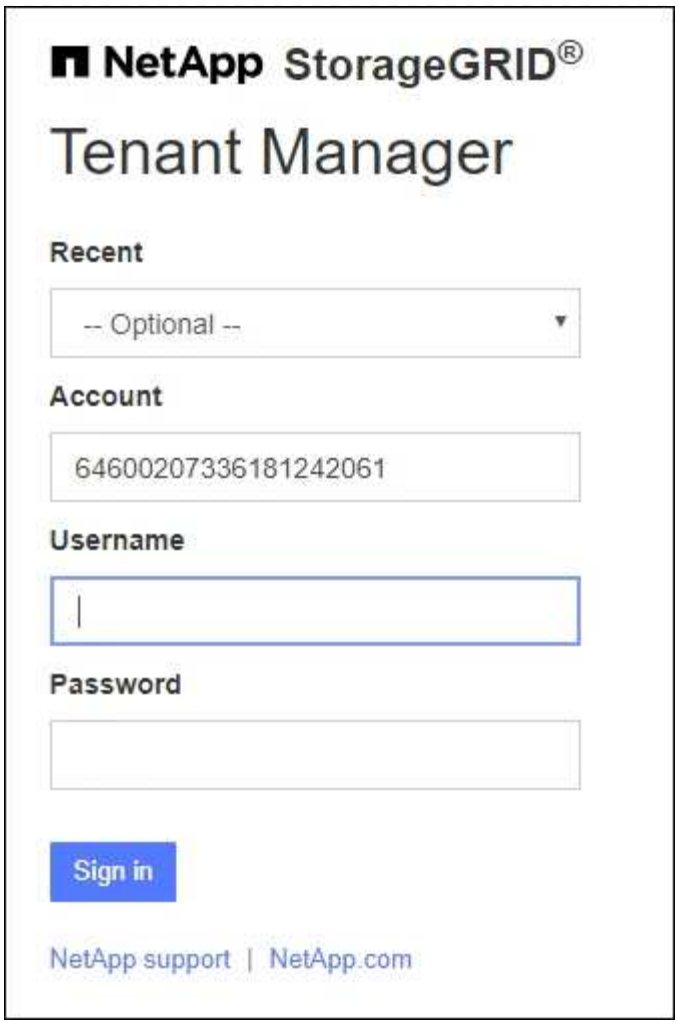
   La pantalla de inicio de sesión que aparece depende de la URL ingresada y de si se ha configurado el inicio de sesión único (SSO) para StorageGRID.

No usar SSO

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

- La página de inicio de sesión de Grid Manager. Seleccione el enlace **Inicio de sesión 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 inquilino, seleccione el nombre de la cuenta del inquilino si aparece en la lista de cuentas recientes o ingrese el ID de cuenta.

ii. Introduzca su nombre de usuario y contraseña.

iii. Seleccionar * Sign in*.

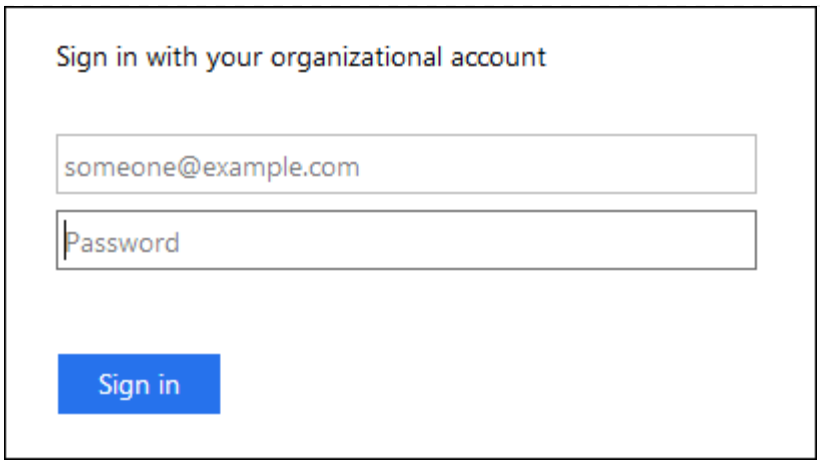
Aparece el panel del Administrador de inquilinos.

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

Usando SSO

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

◦ La página SSO de su organización. Por ejemplo:



Ingrese sus credenciales SSO estándar y seleccione * Sign in*.

- La página de inicio de sesión SSO del administrador de inquilinos.

i. Si no se muestra el ID de cuenta de 20 dígitos del inquilino, seleccione el nombre de la cuenta del inquilino si aparece en la lista de cuentas recientes o ingrese el ID de cuenta.
ii. Seleccionar * Sign in*.
iii. Sign in con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

Aparece el panel del Administrador de inquilinos.

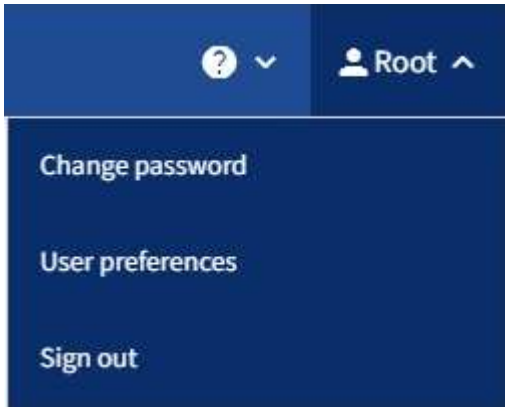
Cerrar sesión en el Administrador de inquilinos

Cuando termine de trabajar con el Administrador de inquilinos, deberá cerrar la sesión

para asegurarse de que usuarios no autorizados no puedan acceder al sistema StorageGRID . Es posible que cerrar su navegador no cierre su sesión del sistema, según la configuración de cookies del navegador.

Pasos

1. Localice el menú desplegable de nombre de usuario en la esquina superior derecha de la interfaz de usuario.



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

   - Si no se utiliza SSO:

     Has cerrado la sesión del nodo de administración. Se muestra la página de inicio de sesión del Administrador de inquilinos.

     Si inició sesión en más de un nodo de administración, deberá cerrar sesión en cada nodo.

   - Si SSO está habilitado:

     Has cerrado la sesión de todos los nodos de administración a los que estabas accediendo. Se muestra la página de Sign in de StorageGRID . El nombre de la cuenta de inquilino a la que acaba de acceder aparece como predeterminado en el menú desplegable **Cuentas recientes** y se muestra el **ID de cuenta** del inquilino.

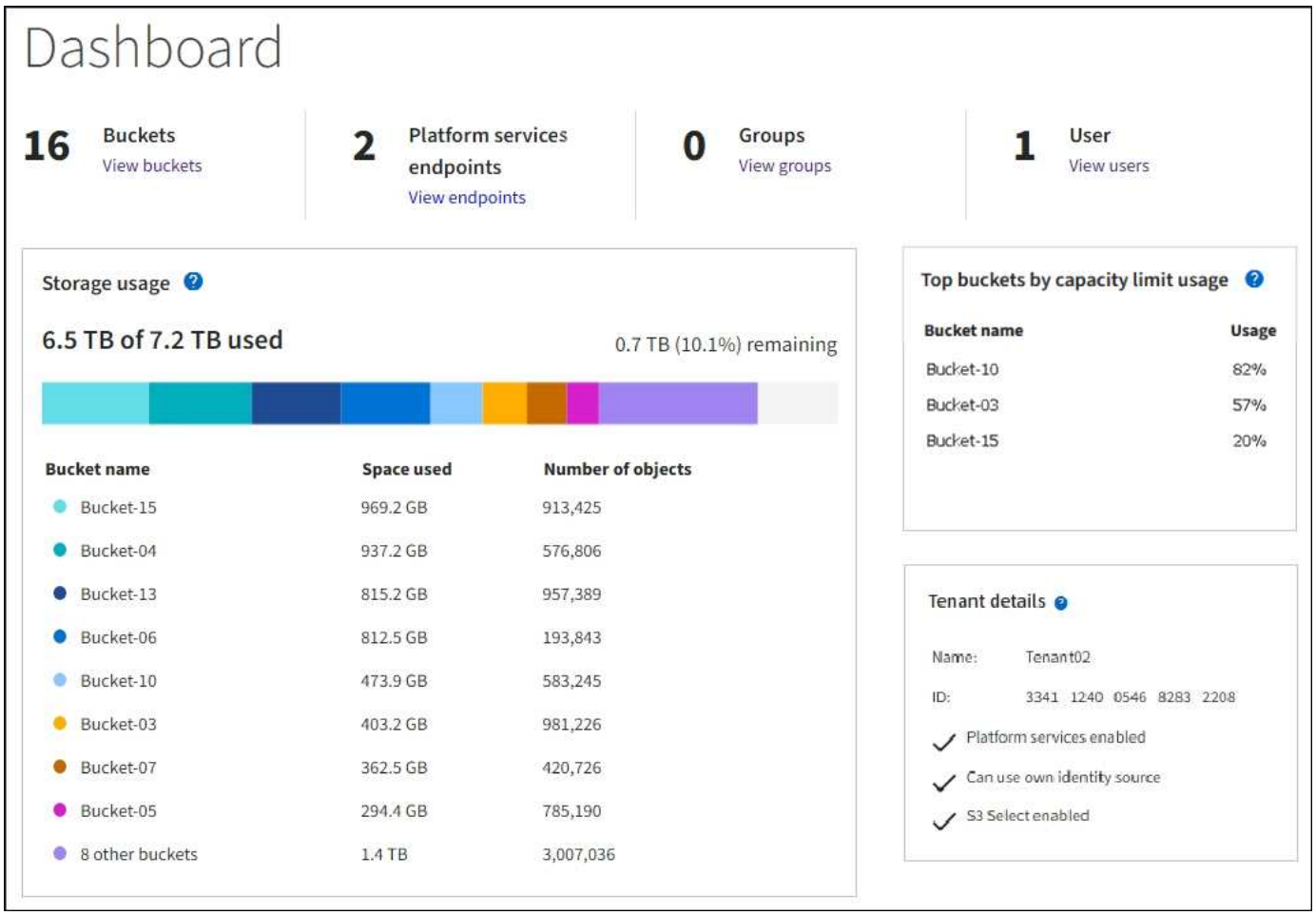
     Si SSO está habilitado y también ha iniciado sesión en Grid Manager, también debe cerrar sesión en Grid Manager para cerrar sesión en SSO.

Comprender el panel de control de Tenant Manager

El panel de Tenant Manager proporciona una descripción general de la configuración de una cuenta de inquilino y la cantidad de espacio utilizado por los objetos en los depósitos (S3) o contenedores (Swift) del inquilino. Si el inquilino tiene una cuota, el panel muestra cuánto de la cuota se utiliza y cuánto queda. Si hay algún error relacionado con la cuenta del inquilino, los errores se muestran en el panel de control.

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

Una vez cargados los objetos, el panel de control se verá como el siguiente ejemplo:



Información de la cuenta del inquilino

En la parte superior del panel se muestra la cantidad de depósitos o contenedores, grupos y usuarios configurados. También muestra el número de puntos finales de servicios de la plataforma, si se ha configurado alguno. Seleccione los enlaces para ver los detalles.

Dependiendo de la"permisos de gestión de inquilinos" Tiene las opciones que ha configurado y el resto del panel muestra varias combinaciones de pautas, uso de almacenamiento, información de objetos y detalles del inquilino.

Uso de almacenamiento y cuotas

El panel de uso de almacenamiento contiene la siguiente información:

- La cantidad de datos de objetos para el inquilino.

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

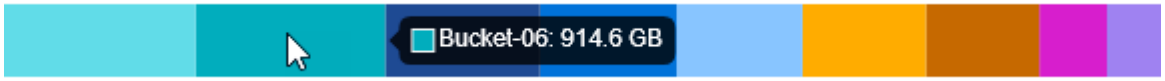
- Si se establece una cuota, la cantidad total de espacio disponible para los datos del objeto y la cantidad y

el porcentaje de espacio restante. La cuota limita la cantidad de datos de objetos que se pueden ingerir.

> El uso de la cuota se basa en estimaciones internas y podría superarse en algunos casos. Por ejemplo, StorageGRID verifica la cuota cuando un inquilino comienza a cargar objetos y rechaza nuevas ingestas si el inquilino ha excedido la cuota. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha excedido la cuota. Si se eliminan objetos, es posible que a un inquilino se le impida temporalmente cargar nuevos objetos hasta que se vuelva a calcular el uso de la cuota. Los cálculos de uso de cuota 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 contenedor o depósito.



- Para corresponder con el gráfico de barras, una lista de los depósitos o contenedores más grandes, incluida la cantidad total de datos de objetos y la cantidad de objetos para cada depósito 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 contenedores o cubos, todos los demás contenedores o cubos se combinan en una sola entrada en la parte inferior de la lista.

> Para cambiar las unidades de 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 luego seleccione **Preferencias de usuario**.

Alertas de uso de cuota

Si se han habilitado las alertas de uso de cuota en el Administrador de red, estas alertas aparecerán en el Administrador de inquilinos cuando la cuota sea baja o se exceda, de la siguiente manera:

- Si se ha utilizado el 90 % o más de la cuota de un inquilino, se activa la alerta **Uso de cuota de inquilino alto**.

  Considere pedirle a su administrador de red que aumente la cuota.

- Si excede su cuota, una notificación le indicará que no puede cargar nuevos objetos.

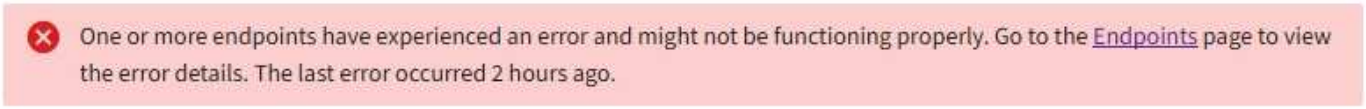
Uso del límite de capacidad

Si ha establecido un límite de capacidad para sus grupos, el panel del Administrador de inquilinos muestra una lista de los grupos principales según el uso del límite de capacidad.

Si no se establece ningún límite para un depósito, su capacidad es ilimitada. Sin embargo, si su cuenta de inquilino tiene una cuota de almacenamiento total y dicha cuota se alcanza, no podrá ingerir más objetos independientemente del límite de capacidad restante en un depósito.

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 Tenant Manager muestra una alerta si se ha producido algún error en los puntos finales en los últimos siete días.



Para ver detalles sobre"errores de punto final de servicios de plataforma" , seleccione **Puntos finales** para mostrar la página Puntos finales.

API de gestión de inquilinos

Comprender la API de gestión de inquilinos

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

La API de gestión de inquilinos:

- Utiliza la plataforma API de código abierto 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 completos y documentación para cada operación de API.
- Usos"control de versiones para soportar actualizaciones sin interrupciones" .

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

1. Sign in en el Administrador de inquilinos.
2. Desde la parte superior del Administrador de inquilinos, seleccione el ícono de ayuda y seleccione **Documentación de API**.

Operaciones de API

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

- **cuenta**: Operaciones en la cuenta del inquilino actual, incluida la obtención de información sobre el uso del almacenamiento.
- **auth**: Operaciones para realizar la autenticación de la sesión del usuario.

  La API de administración de inquilinos admite el esquema de autenticación de token de portador. Para iniciar sesión en 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 debe proporcionarse en el encabezado de las solicitudes de API posteriores ("Autorización: Token de portador").

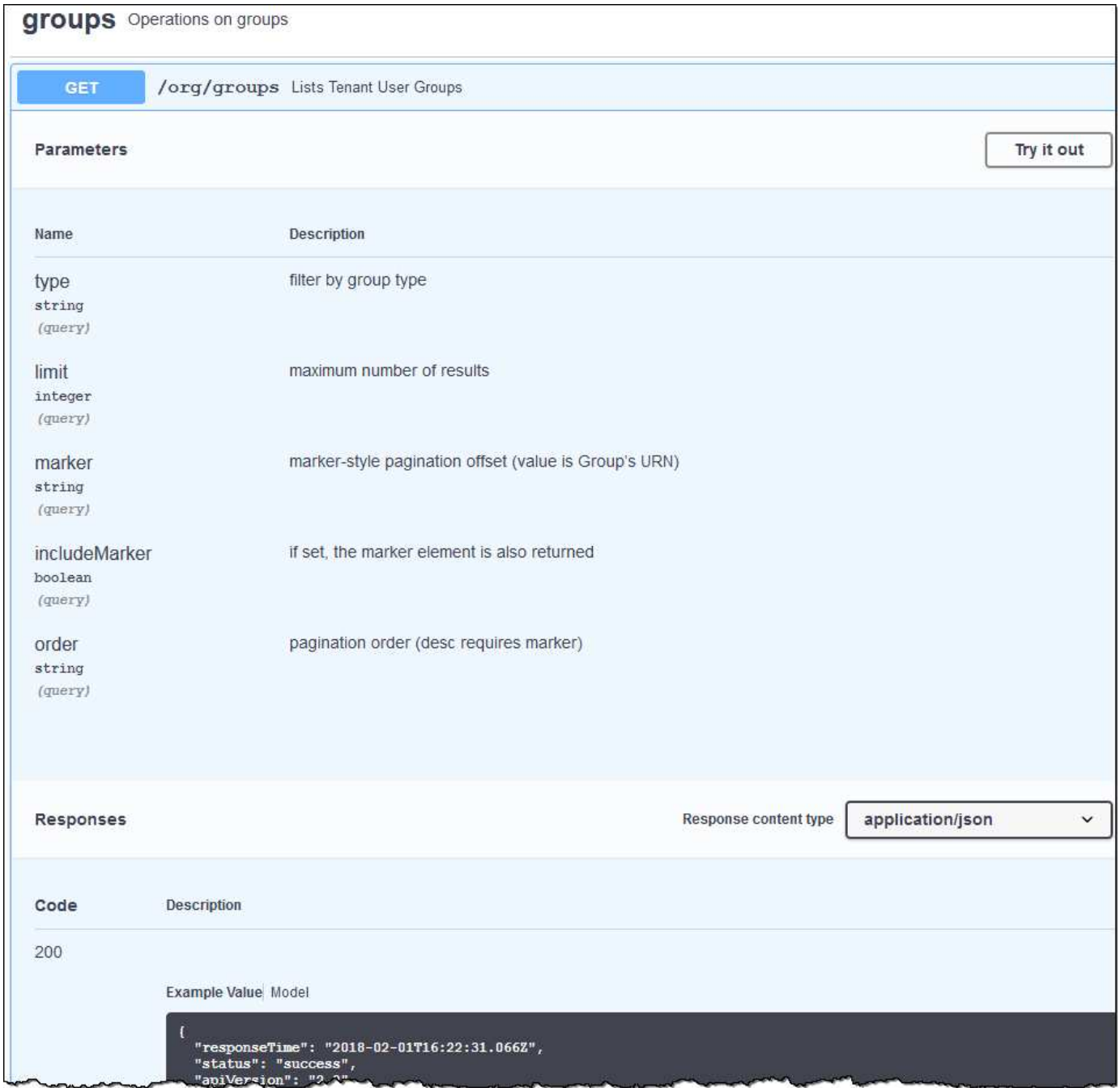
  Para obtener información sobre cómo mejorar la seguridad de la autenticación, consulte"Protección contra la falsificación de solicitudes entre sitios" .

  > Si el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID , debe realizar diferentes pasos para autenticarse. Ver el"Instrucciones para utilizar la API de administración de red" .

- **config**: Operaciones relacionadas con el lanzamiento del producto y las versiones de la API de administración de inquilinos. Puede enumerar la versión de lanzamiento del producto y las versiones principales de la API compatibles con esa versión.
- **contenedores**: Operaciones en buckets S3 o contenedores Swift.
- **funciones-desactivadas**: Operaciones para ver funciones que podrían haber sido desactivadas.
- **endpoints**: Operaciones para administrar un punto final. Los puntos finales permiten que un bucket S3 utilice un servicio externo para la replicación, las notificaciones o la integración de búsqueda de StorageGRID CloudMirror.
- **grid-federation-connections**: Operaciones en conexiones de federación de redes y replicación entre redes.
- **grupos**: Operaciones para administrar grupos de inquilinos locales y recuperar grupos de inquilinos federados desde una fuente de identidad externa.
- **identity-source**: Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información de usuarios y grupos federados.
- **ilm**: Operaciones en configuraciones de gestión del ciclo de vida de la información (ILM).
- **regiones**: 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 bloqueo de objetos S3, utilizadas para respaldar el cumplimiento normativo.
- **usuarios**: Operaciones para ver y administrar los usuarios del inquilino.

Detalles de la operación

Al expandir cada operación de API, puede ver su acción HTTP, la URL del punto final, una lista de parámetros obligatorios u opcionales, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.



Emitir solicitudes de API

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

Pasos

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

2. Determinar si la solicitud requiere parámetros adicionales, como un ID de grupo o usuario. Luego, obtenga estos valores. Es posible que primero debas emitir una solicitud API diferente para obtener la información que necesitas.
3. Determina si necesitas modificar el cuerpo de la solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.
4. Seleccione **Probarlo**.
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 fue exitosa.

Control de versiones de la API de gestión de inquilinos

La API de administración de inquilinos utiliza versiones para admitir actualizaciones sin interrupciones.

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

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

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

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

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

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

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

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

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

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

Determinar qué versiones de API son compatibles con la versión actual

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

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

Especificar una versión de API para una solicitud

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

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

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

Protección contra la falsificación de solicitudes entre sitios (CSRF)

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

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

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

Para habilitar la función, configure el `csrfToken` parámetro a `true` durante la autenticación. El valor predeterminado es `false` .

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

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

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

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

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

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

Utilizar conexiones de federación de red

Clonar grupos de inquilinos y usuarios

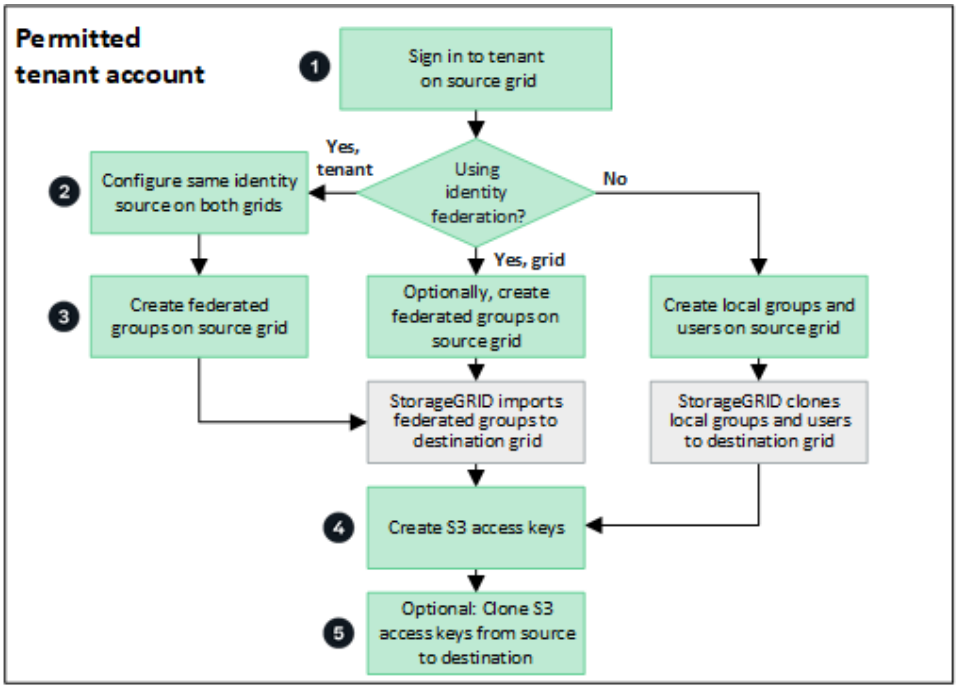
Si se creó o editó un inquilino para usar una conexión de federación de red, ese inquilino se replica desde un sistema StorageGRID (el inquilino de origen) a otro sistema StorageGRID (el inquilino de réplica). Una vez replicado el inquilino, todos los grupos y usuarios agregados al inquilino de origen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

El sistema StorageGRID donde se crea originalmente el inquilino es la *cuadrícula de origen* del inquilino. El sistema StorageGRID donde se replica el inquilino es la *red 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 más detalles, véase"¿Qué es la clonación de cuenta?" y"Gestionar inquilinos permitidos" .

La clonación de la información de la cuenta del inquilino es necesaria para"replicación entre redes" de objetos de cubo. Tener los mismos grupos de inquilinos y usuarios en ambas redes garantiza que pueda acceder a los depósitos y objetos correspondientes en cualquiera de las redes.

Flujo de trabajo del inquilino para la clonación de cuentas

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, 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 Sign in en el inquilino

Sign in en la cuenta del inquilino en la cuadrícula de origen (la cuadrícula donde se creó inicialmente el inquilino).

2 Opcionalmente, configure la federación de identidad

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

3 Crear grupos y usuarios

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

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

4 Crear claves de acceso S3

Puede"crea tus propias claves de acceso" o a"crear las claves de acceso de otro usuario" en la red de origen o en la red de destino para acceder a los contenedores en esa red.

5 **Opcionalmente, clonar claves de acceso S3**

Si necesita acceder a depósitos con las mismas claves de acceso en ambas cuadrículas, cree las claves de acceso en la cuadrícula de origen y luego use la API de Tenant Manager para clonarlas manualmente en la cuadrícula de destino. Para obtener instrucciones, consulte"Clonar claves de acceso S3 usando la API" .

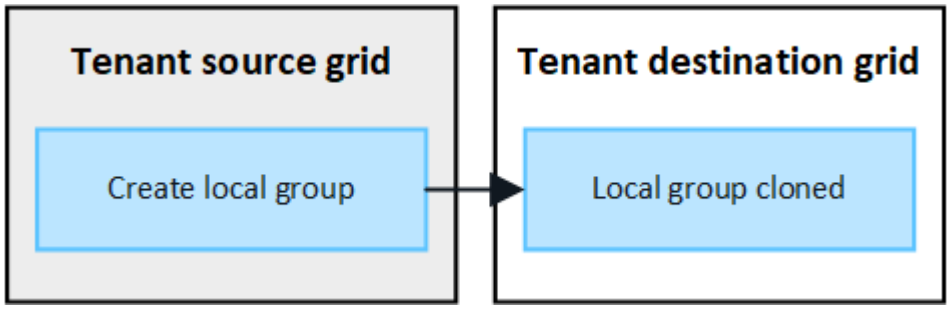
¿Cómo se clonan grupos, usuarios y claves de acceso S3?

Revise esta sección para comprender cómo se clonan los grupos, los usuarios y las claves de acceso de S3 entre la red de origen del inquilino y la red de destino del inquilino.

Los grupos locales creados en la red de origen se clonan

Una vez que se crea una cuenta de inquilino y se replica en la red de destino, StorageGRID clona automáticamente cualquier grupo local que agregue a la red de origen del inquilino en la red de destino del inquilino.

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

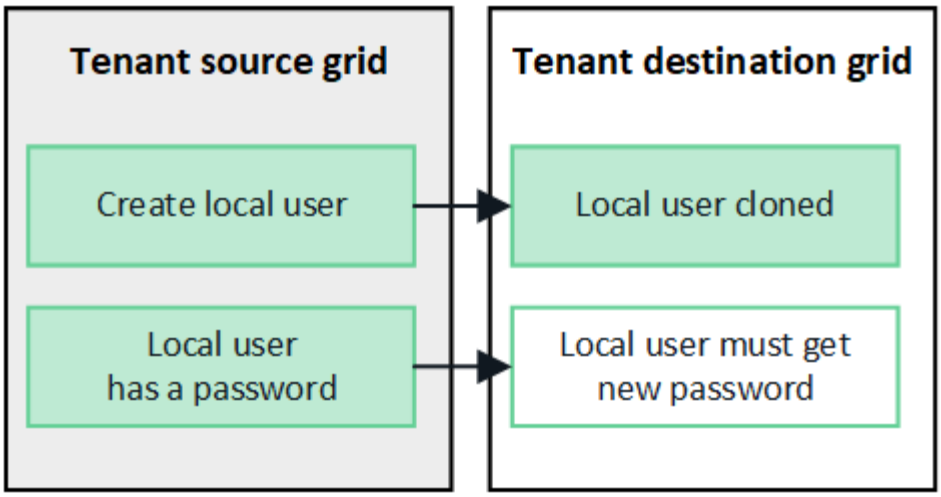


Cualquier usuario que seleccione al crear un grupo local en la cuadrícula de origen no se incluirá cuando el grupo se clone en la cuadrícula de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Los usuarios locales creados en la red de origen se clonan

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

Por razones de seguridad, las contraseñas de los usuarios locales no se clonan en la red de destino. Si un usuario local necesita acceder a Tenant Manager en la red de destino, el usuario raíz de la cuenta de inquilino debe agregar una contraseña para ese usuario en la red de destino. Para obtener instrucciones, consulte"Administrar usuarios locales" .

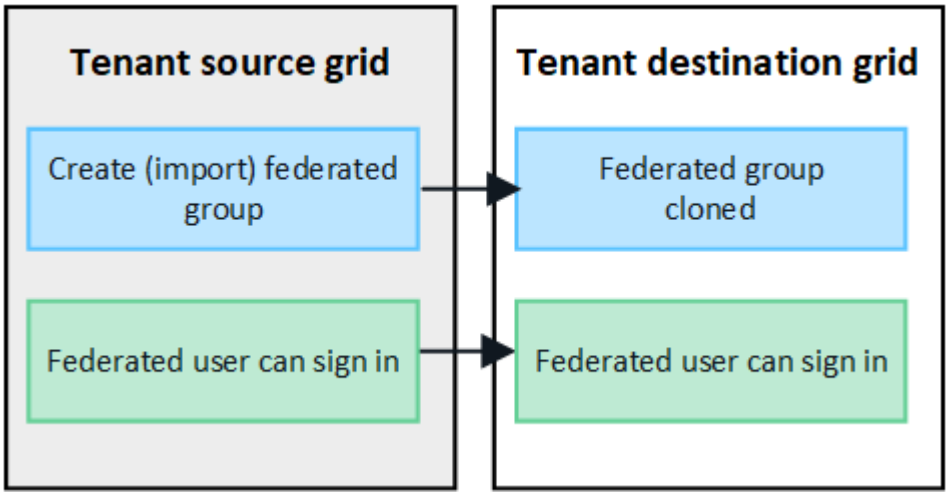


Los grupos federados creados en la red de origen se clonan

Suponiendo que se cumplen los requisitos para usar la clonación de cuenta con"inicio de sesión único" y"federación de identidades" Una vez cumplidos, los grupos federados que cree (importe) para el inquilino en la red de origen se clonan automáticamente en el inquilino en la red de destino.

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

Una vez creados los grupos federados para el inquilino de origen y clonados en el inquilino de destino, los usuarios federados pueden iniciar sesión en el inquilino en cualquiera de las cuadrículas.

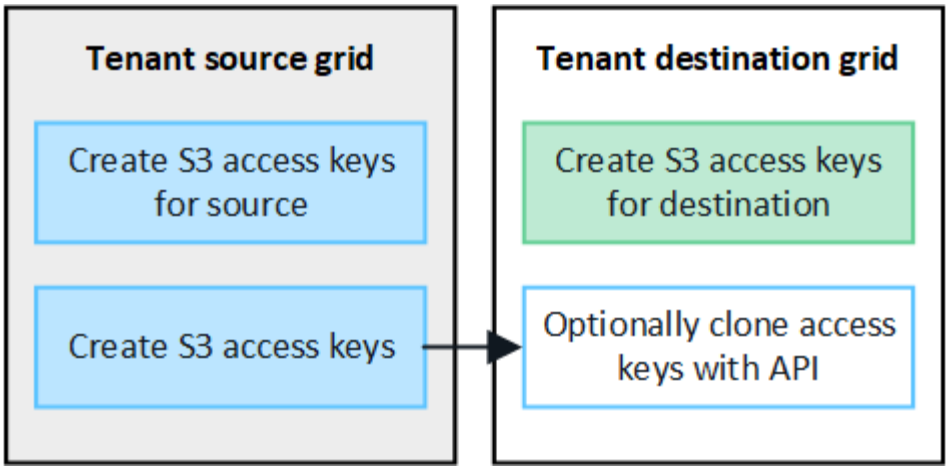


Las claves de acceso S3 se pueden clonar manualmente

StorageGRID no clona automáticamente las claves de acceso de S3 porque la seguridad se mejora al tener claves diferentes en cada cuadrícula.

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

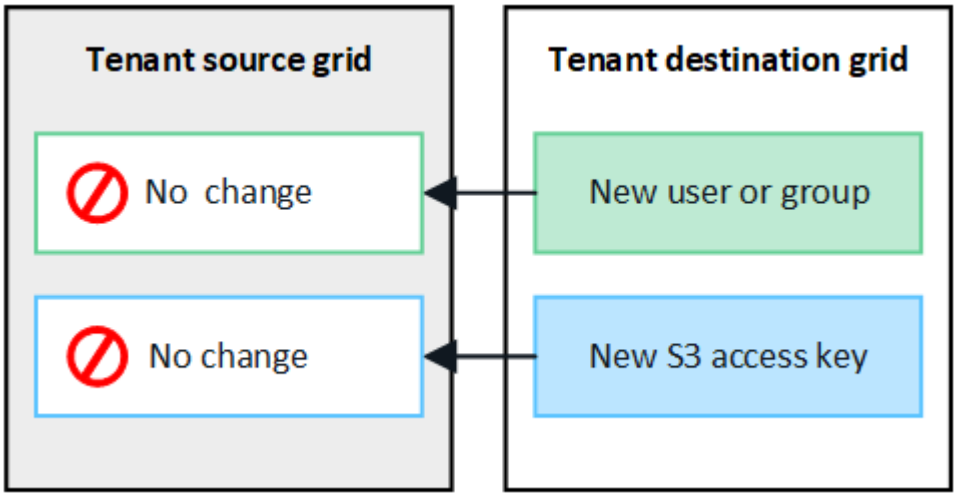
- Si no necesita utilizar las mismas claves para cada cuadrícula, puede"crea tus propias claves de acceso" o"crear las claves de acceso de otro usuario" en cada cuadrícula.
- Si necesita usar las mismas claves en ambas cuadrículas, puede crear claves en la cuadrícula de origen y luego usar la API de Tenant Manager para hacerlo manualmente."clonar las claves" a la red de destino.



Cuando se clonan 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 agregados a la cuadrícula de destino no se clonan

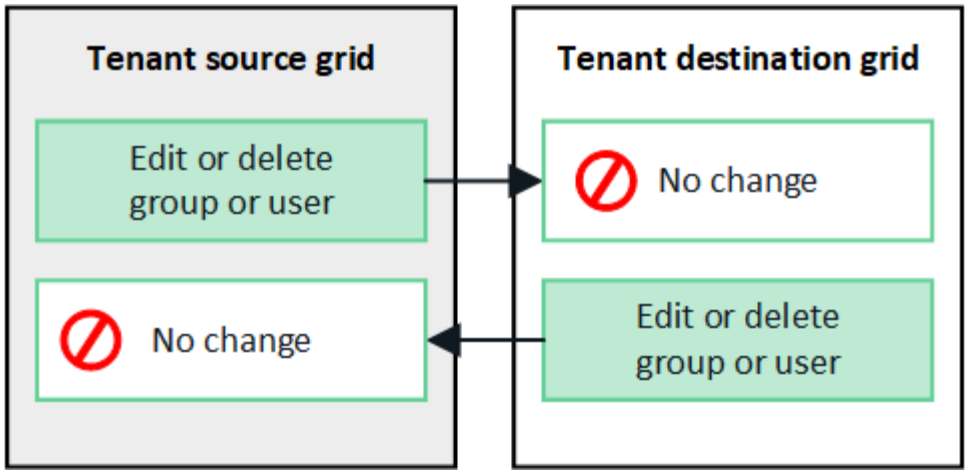
La clonación se produce únicamente desde la red de origen del inquilino a la red de destino del inquilino. Si crea o importa grupos y usuarios en la cuadrícula de destino del inquilino, StorageGRID no clonará estos elementos en la cuadrícula de origen del inquilino.



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

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

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



Clonar claves de acceso S3 usando la API

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

Antes de empezar

- La cuenta de inquilino tiene el permiso **Usar conexión de federación de red**.
- La conexión de la federación de red tiene un **Estado de conexión** de **Conectado**.
- Ha iniciado sesión en el Administrador de inquilinos en la cuadrícula de origen del inquilino mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Administre sus propias credenciales S3 o permiso de acceso root" .
- Si está clonando claves de acceso para un usuario local, el usuario ya existe en ambas cuadrículas.

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

Clona tus propias claves de acceso

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

Pasos

1. Usando el Administrador de inquilinos en la red de origen,"crea tus propias claves de acceso" y descargar el `.csv` archivo.
2. Desde la parte superior del Administrador de inquilinos, seleccione el ícono de ayuda y seleccione **Documentación de API**.
3. En la sección **s3**, seleccione el siguiente punto final:

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

4. Seleccione **Probarlo**.
5. En el cuadro de texto **body**, reemplace las entradas de ejemplo para **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 caducará, reemplace la entrada de ejemplo para **expires** con la fecha y hora de caducidad como una cadena en formato de datos y tiempo ISO 8601 (por ejemplo, `2024-02-28T22:46:33-08:00`). Si la clave no caducará, ingrese **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 red 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.

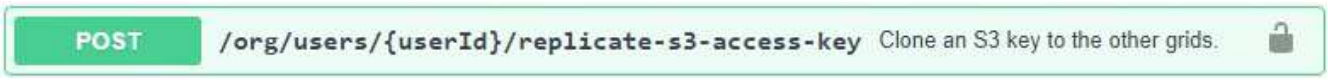
Pasos

1. Usando el Administrador de inquilinos en la red de origen,"crear las claves de acceso S3 del otro usuario" y descargar el `.csv` archivo.
2. Desde la parte superior del Administrador de inquilinos, seleccione el ícono de ayuda y seleccione **Documentación de API**.
3. Obtener el ID del usuario. Necesitará este valor para clonar las claves de acceso del otro usuario.
   a. Desde la sección **usuarios**, seleccione el siguiente punto final:

      `GET /org/users`

   b. Seleccione **Probarlo**.
   c. Especifique cualquier parámetro 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 **Probarlo**.
6. En el cuadro de texto **userId**, pegue el ID de usuario que copió.
7. En el cuadro de texto **body**, reemplace las entradas de ejemplo para **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.

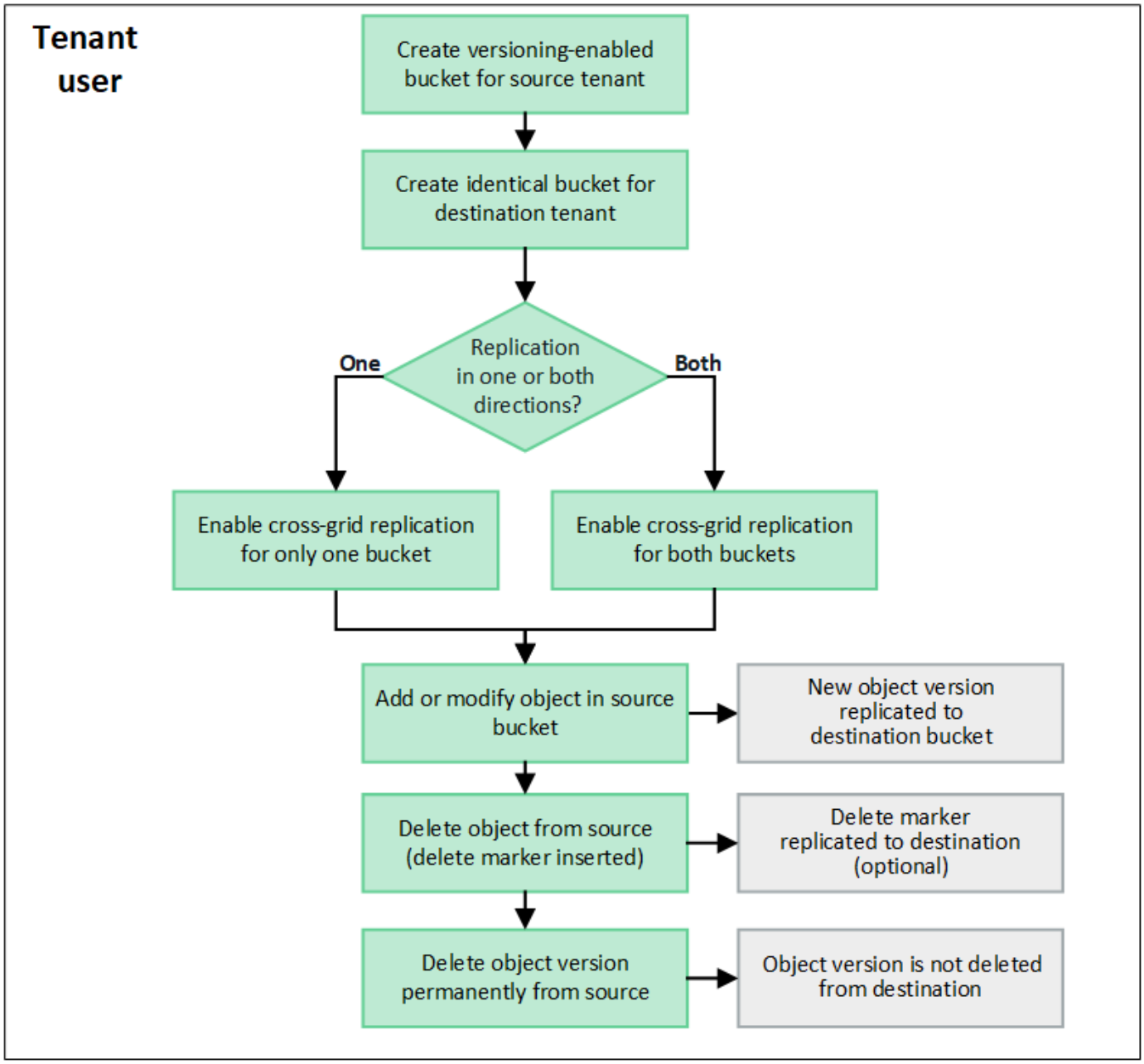
8. Si la clave caducará, reemplace la entrada de ejemplo para **expires** con la fecha y hora de caducidad como una cadena en formato de datos y tiempo ISO 8601 (por ejemplo, `2023-02-28T22:46:33-08:00`). Si la clave no caducará, ingrese **null** como valor para la entrada **expires** (o elimine la línea **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 red de destino.

Administrar la replicación entre redes

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

Flujo de trabajo para la replicación entre redes

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



Configurar la replicación entre redes

Antes de poder utilizar la replicación entre redes, debe iniciar sesión en las cuentas de inquilino correspondientes en cada red y crear grupos idénticos. Luego, puedes habilitar la replicación entre redes en uno o ambos depósitos.

Antes de empezar

- Ha revisado los requisitos para la replicación entre redes. Ver "¿Qué es la replicación entre redes?" .
- Estás usando un"navegador web compatible" .
- La cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y existen cuentas de inquilino idénticas en ambas redes. Ver "Administrar los inquilinos permitidos para la conexión de la federación de red" .
- El usuario inquilino con el que iniciará sesión ya existe en ambas redes y pertenece a un grupo de usuarios que tiene la"Permiso de acceso root" .

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

Crea dos cubos idénticos

Como primer paso, inicie sesión en las cuentas de inquilino correspondientes en cada red y cree grupos idénticos.

Pasos

1. A partir de cualquiera de las cuadrículas en la conexión de la federación de cuadrículas, cree un nuevo depósito:
   a. Sign in en la cuenta del inquilino utilizando las credenciales de un usuario inquilino que exista en ambas redes.

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

   b. Siga las instrucciones para"crear un bucket S3" .
   c. En la pestaña **Administrar configuración de objetos**, seleccione **Habilitar control de versiones de objetos**.
   d. Si el Bloqueo de objetos S3 está habilitado para su sistema StorageGRID , no habilite el Bloqueo de objetos S3 para el depósito.
   e. Seleccione **Crear depósito**.
   f. Seleccione **Finalizar**.
2. Repita estos pasos para crear un depósito idéntico para la misma cuenta de inquilino en la otra red en la conexión de federación de red.

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

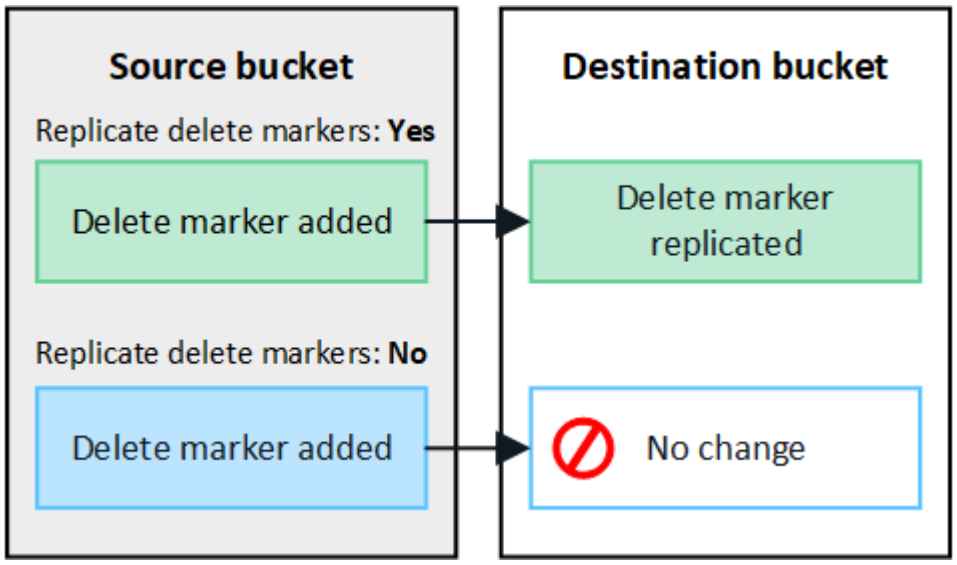
Habilitar la replicación entre redes

Debes realizar estos pasos antes de agregar cualquier objeto a cualquiera de los depósitos.

Pasos

1. A partir de una cuadrícula cuyos objetos desea replicar, habilite"replicación entre redes en una dirección" :
   a. Sign in en la cuenta de inquilino del depósito.
   b. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
   c. Seleccione el nombre del depósito de la tabla para acceder a la página de detalles del depósito.
   d. Seleccione la pestaña **Replicación entre cuadrículas**.
   e. Seleccione **Habilitar** y revise la lista de requisitos.
   f. Si se cumplen todos los requisitos, seleccione la conexión de federación de red que desea utilizar.
   g. De manera opcional, 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** (predeterminado): se agrega un marcador de eliminación al depósito de origen y se replica en el depósito de destino.
- **No**: Se agrega un marcador de eliminación al depósito de origen, pero no se replica en el depósito de destino.



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

Ver"¿Qué es la replicación entre redes?" Para más detalles.

a. De manera opcional, cambie la configuración de la categoría de auditoría **Replicación entre redes** para administrar el volumen de mensajes de auditoría:
   - **Error** (predeterminado): solo las solicitudes de replicación entre redes fallidas se incluyen en la salida de auditoría.
   - **Normal**: Se incluyen todas las solicitudes de replicación entre redes, lo que aumenta significativamente el volumen de la salida de auditoría.
b. Revise sus selecciones. No podrás cambiar estas configuraciones a menos que ambos depósitos 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 entre redes** se muestra como una función habilitada en la página de detalles del depósito.

2. Opcionalmente, vaya al bucket correspondiente en la otra cuadrícula y"Permitir la replicación entre redes en ambas direcciones" .

Prueba de replicación entre redes

Si la replicación entre redes está habilitada para un depósito, es posible que deba verificar que la conexión y la replicación entre redes funcionen correctamente y que los depósitos de origen y destino aún cumplan con todos los requisitos (por ejemplo, el control de versiones aún esté habilitado).

Antes de empezar

- Estás usando un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" .

Pasos

1. Sign in en la cuenta de inquilino del depósito.
2. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
3. Seleccione el nombre del depósito de la tabla para acceder a la página de detalles del depósito.
4. Seleccione la pestaña **Replicación entre cuadrículas**.
5. Seleccione **Probar conexión**.

   Si la conexión es saludable, aparece un banner de éxito. De lo contrario, aparecerá un mensaje de error que usted y el administrador de la red pueden utilizar para resolver el problema. Para obtener más información, consulte "Solucionar errores de federación de red" .

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

Deshabilitar la replicación entre redes

Puede detener permanentemente la replicación entre cuadrículas si ya no desea copiar objetos a la otra cuadrícula.

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

- Deshabilitar la replicación entre cuadrículas no elimina ningún objeto que ya se haya copiado entre cuadrículas. Por ejemplo, los objetos en `my-bucket` en la cuadrícula 1 que se han copiado a `my-bucket` en Grid 2 no se eliminan si deshabilita la replicación entre redes para ese depósito. Si desea eliminar estos objetos, deberá eliminarlos manualmente.
- Si se habilitó la replicación entre redes para cada uno de los buckets (es decir, si la replicación ocurre en ambas direcciones), puede deshabilitar la replicación entre redes para uno o ambos buckets. Por ejemplo, es posible que desee deshabilitar la replicación de objetos desde `my-bucket` en la cuadrícula 1 a `my-bucket` en la cuadrícula 2, mientras continúa replicando objetos desde `my-bucket` en la red 2 a `my-bucket` en la cuadrícula 1.
- Debe deshabilitar la replicación entre redes antes de poder quitar el permiso de un inquilino para usar la conexión de federación de red. Ver "Gestionar inquilinos permitidos" .
- Si deshabilita la replicación entre cuadrículas para un depósito que contiene objetos, no podrá volver a habilitarla a menos que elimine todos los objetos de los depósitos de origen y destino.

  No se puede volver a habilitar la replicación a menos que ambos depósitos estén vacíos.

Antes de empezar

- Estás usando un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" .

Pasos

1. A partir de la cuadrícula cuyos objetos ya no desea replicar, detenga la replicación entre cuadrículas para el depósito:

a. Sign in en la cuenta de inquilino del depósito.
b. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
c. Seleccione el nombre del depósito de la tabla para acceder a la página de detalles del depósito.
d. Seleccione la pestaña **Replicación entre cuadrículas**.
e. Seleccione **Deshabilitar replicación**.
f. Si está seguro de que desea deshabilitar la replicación entre redes para este bucket, escriba **Sí** en el cuadro de texto y seleccione **Deshabilitar**.

   Después de unos momentos, aparece un mensaje de éxito. Los nuevos objetos agregados a este depósito ya no se pueden replicar automáticamente en la otra cuadrícula. **La replicación entre cuadrículas** ya no se muestra como una función habilitada en la página de Cubos.

2. Si la replicación entre redes se configuró para que ocurriera en ambas direcciones, vaya al depósito correspondiente en la otra red y detenga la replicación entre redes en la otra dirección.

Ver las conexiones de la federación de red

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

Antes de empezar

- La cuenta de inquilino tiene el permiso **Usar conexión de federación de red**.
- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" .

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Conexiones de federación de red**.

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

Columna	Descripción
Nombre de la conexión	Las conexiones de la federación de red que este inquilino tiene permiso para utilizar.
Cubos con replicación entre redes	Para cada conexión de federación de red, los grupos de inquilinos que tienen habilitada la replicación entre redes. Los objetos agregados a estos depósitos se replicarán en la otra cuadrícula de la conexión.
Último error	Para cada conexión de federación de red, el error más reciente que ocurrió, si lo hubo, cuando se replicaron los datos a la otra red. Ver Borrar el último error .

2. Opcionalmente, seleccione un nombre de depósito para"ver detalles del depósito" .

Borrar el último error

Podría aparecer un error en la columna **Último error** por uno de estos motivos:

- No se encontró la versión del objeto de origen.
- No se encontró el depósito de origen.
- Se eliminó el depósito de destino.
- El depósito de destino fue recreado por una cuenta diferente.
- El bucket de destino tiene la versión suspendida.
- El depósito de destino fue recreado por la misma cuenta pero ahora no tiene versión.

> Esta columna solo muestra el último error de replicación entre redes que ocurrió; no se mostrarán los errores anteriores que pudieran haber ocurrido.

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 redes estaba en un estado no válido, posiblemente porque se suspendió el control de versiones o se habilitó el bloqueo de objetos S3.

2. Realice cualquier acción recomendada. Por ejemplo, si se suspendió el control de versiones en el depósito de destino para la replicación entre redes, vuelva a habilitar el control de versiones para ese depósito.
3. Seleccione la conexión de la tabla.
4. Seleccione **Borrar error**.
5. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espere 5-6 minutos y luego ingiera un nuevo objeto en el balde. Confirme que el mensaje de error no vuelva a aparecer.

   > Para garantizar que se borre el mensaje de error, espere al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingerir un nuevo objeto.

7. Para determinar si algún objeto no se pudo replicar debido al error del depósito, consulte"Identificar y reintentar operaciones de replicación fallidas" .

Administrar grupos y usuarios

Utilizar la federación de identidades

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

Configurar la federación de identidades para Tenant Manager

Puede configurar la federación de identidad para el Administrador de inquilinos si desea que los grupos de inquilinos y los usuarios se administren en otro sistema, como Active Directory, Azure Active Directory (Azure

AD), OpenLDAP u Oracle Directory Server.

Antes de empezar

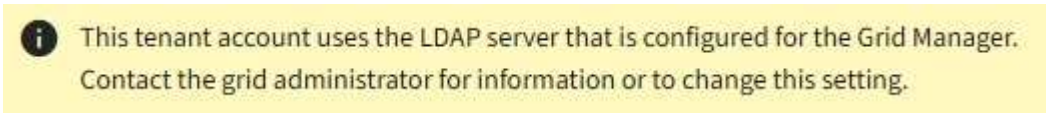
- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" .
- Está utilizando Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidad.

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

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Ver Directrices para configurar el servidor OpenLDAP .
- Si planea utilizar Seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidad debe utilizar TLS 1.2 o 1.3. Ver "Cifrados compatibles para conexiones TLS salientes" .

Acerca de esta tarea

La posibilidad de configurar un servicio de federación de identidad para su inquilino depende de cómo se configuró su cuenta de inquilino. Es posible que su inquilino comparta el servicio de federación de identidad que se configuró para Grid Manager. Si ve este mensaje cuando accede a la página Federación de identidad, no puede configurar una fuente de identidad federada separada para este inquilino.

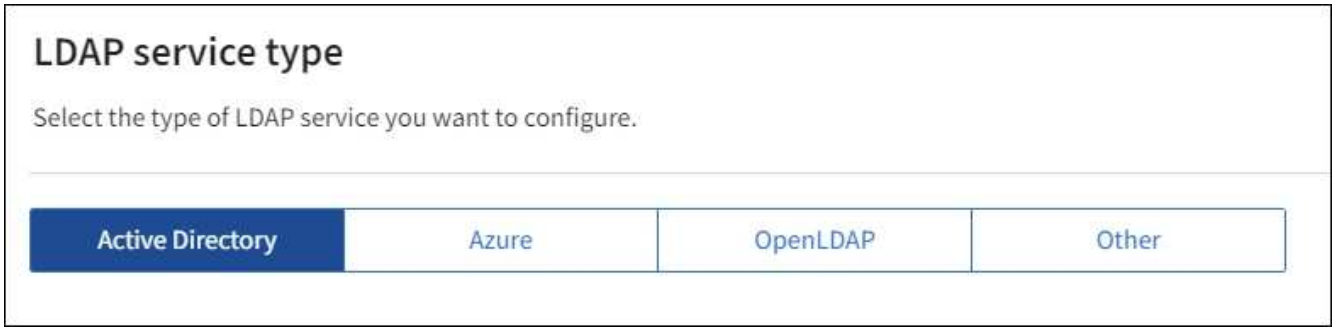


Ingresar configuración

Cuando configura la federación de identidad, proporciona los valores que StorageGRID necesita para conectarse a un servicio LDAP.

Pasos

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



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

4. Si seleccionó **Otro**, complete los campos en la sección Atributos LDAP. De lo contrario, vaya al siguiente paso.

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

5. Para todos los tipos de servicios LDAP, ingrese la información de conexión de red y servidor LDAP requerida en la sección Configurar servidor LDAP.
   - **Nombre de host**: el nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
   - **Puerto**: El puerto utilizado para conectarse al servidor LDAP.

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

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

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

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

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

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

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

   - **DN base de grupo**: la ruta completa del nombre distinguido (DN) de un subárbol LDAP en el que desea buscar grupos. En el ejemplo de Active Directory (abajo), todos los grupos cuyo nombre

distintivo es relativo al DN base (DC=storagegrid,DC=example,DC=com) se pueden usar como grupos federados.

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

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

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

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

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

  Introduzca uno de estos patrones:

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

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

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

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

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

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

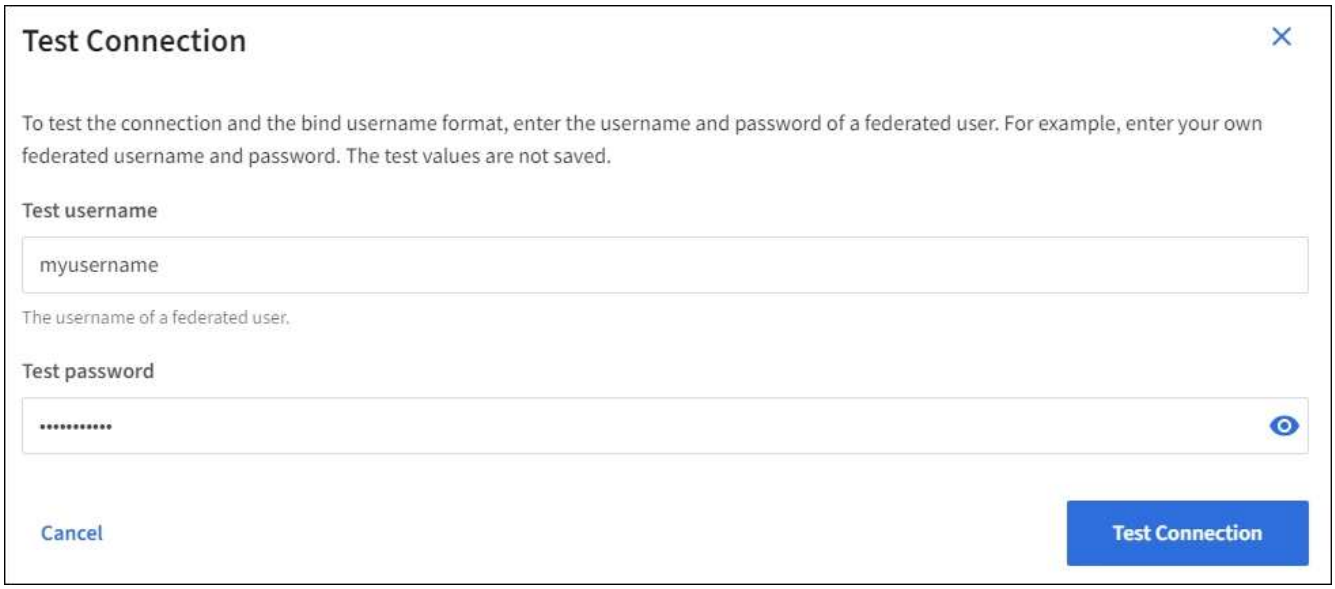
Pruebe la conexión y guarde la configuración

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

Pasos

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

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



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

Forzar la sincronización con la fuente de identidad

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

Pasos

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

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

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

Deshabilitar la federación de identidades

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

Acerca de esta tarea

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

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

Pasos

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

Directrices para configurar el servidor OpenLDAP

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

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

Superposiciones de miembros y refinaciones

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

Indexación

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

- `olcDbIndex: objectClass eq`

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

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

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

Administrar grupos de inquilinos

Crear grupos para un inquilino de S3

Puede administrar permisos para grupos de usuarios de S3 importando grupos federados o creando grupos locales.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" .
- Si planea importar un grupo federado, debe"federación de identidad configurada" , y el grupo federado ya existe en la fuente de identidad configurada.
- Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, ha revisado el flujo de trabajo y las consideraciones para"Clonación de grupos de inquilinos y usuarios" , y ha iniciado sesión en la red de origen del inquilino.

Acceder al asistente para crear grupos

Como primer paso, acceda al asistente para crear grupos.

Pasos

1. Seleccione **GESTIÓN DE ACCESO** > **Grupos**.
2. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, confirme que aparece un banner azul que indica que los nuevos grupos creados en esta red se clonarán en el mismo inquilino en la otra red de la conexión. Si este banner no aparece, es posible 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 pestaña **Grupo local** para crear un grupo local, o seleccione la pestaña **Grupo federado** para importar un grupo desde la fuente de identidad configurada previamente.

   Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID , los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Administrador de inquilinos, aunque podrán usar aplicaciones cliente para administrar los recursos del inquilino, según los permisos del grupo.

2. Introduzca el nombre del grupo.
   - **Grupo local**: Ingrese un nombre para mostrar y un nombre único. Podrás editar el nombre para mostrar más tarde.

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

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

Administrar permisos de grupo

Los permisos de grupo controlan qué tareas pueden realizar los usuarios en el Administrador de inquilinos y la API de administración de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:
   - **Lectura y escritura** (predeterminado): los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.

- **Solo lectura**: los usuarios solo pueden ver configuraciones y funciones. No pueden realizar ningún cambio ni realizar ninguna operación en el Administrador de inquilinos ni en la API de administración de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

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

2. Seleccione uno o más permisos para este grupo.

   Ver "Permisos de gestión de inquilinos" .

3. Seleccione **Continuar**.

Establecer la política de grupo de S3

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

Pasos

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

Política de grupo	Descripción
Sin acceso a S3	Por defecto. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se les conceda acceso con una política de bucket. Si selecciona esta opción, solo el usuario root tendrá acceso a los recursos de S3 de forma predeterminada.
Acceso de solo 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 puedes editar esta cadena.
Acceso completo	Los usuarios de este grupo tienen acceso completo a los recursos de S3, incluidos los buckets. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puedes editar esta cadena.
Mitigación de 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 eliminar de forma permanente objetos de los depósitos que tienen habilitada la versión de objetos. Los usuarios del administrador de inquilinos que tienen el permiso **Administrar todos los depósitos** pueden anular esta política de grupo. Limite el permiso Administrar todos los depósitos a usuarios de confianza y utilice la autenticación multifactor (MFA) cuando esté disponible.

Política de grupo	Descripción
Costumbre	A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

2. Si seleccionó **Personalizado**, ingrese la política de grupo. Cada política de grupo tiene un límite de tamaño de 5120 bytes. Debe ingresar una cadena con formato JSON válida.

   Para obtener información detallada sobre las políticas de grupo, incluida la sintaxis del lenguaje y ejemplos, consulte"Políticas de grupo de ejemplo" .

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

Agregar usuarios (solo grupos locales)

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 red**, cualquier usuario que seleccione al crear un grupo local en la red de origen no se incluirá cuando el grupo se clone en la red 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 más usuarios locales para este grupo.
2. Seleccione **Crear grupo** y **Finalizar**.

   El grupo que usted creó aparece en la lista de grupos.

   Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y usted está en la red de origen del inquilino, el nuevo grupo se clona en la red de destino del inquilino. **Éxito** aparece como **Estado de clonación** en la sección Descripción general de la página de detalles del grupo.

Crear grupos para un inquilino de Swift

Puede administrar los permisos de acceso para una cuenta de inquilino de Swift importando grupos federados o creando grupos locales. Al menos un grupo debe tener el permiso de administrador de Swift, que es necesario para administrar los contenedores y objetos de una cuenta de inquilino de Swift.

> La compatibilidad con aplicaciones cliente Swift ha quedado obsoleta y se eliminará en una versión futura.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" .
- Si planea importar un grupo federado, debe"federación de identidad configurada" , y el grupo federado ya existe en la fuente de identidad configurada.

Acceder al asistente para crear grupos

Pasos

Como primer paso, acceda al asistente para crear grupos.

1. Seleccione **GESTIÓN 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 pestaña **Grupo local** para crear un grupo local, o seleccione la pestaña **Grupo federado** para importar un grupo desde la fuente de identidad configurada previamente.

   Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID , los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Administrador de inquilinos, aunque podrán usar aplicaciones cliente para administrar los recursos del inquilino, según los permisos del grupo.

2. Introduzca el nombre del grupo.
   - **Grupo local**: Ingrese un nombre para mostrar y un nombre único. Podrás editar el nombre para mostrar más tarde.
   - **Grupo federado**: Ingrese el nombre único. Para Active Directory, el nombre único es el nombre asociado con el `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con el `uid` atributo.
3. Seleccione **Continuar**.

Administrar permisos de grupo

Los permisos de grupo controlan qué tareas pueden realizar los usuarios en el Administrador de inquilinos y la API de administración de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:
   - **Lectura y escritura** (predeterminado): los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.
   - **Solo lectura**: los usuarios solo pueden ver configuraciones y funciones. No pueden realizar ningún cambio ni realizar ninguna operación en el Administrador de inquilinos ni en la API de administración de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

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

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**.

Establecer 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 **Administrador de Swift** 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**.

Agregar usuarios (solo 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 más usuarios locales para este grupo.

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

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

   El grupo que usted creó aparece en la lista de grupos.

Permisos de gestión de inquilinos

Antes de crear un grupo de inquilinos, considere qué permisos desea asignar a ese grupo. Los permisos de administración de inquilinos determinan qué tareas pueden realizar los usuarios mediante el Administrador de inquilinos o la API de administración 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 inquilinos o utilizar la API de administración de inquilinos, los usuarios deben pertenecer a un grupo que tenga al menos un permiso. Todos los usuarios que puedan iniciar sesión podrán realizar las siguientes tareas:

- Ver el panel de control
- 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 configuraciones y realizar operaciones o si solo pueden ver las configuraciones y funciones relacionadas.

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

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 root	Proporciona acceso completo al Administrador de inquilinos y a la API de administración de inquilinos.	Los usuarios de Swift deben tener permiso de acceso de root para iniciar sesión en la cuenta del inquilino.
Administrador	Solo inquilinos rápidos. Proporciona acceso completo a los contenedores y objetos Swift para esta cuenta de inquilino	Los usuarios de Swift deben tener permiso de administrador de Swift para realizar cualquier operación con la API REST de Swift.
Administre sus propias credenciales 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 **ALMACENAMIENTO (S3)** > **Mis claves de acceso S3**.
Ver todos los buckets	**Inquilinos de S3**: permite a los usuarios ver todos los depósitos y sus configuraciones. **Inquilinos de Swift**: permite a los usuarios de Swift ver todos los contenedores y configuraciones de contenedores mediante la API de administración de inquilinos.	Los usuarios que no tienen el permiso Ver todos los depósitos o Administrar todos los depósitos no ven la opción de menú **Cubos**. Este permiso es reemplazado por el permiso Administrar todos los depósitos. No afecta las políticas de grupo o bucket S3 utilizadas por los clientes S3 o la consola S3. Solo puede asignar este permiso a grupos Swift desde la API de administración de inquilinos. No puedes asignar este permiso a grupos Swift mediante el Administrador de inquilinos.
Administrar todos los depósitos	**Inquilinos de S3**: permite a los usuarios usar el Administrador de inquilinos y la API de administración de inquilinos para crear y eliminar depósitos S3 y administrar las configuraciones de todos los depósitos S3 en la cuenta del inquilino, independientemente de las políticas de grupo o depósito S3. **Inquilinos de Swift**: permite a los usuarios de Swift controlar la consistencia de los contenedores de Swift mediante la API de administración de inquilinos.	Los usuarios que no tienen el permiso Ver todos los depósitos o Administrar todos los depósitos no ven la opción de menú **Cubos**. Este permiso reemplaza al permiso Ver todos los depósitos. No afecta las políticas de grupo o bucket S3 utilizadas por los clientes S3 o la consola S3. Solo puede asignar este permiso a grupos Swift desde la API de administración de inquilinos. No puedes asignar este permiso a grupos Swift mediante el Administrador de inquilinos.
Administrar puntos finales	Permite a los usuarios utilizar el Administrador de inquilinos o la API de administración de inquilinos para crear o editar puntos finales de servicio de la plataforma, que se utilizan como destino para los servicios de la plataforma StorageGRID .	Los usuarios que no tienen este permiso no ven la opción de menú **Puntos finales de servicios de la plataforma**.

Permiso	Descripción	Detalles
Usar la pestaña Consola S3	Cuando se combina con el permiso Ver todos los depósitos o Administrar todos los depósitos, permite a los usuarios ver y administrar objetos desde la pestaña de la Consola S3 en la página de detalles de un depósito.	

Administrar grupos

Administre sus grupos de inquilinos según sea necesario para ver, editar o duplicar un grupo y más.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" .

Ver o editar grupo

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

Pasos

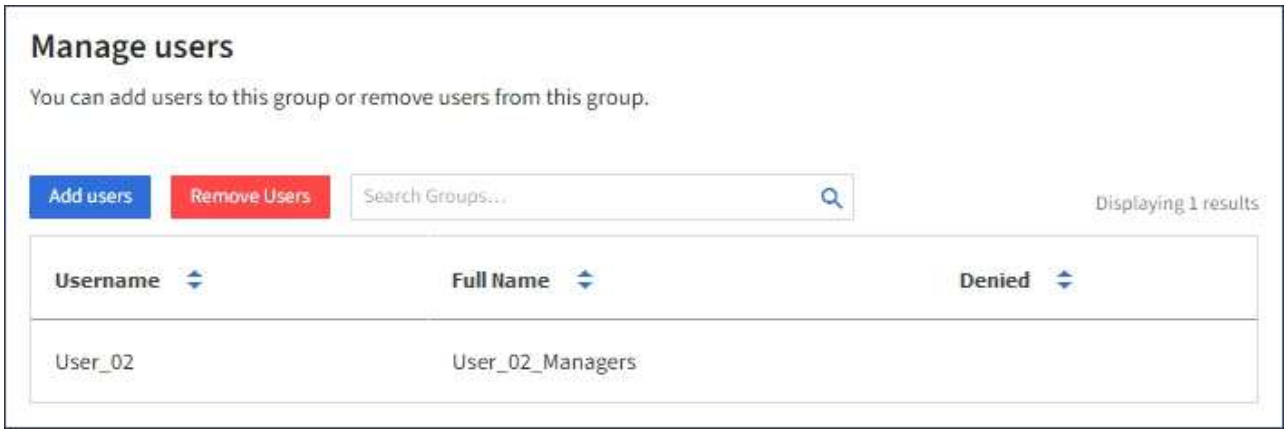
1. Seleccione **GESTIÓN DE ACCESO** > **Grupos**.
2. Revise la información proporcionada en la página Grupos, que enumera información básica de todos los grupos locales y federados para esta cuenta de inquilino.

   Si la cuenta del inquilino tiene el permiso **Usar conexión de federación de red** y está viendo grupos en la red de origen del inquilino:

   - Un mensaje de banner indica que si edita o elimina un grupo, sus 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 red de destino. Puedereintentar una clonación de grupo Eso falló.
3. Si desea cambiar el nombre del grupo:
   a. Seleccione la casilla de verificación del grupo.
   b. Seleccione **Acciones** > **Editar nombre del grupo**.
   c. Introduzca el nuevo nombre.
   d. Seleccione **Guardar cambios.**
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre del grupo.
   - Seleccione la casilla de verificación del grupo y seleccione **Acciones** > **Ver detalles del grupo**.
5. Revise la sección Descripción general, que muestra la siguiente información para cada grupo:
   - Nombre para mostrar
   - Nombre único
   - Tipo

- Modo de acceso
- Permisos
- Política S3
- Número de usuarios en este grupo
- Campos adicionales si la cuenta del inquilino tiene el permiso **Usar conexión de federación de red** y está viendo el grupo en la red de origen del inquilino:
  - Estado de clonación: **Éxito** o **Fracaso**
  - Un banner azul que indica que si edita o elimina este grupo, sus cambios no se sincronizarán con la otra cuadrícula.

6. Edite la configuración del grupo según sea necesario. Ver"Crear grupos para un inquilino de S3" y"Crear grupos para un inquilino de Swift" para obtener detalles sobre qué ingresar.
   a. En la sección Descripción general, cambie el nombre para mostrar seleccionando el nombre o el ícono 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 necesarios y seleccione **Guardar cambios**.
      - Si está editando un grupo S3, opcionalmente seleccione una política de grupo S3 diferente o ingrese la cadena JSON para una política personalizada, según sea necesario.
      - Si está editando un grupo Swift, opcionalmente seleccione o desmarque la casilla de verificación **Administrador Swift**.
7. Para agregar uno o más usuarios locales existentes al grupo:
   a. Seleccione la pestaña Usuarios.



   b. Seleccione **Agregar 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 pestaña Usuarios.
   b. Seleccione **Eliminar usuarios**.
   c. Seleccione los usuarios que desea eliminar y seleccione **Eliminar usuarios**.

      Aparece un mensaje de éxito en la parte superior derecha.

9. Confirme que ha seleccionado **Guardar cambios** para cada sección que haya modificado.

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 red** y duplica un grupo de la red de origen del inquilino, el grupo duplicado se clonará en la red de destino del inquilino.

Pasos

1. Seleccione **GESTIÓN DE ACCESO** > **Grupos**.
2. Seleccione la casilla de verificación del grupo que desea duplicar.
3. Seleccione **Acciones** > **Duplicar grupo**.
4. Ver"Crear grupos para un inquilino de S3" o"Crear grupos para un inquilino de Swift" para obtener detalles sobre qué ingresar.
5. Seleccione **Crear grupo**.

[[grupos de clones]]Reintentar clonar grupo

Para volver a intentar una clonación que falló:

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

Para obtener información adicional, consulte"Clonar grupos de inquilinos y usuarios" .

Eliminar uno o más grupos

Puedes eliminar uno o más grupos. Cualquier usuario que pertenezca únicamente a un grupo eliminado ya no podrá iniciar sesión en el Administrador de inquilinos ni usar la cuenta de inquilino.

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

Pasos

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

   Aparece un cuadro de diálogo de confirmación.

4. Seleccione **Eliminar grupo** o **Eliminar grupos**.

Administrar usuarios locales

Puede crear usuarios locales y asignarlos a grupos locales para determinar a qué

funciones pueden acceder estos usuarios. El administrador de inquilinos incluye un usuario local predefinido, llamado "root". Aunque puedes agregar y eliminar usuarios locales, no puedes eliminar el usuario root.

> Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID , los usuarios locales no podrán iniciar sesión en el Administrador de inquilinos ni en la API de administración de inquilinos, aunque podrán usar 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" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" .
- Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, ha revisado el flujo de trabajo y las consideraciones para"Clonación de grupos de inquilinos y usuarios" , y ha iniciado sesión en la red de origen del inquilino.

Crear un usuario local

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

Los usuarios de S3 que no pertenecen a ningún grupo no tienen permisos de administración ni políticas de grupo de S3 aplicadas a ellos. A estos usuarios se les podría otorgar acceso al bucket S3 a través de una política de bucket.

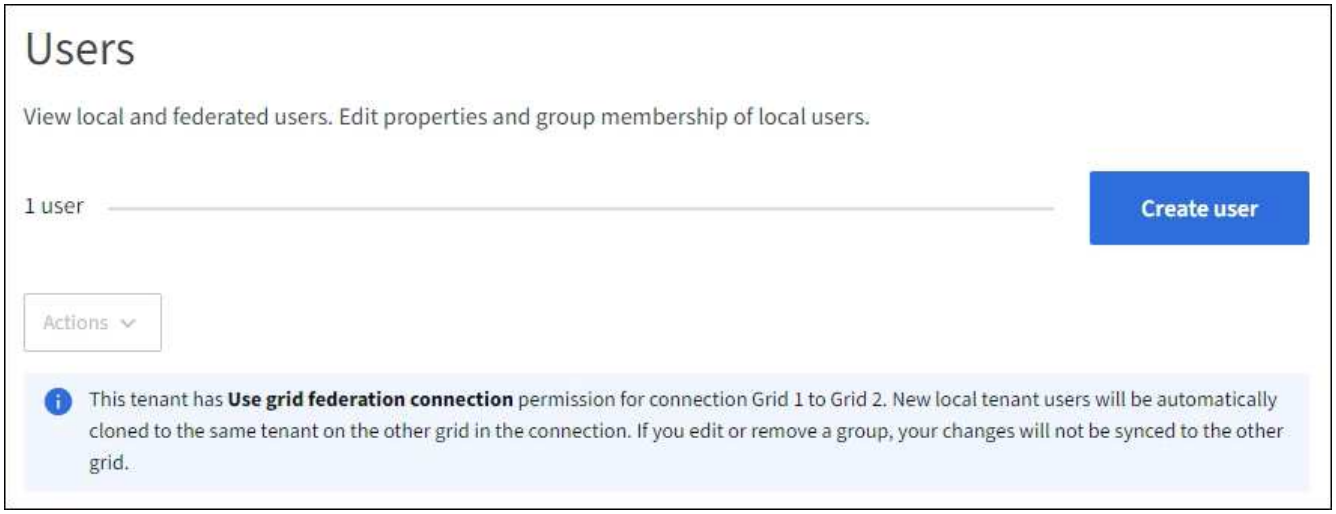
Los usuarios de Swift que no pertenecen a ningún grupo no tienen permisos de administración ni acceso al contenedor Swift.

Acceder al asistente para crear usuarios

Pasos

1. Seleccione **GESTIÓN DE ACCESO** > **Usuarios**.

   Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, un banner azul indica que esta es la red de origen del inquilino. Cualquier usuario local que cree en esta red se clonará en la otra red de la conexión.



2. Seleccione **Crear usuario**.

Ingresar credenciales

Pasos

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

Campo	Descripción
Nombre completo	El nombre completo de este usuario, por ejemplo, el nombre y apellido de una persona o el nombre de una aplicación.
Nombre de usuario	El nombre que este usuario usará 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 red**, se producirá un error de clonación si ya existe el mismo **Nombre de usuario** para el inquilino en la red de destino.
Contraseña y Confirmar 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, incluso si aún pertenece a uno o más grupos. Por ejemplo, seleccione **Sí** para suspender temporalmente la capacidad de un usuario de iniciar sesión.

2. Seleccione **Continuar**.

Asignar a grupos

Pasos

1. Asigne el usuario a uno o más grupos locales para determinar qué tareas puede 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 pertenecen 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 pertenecen. Ver "Permisos de gestión de inquilinos" .

2. Seleccione **Crear usuario**.

   Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y usted está en la red de origen del inquilino, el nuevo usuario local se clona en la red de destino del inquilino. **Éxito** aparece como **Estado de clonación** en la sección Descripción general de la página de detalles del usuario.

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

Ver o editar usuario local

Pasos

1. Seleccione **GESTIÓN DE ACCESO** > **Usuarios**.
2. Revise la información proporcionada en la página Usuarios, que enumera información básica de todos los usuarios locales y federados para esta cuenta de inquilino.

   Si la cuenta del inquilino tiene el permiso **Usar conexión de federación de red** y está viendo al usuario en la red de origen del inquilino:

   - Un mensaje de banner indica que si edita o elimina un usuario, sus cambios no se sincronizarán con la otra cuadrícula.
   - Según sea necesario, un mensaje de banner indica si los usuarios no fueron clonados al inquilino en la red de destino. Puede Reintentar una clonación de usuario que falló Es
3. Si desea cambiar el nombre completo del usuario:
   a. Seleccione la casilla de verificación para el usuario.
   b. Seleccione **Acciones** > **Editar nombre completo**.
   c. Introduzca el nuevo nombre.
   d. Seleccione **Guardar cambios.**
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre de usuario.
   - Seleccione la casilla de verificación del usuario y seleccione **Acciones** > **Ver detalles del usuario**.
5. Revise la sección Descripción general, que muestra la siguiente información para cada usuario:
   - Nombre completo
   - Nombre de usuario
   - Tipo de usuario
   - Acceso denegado
   - Modo de acceso
   - Membresía grupal
   - Campos adicionales si la cuenta del inquilino tiene el permiso **Usar conexión de federación de red** y está viendo al usuario en la red de origen del inquilino:
     - Estado de clonación: **Éxito** o **Fracaso**
     - Un banner azul que indica que si edita este usuario, sus cambios no se sincronizarán con la otra cuadrícula.
6. Edite la configuración del usuario según sea necesario. VerCrear usuario local para obtener detalles sobre qué ingresar.
   a. En la sección Descripción general, cambie el nombre completo seleccionando el nombre o el ícono de edición .

      No puedes cambiar el nombre de usuario.

   b. En la pestaña **Contraseña**, cambie la contraseña del usuario y seleccione **Guardar cambios**.
   c. En la pestaña **Acceso**, seleccione **No** para permitir que el usuario inicie sesión o seleccione **Sí** para evitar que el usuario inicie sesión. Luego, seleccione **Guardar cambios**.

d. En la pestaña **Teclas de acceso**, seleccione **Crear clave** y siga las instrucciones para"creando las claves de acceso S3 de otro usuario" .

e. En la pestaña **Grupos**, seleccione **Editar grupos** para agregar el usuario a grupos o eliminarlo de grupos. Luego, seleccione **Guardar cambios**.

7. Confirme que ha seleccionado **Guardar cambios** para cada sección que haya modificado.

Usuario local duplicado

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

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

Pasos

1. Seleccione **GESTIÓN DE ACCESO** > **Usuarios**.
2. Seleccione la casilla de verificación del usuario que desea duplicar.
3. Seleccione **Acciones** > **Duplicar usuario**.
4. VerCrear usuario local para obtener detalles sobre qué ingresar.
5. Seleccione **Crear usuario**.

Reintentar clonar usuario

Para volver a intentar una clonación que falló:

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

Para obtener información adicional, consulte"Clonar grupos de inquilinos y usuarios" .

Eliminar uno o más usuarios locales

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

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y elimina un usuario local, StorageGRID no eliminará el usuario correspondiente en la otra red. Si necesita mantener esta información sincronizada, debe eliminar el mismo usuario de ambas cuadrículas.

> Debe utilizar la fuente de identidad federada para eliminar usuarios federados.

Pasos

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

Aparece un cuadro de diálogo de confirmación.

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

Administrar claves de acceso S3

Administrar claves de acceso S3

Cada usuario de una cuenta de inquilino 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 S3** pueden crear o eliminar sus propias claves de acceso S3.
- Los usuarios que tienen permiso de **acceso root** pueden administrar las claves de acceso para la cuenta raíz S3 y todos los demás usuarios. Las claves de acceso raíz brindan acceso completo a todos los depósitos y objetos para el inquilino, a menos que una política de depósito los deshabilite explícitamente.

StorageGRID admite la autenticación Signature Version 2 y Signature Version 4. No se permite el acceso entre cuentas a menos que lo habilite explícitamente una política de bucket.

Crea tus propias claves de acceso S3

Si está utilizando un inquilino S3 y tiene el permiso adecuado, puede crear sus propias claves de acceso S3. Debe tener una clave de acceso para acceder a sus depósitos y objetos.

Antes de empezar

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

Acerca de esta tarea

Puede crear una o más claves de acceso S3 que le permitan crear y administrar depósitos para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con su nueva ID de clave de acceso y su clave de acceso secreta. Por seguridad, no cree más claves de las que necesita y elimine las claves que no esté utilizando. Si solo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la anterior y luego elimínela.

Cada clave puede tener un tiempo de expiración específico o no tener expiración. Siga estas pautas para el tiempo de vencimiento:

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

Se puede acceder a los depósitos y objetos S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de su cuenta y nunca las comparta con otros usuarios.

Pasos

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

   Aparece la página Mis claves de acceso y enumera todas las claves de acceso existentes.

2. Seleccione **Crear clave**.
3. Debe realizar una de las siguientes acciones:
   - Seleccione **No establecer un tiempo de expiración** para crear una clave que no caduque. (Por defecto)
   - Seleccione **Establecer una hora de vencimiento** y configure la fecha y hora de vencimiento.

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

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

   Aparece el cuadro de diálogo Descargar clave de acceso, que incluye el ID de su clave de acceso y su 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 la clave de acceso y la clave de acceso secreta.

   No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No es posible copiar ni descargar claves una vez cerrado 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 red**, utilice opcionalmente la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la red de origen al inquilino en la red de destino. Ver "Clonar claves de acceso S3 usando la API" .

Ver sus claves de acceso S3

Si está utilizando un inquilino S3 y tiene la"permiso apropiado" , puede ver una lista de sus claves de acceso S3. Puede ordenar la lista por tiempo de expiración, para poder determinar qué claves expirarán pronto. Según sea necesario, puede"crear nuevas claves" o"borrar teclas" que ya no estas usando.

Se puede acceder a los depósitos y objetos S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas 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 la opción Administrar sus propias credenciales de 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 vencimiento** o **ID de clave de acceso**.
3. Según sea necesario, cree nuevas claves o elimine aquellas que ya no utilice.

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

   Las claves caducadas se eliminan automáticamente.

Eliminar sus propias claves de acceso S3

Si está utilizando un inquilino S3 y tiene el permiso adecuado, puede eliminar sus propias claves de acceso S3. Una vez que se elimina una clave de acceso, ya no se puede usar para acceder a los objetos y depósitos en la cuenta del inquilino.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Tú tienes el"Administrar sus propios permisos de credenciales S3" .

Se puede acceder a los depósitos y objetos S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de su cuenta y nunca las comparta con otros usuarios.

Pasos

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

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

Crear las claves de acceso S3 de otro usuario

Si utiliza un inquilino S3 y tiene el permiso adecuado, puede crear claves de acceso S3 para otros usuarios, como aplicaciones que necesitan acceso a depósitos y objetos.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" .

Acerca de esta tarea

Puede crear una o más claves de acceso S3 para otros usuarios para que puedan crear y administrar depósitos para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con la nueva 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 estén utilizando. Si solo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la anterior y luego elimínela.

Cada clave puede tener un tiempo de expiración específico o no tener expiración. Siga estas pautas para el tiempo de vencimiento:

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

> Se puede acceder a los depósitos y objetos S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **GESTIÓN DE ACCESO** > **Usuarios**.
2. Seleccione el usuario cuyas claves de acceso S3 desea administrar.

   Aparece la página de detalles del usuario.
3. Seleccione **Teclas de acceso** y luego seleccione **Crear clave**.
4. Debe realizar una de las siguientes acciones:
   - Seleccione **No establecer un tiempo de expiración** para crear una clave que no expire. (Por defecto)
   - Seleccione **Establecer una hora de vencimiento** y configure la fecha y hora de vencimiento.

     > La fecha de vencimiento puede ser de un máximo de cinco años a partir de la fecha actual. El tiempo de expiración puede ser de un mínimo de un minuto a partir de la hora actual.
5. Seleccione **Crear clave de acceso**.

Aparece el cuadro de diálogo Descargar clave de acceso, que enumera el ID de la 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 la clave de acceso y la clave de acceso secreta.

   > No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No es posible copiar ni descargar claves una vez cerrado el cuadro de diálogo.

7. Seleccione **Finalizar**.

   La nueva clave aparece en la pestaña Teclas de acceso de la página de detalles del usuario.

8. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, utilice opcionalmente la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la red de origen al inquilino en la red de destino. Ver "Clonar claves de acceso S3 usando la API" .

Ver las claves de acceso S3 de otro usuario

Si está utilizando un inquilino S3 y tiene los permisos adecuados, puede ver las claves de acceso S3 de otro usuario. Puede ordenar la lista por tiempo de vencimiento para poder determinar qué claves caducarán pronto. Según sea necesario, puede crear nuevas claves y eliminar claves que ya no se utilizan.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Tú tienes el"Permiso de acceso root" .

> Se puede acceder a los depósitos y objetos S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **GESTIÓN DE ACCESO** > **Usuarios**.
2. Desde la página Usuarios, seleccione el usuario cuyas claves de acceso S3 desea ver.
3. Desde la página de detalles del usuario, seleccione **Teclas de acceso**.
4. Ordene las claves por **Tiempo de expiración** o **ID de clave de acceso**.
5. Según sea necesario, cree nuevas claves y elimine manualmente las claves que ya no se utilizan.

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

   Las claves caducadas se eliminan automáticamente.

Información relacionada

- "Crear las claves de acceso S3 de otro usuario"

- "Eliminar las claves de acceso S3 de otro usuario"

Eliminar las claves de acceso S3 de otro usuario

Si está utilizando un inquilino S3 y tiene los permisos adecuados, puede eliminar las claves de acceso S3 de otro usuario. Una vez que se elimina una clave de acceso, ya no se puede usar para acceder a los objetos y depósitos en la cuenta del inquilino.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Tú tienes el"Permiso de acceso root" .

> Se puede acceder a los depósitos y objetos S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **GESTIÓN DE ACCESO** > **Usuarios**.
2. Desde la página Usuarios, seleccione el usuario cuyas claves de acceso S3 desea administrar.
3. Desde la página de detalles del usuario, seleccione **Teclas de acceso** y luego seleccione la casilla de verificación para cada tecla de acceso que desee eliminar.
4. Seleccione **Acciones** > **Eliminar clave seleccionada**.
5. Desde el cuadro de diálogo de confirmación, seleccione **Eliminar tecla**.

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

Administrar depósitos S3

Crear un bucket S3

Puede utilizar el Administrador de inquilinos para crear depósitos S3 para 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 de root o administra todos los buckets"permiso" . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.

  > Los permisos para establecer o modificar las propiedades de bloqueo de objetos S3 de depósitos u objetos se pueden otorgar mediante"política de cubos o política de grupo" .

- Si planea habilitar el Bloqueo de objetos S3 para un depósito, un administrador de la red ha habilitado la configuración global de Bloqueo de objetos S3 para el sistema StorageGRID y usted ha revisado los requisitos para los depósitos y objetos de Bloqueo de objetos S3.

- Si cada inquilino tendrá 5000 depósitos, cada nodo de almacenamiento en la red tendrá un mínimo de 64 GB de RAM.

> Cada cuadrícula puede tener un máximo de 100.000 contenedores.

Acceder al asistente

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
2. Seleccione **Crear depósito**.

Introducir detalles

Pasos

1. Introduzca detalles para el depósito.

Campo	Descripción
Nombre del depósito	Un nombre para el depósito que cumple con estas reglas: • Debe ser único en cada sistema StorageGRID (no solo único dentro de la cuenta del inquilino). • Debe ser compatible con DNS. • Debe contener 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 contener puntos en las solicitudes de estilo alojado virtualmente. Los períodos causarán problemas con la verificación del certificado comodín del servidor. Para obtener más información, consulte la "Documentación de Amazon Web Services (AWS) sobre las reglas de nombres de bucket" . **Nota**: No puedes cambiar el nombre del depósito después de crearlo.
Región	La región del cubo. Su administrador de StorageGRID administra las regiones disponibles. La región de un depósito puede afectar la política de protección de datos aplicada a los objetos. De forma predeterminada, todos los depósitos se crean en el `us-east-1` región. **Nota**: No puedes cambiar la región después de crear el depósito.

2. Seleccione **Continuar**.

Administrar configuraciones

Pasos

1. De manera opcional, habilite el control de versiones de objetos para el depósito.

   Habilite el control de versiones de objetos si desea almacenar todas las versiones de cada objeto en este depósito. Luego puede recuperar versiones anteriores de un objeto según sea necesario. Debe habilitar el control de versiones de objetos si el depósito se utilizará para la replicación entre redes.

2. Si la configuración global de Bloqueo de objetos S3 está habilitada, habilite opcionalmente el Bloqueo de objetos S3 para que el depósito almacene objetos utilizando un modelo de escritura única, lectura múltiple (WORM).

   Habilite el bloqueo de objetos S3 para un depósito solo si necesita conservar objetos durante un período de tiempo fijo, por ejemplo, para cumplir con ciertos requisitos reglamentarios. El bloqueo de objetos S3 es una configuración permanente que le ayuda a evitar que los objetos se eliminen o sobrescriban durante un período de tiempo fijo o de manera indefinida.

   > Una vez habilitada la configuración de bloqueo de objetos S3 para un depósito, no se puede deshabilitar. Cualquier persona con los permisos correctos puede agregar objetos a este depósito que no se pueden modificar. Es posible que no puedas eliminar estos objetos ni el depósito en sí.

   Si habilita el Bloqueo de objetos S3 para un depósito, el control de versiones del depósito se habilita automáticamente.

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

   > Su administrador de red debe darle permiso para"Utilice funciones específicas de S3 Object Lock" .

   Cuando la **Retención predeterminada** está habilitada, los objetos nuevos agregados al depósito estarán automáticamente protegidos contra eliminación o sobrescritura. La configuración **Retención predeterminada** no se aplica a los objetos que tienen sus propios períodos de retención.

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

Modo de retención predeterminado	Descripción
Gobernancia	• Usuarios con la `s3:BypassGovernanceRetention` El permiso puede utilizar el `x-amz-bypass-governance-retention: true` encabezado de solicitud para omitir la configuración de retención. • Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.

Modo de retención predeterminado	Descripción
Cumplimiento	• El objeto no se puede eliminar hasta que se alcance su fecha de conservación. • La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir. • La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha. **Nota**: El administrador de su red debe permitirle utilizar el modo de cumplimiento.

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

   El **Período de retención predeterminado** indica durante cuánto tiempo se deben conservar los objetos nuevos agregados a este depósito, a partir del momento en que se ingieren. Especifique un valor que sea menor o igual al período de retención máximo para el inquilino, según lo establecido por el administrador de la red.

Se establece un período de retención *máximo*, que puede tener un valor de entre 1 día y 100 años, cuando el administrador de la red crea el inquilino. Cuando se establece un período de retención *predeterminado*, no puede exceder el valor establecido para el período de retención máximo. Si es necesario, solicite al administrador de su red que aumente o disminuya el período máximo de retención.

4. Opcionalmente, seleccione **Habilitar límite de capacidad**.

   El límite de capacidad es la capacidad máxima disponible para los objetos de este bucket. Este valor representa una cantidad lógica (tamaño del objeto), no una cantidad física (tamaño en disco).

   Si no se establece ningún límite, la capacidad de este depósito es ilimitada. Consulte "Uso del límite de capacidad" Para más información.

5. Seleccione **Crear depósito**.

   El depósito se crea y se agrega a la tabla en la página Depósitos.

6. Opcionalmente, seleccione **Ir a la página de detalles del depósito** para"ver detalles del depósito" y realizar una configuración adicional.

Ver detalles del depósito

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" .
- Perteneces a un grupo de usuarios que tiene la"Permiso para acceso root, administrar todos los depósitos o ver todos los depósitos" . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.

Pasos

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

   Aparece la página Cubos.

2. Revise la tabla de resumen para cada segmento.

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

   > Los valores de recuento de objetos, espacio utilizado y uso que se muestran son estimaciones. Estas estimaciones se ven afectadas por el momento de la ingesta, la conectividad de la red y el estado del nodo. Si los depósitos tienen habilitada la gestión de versiones, las versiones de los objetos eliminados se incluyen en el recuento de objetos.

   Nombre
   El nombre único del depósito, que no se puede cambiar.

   Funciones habilitadas
   La lista de funciones que están habilitadas para el depósito.

   Bloqueo de objetos S3
   Si el bloqueo de objetos S3 está habilitado para el depósito.

   Esta columna solo aparece si el bloqueo de objetos S3 está habilitado para la cuadrícula. Esta columna también muestra información sobre cualquier depósito compatible heredado.

   Región
   La región del cubo, que no se puede cambiar. Esta columna está oculta de forma predeterminada.

   Recuento de objetos
   La cantidad de objetos en este depósito. Si los depósitos tienen habilitada la gestión de versiones, las versiones de objetos no actuales se incluyen en este valor.

   Cuando se agregan o eliminan objetos, es posible que este valor no se actualice inmediatamente.

   Espacio utilizado
   El tamaño lógico de todos los objetos en el depósito. El tamaño lógico no incluye el espacio real requerido para copias replicadas o codificadas por borrado o para metadatos de objetos.

   Este valor puede tardar hasta 10 minutos en actualizarse.

   Uso
   El porcentaje utilizado del límite de capacidad del depósito, si se ha establecido uno.

   El valor de uso se basa en estimaciones internas y podría superarse en algunos casos. Por ejemplo, StorageGRID verifica el límite de capacidad (si está configurado) cuando un inquilino comienza a cargar objetos y rechaza nuevas ingestas en este depósito si el inquilino ha excedido el límite de capacidad. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha excedido el límite de capacidad. Si se eliminan objetos, es posible que se le impida temporalmente a un inquilino cargar nuevos objetos en este depósito hasta que se vuelva a calcular el uso del límite de capacidad. Los cálculos pueden tardar 10 minutos o más.

   Este valor indica el tamaño lógico, no el tamaño físico necesario para almacenar los objetos y sus

metadatos.

Capacidad
Si se establece, el límite de capacidad del depósito.

Fecha de creación
La fecha y hora en que se creó el depósito. Esta columna está oculta de forma predeterminada.

3. Para ver los detalles de un depósito específico, seleccione el nombre del depósito en la tabla.
   a. Vea la información resumida en la parte superior de la página web para confirmar los detalles del depósito, como la región y la cantidad de objetos.
   b. Ver la barra de uso del límite de capacidad. Si el uso es del 100% o cercano al 100%, considere aumentar el límite o eliminar algunos objetos.
   c. Según sea necesario, seleccione **Eliminar objetos en el depósito** y **Eliminar depósito**.

      Preste mucha atención a las precauciones que aparecen al seleccionar cada una de estas opciones. Para obtener más información, consulte:

      - "Eliminar todos los objetos en un depósito"
      - "Eliminar un depósito"(el cubo debe estar vacío)

   d. Vea o cambie la configuración del depósito en cada una de las pestañas según sea necesario.
      - **Consola S3**: Ver los objetos del depósito. Para obtener más información, consulte "Usar la consola S3" .
      - **Opciones de depósito**: Ver o cambiar la configuración de las opciones. Algunas configuraciones, como el bloqueo de objetos S3, no se pueden cambiar una vez creado el depósito.
        - "Gestionar la consistencia del depósito"
        - "Actualizaciones de la última hora de acceso"
        - "Límite de capacidad"
        - "Control de versiones de objetos"
        - "Bloqueo de objetos S3"
        - "Retención de depósito predeterminada"
        - "Administrar la replicación entre redes"(si está permitido para el inquilino)
      - **Servicios de plataforma**:"Administrar los servicios de la plataforma" (si está permitido para el inquilino)
      - **Acceso al bucket**: Ver o cambiar la configuración de las opciones. Debe tener permisos de acceso específicos.
        - Configurar"Intercambio de recursos entre orígenes (CORS)" De esta forma, el depósito y los objetos dentro del depósito serán accesibles para las aplicaciones web en otros dominios.
        - "Controlar el acceso de los usuarios"para un bucket S3 y los objetos dentro de ese bucket.

Aplicar una etiqueta de política ILM a un depósito

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

La política ILM controla dónde se almacenan los datos del objeto y si se eliminan después de un cierto período de tiempo. El administrador de su red crea políticas ILM y las asigna a etiquetas de políticas ILM cuando utiliza múltiples políticas activas.

> Evite reasignar con frecuencia la etiqueta de política de un depósito. De lo contrario, podrían surgir problemas de rendimiento.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso para acceso root, administrar todos los depósitos o ver todos los depósitos" . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.

Pasos

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

   Aparece la página Cubos. Según sea necesario, puede ordenar la información por cualquier columna o puede avanzar o retroceder en la lista.

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

   También puede cambiar la asignación de etiqueta de la política ILM para un depósito que ya tiene una etiqueta asignada.

   > Los valores de recuento de objetos y espacio utilizado que se muestran son estimaciones. Estas estimaciones se ven afectadas por el momento de la ingesta, la conectividad de la red y el estado del nodo. Si los depósitos tienen habilitada la gestión de versiones, las versiones de los objetos eliminados se incluyen en el recuento de objetos.

3. En la pestaña Opciones de depósito, expanda el acordeón de etiquetas de política ILM. Este acordeón solo aparece si el administrador de su red ha habilitado el uso de etiquetas de políticas personalizadas.
4. Lea la descripción de cada etiqueta de política para determinar qué etiqueta debe aplicarse al depósito.

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

5. Seleccione el botón de opción correspondiente a la etiqueta que desea asignar al depósito.
6. Seleccione **Guardar cambios**. Se establecerá una nueva etiqueta de depósito S3 en el depósito con la clave `NTAP-SG-ILM-BUCKET-TAG` y el valor del nombre de la etiqueta de política ILM.

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

   > Establezca y modifique las etiquetas de política de ILM utilizando únicamente el Administrador de inquilinos o la API del Administrador de inquilinos donde se valida la etiqueta de política de ILM. No modifique el `NTAP-SG-ILM-BUCKET-TAG` Etiqueta de política ILM que utiliza la API S3 PutBucketTagging o la API S3 DeleteBucketTagging.

Cambiar la etiqueta de política asignada a un depósito tiene un impacto temporal en el rendimiento mientras se reevalúan los objetos utilizando la nueva política ILM.

Administrar la política de depósitos

Puede controlar el acceso de los usuarios a un bucket S3 y a los objetos que contiene.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" . Los permisos Ver todos los depósitos y Administrar todos los depósitos solo permiten la visualización.
- Ha verificado que la cantidad requerida de nodos de almacenamiento y sitios están disponibles. Si dos o más nodos de almacenamiento no están disponibles dentro de algún sitio, o si un sitio no está disponible, es posible que los cambios en estas configuraciones no estén disponibles.

Pasos

1. Seleccione **Cubos** y luego seleccione el cubo que desea administrar.
2. En la página de detalles del depósito, seleccione **Acceso al depósito** > **Política del depósito**.
3. Debe realizar una de las siguientes acciones:
   - Introduzca una política de depósito seleccionando la casilla de verificación **Habilitar política**. Luego ingrese una cadena con formato JSON válida.

     Cada política de bucket tiene un límite de tamaño de 20 480 bytes.
   - Modifique una política existente editando la cadena.
   - Deshabilite una política desmarcando la opción **Habilitar política**.

Para obtener información detallada sobre las políticas de bucket, incluida la sintaxis del lenguaje y ejemplos, consulte"Ejemplos de políticas de depósito" .

Gestionar la consistencia del depósito

Los valores de consistencia se pueden usar para especificar la disponibilidad de los cambios de configuración del depósito, así como para proporcionar un equilibrio entre la disponibilidad de los objetos dentro de un depósito y la consistencia de esos objetos en diferentes nodos de almacenamiento y sitios. Puede cambiar los valores de consistencia 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" .
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.

Pautas de consistencia del cubo

La consistencia del depósito se utiliza para determinar la consistencia de las aplicaciones cliente que afectan a los objetos dentro de ese depósito S3. En general, debe utilizar la consistencia **Lectura después de nueva**

escritura para sus depósitos.

Cambiar la consistencia del depósito

Si la consistencia de **Lectura después de nueva escritura** no cumple con los requisitos de la aplicación cliente, puede cambiar la consistencia configurando la consistencia del depósito o utilizando el `Consistency-Control` encabezamiento. El `Consistency-Control` El encabezado anula la consistencia del depósito.

> Cuando se cambia la consistencia de un bucket, solo aquellos objetos que se ingieran después del cambio tienen la garantía de cumplir con la configuración revisada.

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
2. Seleccione el nombre del depósito de la tabla.

   Aparece la página de detalles del depósito.

3. Desde la pestaña **Opciones de depósito**, seleccione el acordeón **.
4. Seleccione una consistencia para las operaciones realizadas en los objetos de este depósito.
   - **Todos**: Proporciona el mayor nivel de consistencia. Todos los nodos reciben los datos inmediatamente o la solicitud fallará.
   - **Strong-global**: garantiza la consistencia de lectura después de escritura para todas las solicitudes de clientes en todos los sitios.
   - **Sitio fuerte**: garantiza la consistencia de lectura después de escritura para todas las solicitudes de clientes dentro de un sitio.
   - **Lectura después de nueva escritura** (predeterminado): proporciona consistencia de lectura después de escritura para objetos nuevos y consistencia eventual para actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Recomendado para la mayoría de los casos.
   - **Disponible**: Proporciona consistencia eventual tanto para objetos nuevos como para actualizaciones de objetos. Para los buckets S3, úselo solo cuando sea necesario (por ejemplo, para un bucket que contiene valores de registro que rara vez se leen, o para operaciones HEAD o GET en claves que no existen). No compatible con depósitos S3 FabricPool .
5. Seleccione **Guardar cambios**.

¿Qué sucede cuando cambias la configuración del depósito?

Los depósitos tienen múltiples configuraciones que afectan el comportamiento de los depósitos y de los objetos dentro de ellos.

Las siguientes configuraciones de depósito utilizan una consistencia **fuerte** de manera predeterminada. Si dos o más nodos de almacenamiento no están disponibles dentro de algún sitio, o si un sitio no está disponible, es posible que los cambios en estas configuraciones no estén disponibles.

- "Eliminación de un depósito vacío en segundo plano"
- "Hora del último acceso"
- "Ciclo de vida del bucket"
- "Política de cubos"

- "Etiquetado de cubos"
- "Control de versiones de bucket"
- "Bloqueo de objetos S3"
- "Cifrado de bucket"

> El valor de consistencia para el control de versiones del bucket, el bloqueo de objetos S3 y el cifrado del bucket no se puede establecer en un valor que no sea fuertemente consistente.

Las siguientes configuraciones de depósito no utilizan una consistencia fuerte y tienen una mayor disponibilidad para los cambios. Los cambios en esta configuración pueden tardar algún tiempo antes de surtir efecto.

- "Configuración de servicios de la plataforma: Integración de notificaciones, replicación o búsqueda"
- "Configuración de CORS"
- Cambiar la consistencia del depósito

> Si la consistencia predeterminada utilizada al cambiar la configuración del depósito no cumple con los requisitos de la aplicación cliente, puede cambiar la consistencia mediante el uso de `Consistency-Control` encabezado para el"API REST de S3" o mediante el uso del `reducedConsistency` o `force` opciones en el"API de gestión de inquilinos" .

Habilitar o deshabilitar las actualizaciones de la última hora de acceso

Cuando los administradores de red crean reglas de administración del ciclo de vida de la información (ILM) para un sistema StorageGRID , pueden especificar opcionalmente que se utilice la última hora de acceso de un objeto para determinar si se debe mover ese objeto a una ubicación de almacenamiento diferente. Si utiliza un inquilino S3, puede aprovechar dichas reglas habilitando actualizaciones de hora del último acceso para los objetos en un bucket S3.

Estas instrucciones solo se aplican a los sistemas StorageGRID que incluyen al menos una regla ILM que utiliza la opción **Hora del último acceso** como filtro avanzado o como hora de referencia. Puede ignorar estas instrucciones si su sistema StorageGRID no incluye dicha regla. Ver"Utilice la hora del último acceso en las reglas de ILM" Para más detalles.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.

Acerca de esta tarea

Hora del último acceso es una de las opciones disponibles para la instrucción de ubicación de **Hora de referencia** para una regla ILM. Establecer la hora de referencia para una regla en Hora del último acceso permite a los administradores de la red especificar que los objetos se coloquen en determinadas ubicaciones de almacenamiento en función de cuándo se recuperaron (leyeron o vieron) por última vez.

Por ejemplo, para garantizar que los objetos vistos recientemente permanezcan en un almacenamiento más rápido, un administrador de red puede crear una regla ILM que especifique lo siguiente:

- Los objetos que se hayan recuperado durante el último mes deben permanecer en los nodos de almacenamiento locales.
- Los objetos que no se hayan recuperado durante el último mes deberán trasladarse a una ubicación fuera del sitio.

De forma predeterminada, las actualizaciones de la hora del último acceso están deshabilitadas. Si su sistema StorageGRID incluye una regla ILM que utiliza la opción **Hora del último acceso** y desea que esta opción se aplique a los objetos en este bucket, debe habilitar las actualizaciones de la hora del último acceso para los buckets S3 especificados en esa regla.

> Actualizar la hora del último acceso cuando se recupera un objeto puede reducir el rendimiento de StorageGRID , especialmente para objetos pequeños.

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

- Actualizar los objetos con nuevas marcas de tiempo
- Agregue los objetos a la cola de ILM, para que puedan reevaluarse según las reglas y políticas de ILM actuales.

La tabla resume el comportamiento aplicado a todos los objetos en el depósito cuando el último tiempo de acceso está deshabilitado o habilitado.

Tipo de solicitud	Comportamiento si el último tiempo de acceso está deshabilitado (predeterminado)		Comportamiento si el último tiempo de acceso está habilitado	
	¿Última hora de acceso actualizada?	¿Objeto agregado a la cola de evaluación de ILM?	¿Última hora de acceso actualizada?	¿Objeto agregado 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
Solicitud de lista de objetos o versiones de objetos	No	No	No	No

Solicitud para copiar un objeto de un depósito a otro	• No, para la copia fuente • Sí, para la copia de destino	• No, para la copia fuente • Sí, para la copia de destino	• Sí, para la copia fuente • Sí, para la copia de destino	• Sí, para la copia fuente • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
2. Seleccione el nombre del depósito de la tabla.

   Aparece la página de detalles del depósito.

3. Desde la pestaña **Opciones de depósito**, seleccione el acordeón **Actualizaciones de hora del último acceso**.
4. Habilitar o deshabilitar las actualizaciones del último tiempo de acceso.
5. Seleccione **Guardar cambios**.

Cambiar la versión de un objeto para un bucket

Si está utilizando un inquilino S3, puede cambiar el estado de la versión de los depósitos S3.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.
- Ha verificado que la cantidad requerida de nodos de almacenamiento y sitios están disponibles. Si dos o más nodos de almacenamiento no están disponibles dentro de algún sitio, o si un sitio no está disponible, es posible que los cambios en estas configuraciones no estén disponibles.

Acerca de esta tarea

Puede habilitar o suspender el control de versiones de objetos para un depósito. Después de habilitar el control de versiones para un depósito, este no podrá regresar a un estado sin versiones. Sin embargo, puedes suspender el control de versiones del depósito.

- Deshabilitado: El control de versiones nunca se ha habilitado
- Habilitado: el control de versiones está habilitado
- Suspendido: el control de versiones estaba habilitado previamente y está suspendido

Para obtener más información, consulte lo siguiente:

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

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
2. Seleccione el nombre del depósito de la tabla.

   Aparece la página de detalles del depósito.

3. Desde la pestaña **Opciones de depósito**, seleccione el acordeón **Versiones de objeto**.
4. Seleccione un estado de control de versiones para los objetos en este depósito.

   El control de versiones de objetos debe permanecer habilitado para un depósito utilizado para la replicación entre redes. Si está habilitado el bloqueo de objetos S3 o la conformidad con versiones anteriores, las opciones de **Control de versiones de objetos** estarán deshabilitadas.

Opción	Descripción
Habilitar control de versiones	Habilite el control de versiones de objetos si desea almacenar todas las versiones de cada objeto en este depósito. Luego puede recuperar versiones anteriores de un objeto según sea necesario. Los objetos que ya estaban en el depósito se versionarán cuando un usuario los modifique.
Suspender el control de versiones	Suspenda el control de versiones de objetos si ya no desea que se creen nuevas versiones de objetos. Aún puedes recuperar cualquier versión de objeto existente.

5. Seleccione **Guardar cambios**.

Utilice S3 Object Lock para retener objetos

Puede utilizar S3 Object Lock si los depósitos y objetos deben cumplir con los requisitos reglamentarios para la retención.

> El administrador de su red debe darle permiso para utilizar funciones específicas de S3 Object Lock.

¿Qué es el bloqueo de objetos S3?

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

Cuando la configuración global de Bloqueo de objetos S3 está habilitada para un sistema StorageGRID , una cuenta de inquilino S3 puede crear depósitos con o sin el Bloqueo de objetos S3 habilitado. Si un bucket tiene habilitado el bloqueo de objetos S3, se requiere el control de versiones del bucket y se habilita automáticamente.

Un depósito sin bloqueo de objetos S3 solo puede tener objetos sin configuraciones de retención especificadas. Ningún objeto ingerido tendrá configuraciones de retención.

Un depósito con bloqueo de objetos S3 puede tener objetos con y sin configuraciones de retención especificadas por las aplicaciones cliente S3. Algunos objetos ingeridos tendrán configuraciones de retención.

Un depósito con bloqueo de objetos S3 y retención predeterminada configurada puede tener objetos cargados con configuraciones de retención especificadas y objetos nuevos sin configuraciones de retención. Los nuevos objetos utilizan la configuración predeterminada, porque la configuración de retención no se ha configurado a nivel de objeto.

De hecho, todos los objetos recién ingeridos tienen configuraciones de retención cuando se configura la retención predeterminada. Los objetos existentes sin configuraciones de retención de objetos no se verán afectados.

Modos de retención

La función de bloqueo de objetos de StorageGRID S3 admite dos modos de retención para aplicar diferentes niveles de protección a los objetos. Estos modos son equivalentes a los modos de retención de Amazon S3.

- En modo de cumplimiento:
  - El objeto no se puede eliminar hasta que se alcance su fecha de conservación.
  - La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir.
  - La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha.
- En modo de gobernanza:
  - Los usuarios con permiso especial pueden usar un encabezado de omisión en las solicitudes para modificar ciertas configuraciones de retención.
  - Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación.
  - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.

Configuración de retención para versiones de objetos

Si se crea un depósito con el bloqueo de objetos S3 habilitado, los usuarios pueden usar la aplicación cliente S3 para especificar opcionalmente las siguientes configuraciones de retención para cada objeto que se agregue al depósito:

- **Modo de retención**: Cumplimiento o gobernanza.
- **Conservar hasta fecha**: si la fecha de conservación de una versión de un objeto está en el futuro, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal**: al aplicar una retención legal a una versión de un objeto, se bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesites colocar una retención legal en un objeto que esté relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, sino que permanece vigente hasta que se elimina explícitamente. Las retenciones legales son independientes de la fecha de conservación.

  > Si un objeto está bajo retención legal, nadie puede eliminarlo, independientemente de su modo de retención.

  Para obtener detalles sobre la configuración de los objetos, consulte"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" .

Configuración de retención predeterminada para depósitos

Si se crea un depósito con el bloqueo de objetos S3 habilitado, los usuarios pueden especificar opcionalmente las siguientes configuraciones predeterminadas para el depósito:

- **Modo de retención predeterminado**: Cumplimiento o gobernanza.
- **Período de retención predeterminado**: durante cuánto tiempo se deben conservar las nuevas versiones de objetos agregadas a este depósito, a partir del día en que se agregan.

La configuración de depósito predeterminada se aplica únicamente a los objetos nuevos que no tienen su propia configuración de retención. Los objetos de bucket existentes no se ven afectados cuando agrega o cambia estas configuraciones predeterminadas.

Ver"Crear un bucket S3" y"Actualizar la retención predeterminada de bloqueo de objetos S3" .

Tareas de bloqueo de objetos S3

Las siguientes listas para administradores de red y usuarios inquilinos contienen las tareas de alto nivel para usar la función de bloqueo de objetos S3.

Administrador de red

- Habilite la configuración global de bloqueo de objetos S3 para todo el sistema StorageGRID .
- Asegúrese de que las políticas de gestión del ciclo de vida de la información (ILM) sean *compatibles*; es decir, que cumplan con los requisitos"Requisitos de los buckets con bloqueo de objetos S3 habilitado" .
- Según sea necesario, permita que un inquilino utilice Cumplimiento como modo de retención. De lo contrario, solo se permite el modo Gobernanza.
- Según sea necesario, establezca un período máximo de retención para un inquilino.

Usuario inquilino

- Revise las consideraciones para depósitos y objetos con bloqueo de objetos S3.
- Según sea necesario, comuníquese con el administrador de la red para habilitar la configuración global de bloqueo de objetos S3 y establecer permisos.
- Cree depósitos con el bloqueo de objetos S3 habilitado.
- De manera opcional, configure los ajustes de retención predeterminados para un depósito:
  - Modo de retención predeterminado: Gobernanza o Cumplimiento, si lo permite el administrador de la red.
  - Período de retención predeterminado: debe ser menor o igual al período de retención máximo establecido por el administrador de la red.
- Utilice la aplicación cliente S3 para agregar objetos y, opcionalmente, configurar la retención específica de objetos:
  - Modo de retención. Gobernanza o Cumplimiento, si lo permite el administrador de la red.
  - Conservar hasta la fecha: debe ser menor o igual a lo permitido por el período máximo de retención establecido por el administrador de la red.

Requisitos para los buckets con el bloqueo de objetos S3 habilitado

- Si la configuración global de Bloqueo de objetos S3 está habilitada para el sistema StorageGRID , puede usar el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3 para crear depósitos con el Bloqueo de objetos S3 habilitado.
- Si planea utilizar S3 Object Lock, debe habilitar S3 Object Lock cuando cree el depósito. No se puede habilitar el bloqueo de objetos S3 para un depósito existente.

- Cuando S3 Object Lock está habilitado para un bucket, StorageGRID habilita automáticamente el control de versiones para ese bucket. No puedes deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones del depósito.
- De manera opcional, puede especificar un modo de retención predeterminado y un período de retención para cada depósito mediante el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3. La configuración de retención predeterminada del depósito se aplica únicamente a los objetos nuevos agregados al depósito que no tienen su propia configuración de retención. Puede anular estas configuraciones predeterminadas especificando un modo de retención y una fecha de retención para cada versión del objeto cuando se carga.
- La configuración del ciclo de vida del bucket es compatible con los buckets que tienen el bloqueo de objetos S3 habilitado.
- La replicación de CloudMirror no es compatible con depósitos con el bloqueo de objetos S3 habilitado.

Requisitos para objetos en depósitos con bloqueo de objetos S3 habilitado

- Para proteger una versión de objeto, puede especificar la configuración de retención predeterminada para el depósito o puede especificar la configuración de retención para cada versión de objeto. Las configuraciones de retención a nivel de objeto se pueden especificar mediante la aplicación cliente S3 o la API REST S3.
- Las configuraciones de retención se aplican a versiones de objetos individuales. Una versión de objeto puede tener una configuración de conservación hasta la fecha y una configuración de conservación legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta la fecha o de retención legal para un objeto, se protege únicamente la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras la versión anterior del objeto permanece bloqueada.

Ciclo de vida de objetos en buckets con S3 Object Lock habilitado

Cada objeto que se guarda en un bucket con el bloqueo de objetos S3 habilitado pasa por estas etapas:

1. **Ingesta de objeto**

   Cuando se agrega una versión de objeto a un depósito que tiene habilitado el Bloqueo de objetos S3, las configuraciones de retención se aplican de la siguiente manera:

   - Si se especifican configuraciones de retención para el objeto, se aplican las configuraciones a nivel de objeto. Se ignoran todas las configuraciones de depósito predeterminadas.
   - Si no se especifican configuraciones de retención para el objeto, se aplican las configuraciones de depósito predeterminadas, si existen.
   - Si no se especifican configuraciones de retención para el objeto o el depósito, el objeto no estará protegido por el bloqueo de objetos S3.

   Si se aplican configuraciones de retención, tanto el objeto como cualquier metadato definido por el usuario de S3 estarán protegidos.

2. **Retención y eliminación de objetos**

   StorageGRID almacena varias copias de cada objeto protegido durante el período de retención especificado. La cantidad exacta y el tipo de copias de objetos y las ubicaciones de almacenamiento están determinados por las reglas compatibles con las políticas ILM activas. Si un objeto protegido se puede eliminar antes de que se alcance su fecha de retención depende de su modo de retención.

   - Si un objeto está bajo retención legal, nadie puede eliminarlo, independientemente de su modo de

retención.

¿Puedo seguir administrando buckets compatibles heredados?

La función de bloqueo de objetos S3 reemplaza la función de cumplimiento que estaba disponible en versiones anteriores de StorageGRID . Si creó depósitos compatibles con una versión anterior de StorageGRID, puede continuar administrando la configuración de estos depósitos; sin embargo, ya no podrá crear nuevos depósitos compatibles. Para obtener instrucciones, consultehttps://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"^] .

Actualizar la retención predeterminada de bloqueo de objetos S3

Si habilitó el bloqueo de objetos S3 cuando creó el depósito, puede editarlo 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" .
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.
- El bloqueo de objetos S3 está habilitado globalmente para su sistema StorageGRID y usted lo habilitó cuando creó el depósito. Ver "Utilice S3 Object Lock para retener objetos" .

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
2. Seleccione el nombre del depósito de la tabla.

   Aparece la página de detalles del depósito.

3. Desde la pestaña **Opciones de depósito**, seleccione el acordeón **Bloqueo de objeto S3**.
4. De manera opcional, habilite o deshabilite la **Retención predeterminada** para este depósito.

   Los cambios en esta configuración no se aplican a los objetos que ya están en el depósito ni a ningún objeto que pueda tener sus propios períodos de retención.

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

Modo de retención predeterminado	Descripción
Gobernancia	• Usuarios con la `s3:BypassGovernanceRetention` El permiso puede utilizar el `x-amz-bypass-governance-retention: true` encabezado de solicitud para omitir la configuración de retención. • Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.
Cumplimiento	• El objeto no se puede eliminar hasta que se alcance su fecha de conservación. • La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir. • La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha. **Nota**: El administrador de su red debe permitirle utilizar el modo de cumplimiento.

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

   El **Período de retención predeterminado** indica durante cuánto tiempo se deben conservar los objetos nuevos agregados a este depósito, a partir del momento en que se ingieren. Especifique un valor que sea menor o igual al período de retención máximo para el inquilino, según lo establecido por el administrador de la red.

   Se establece un período de retención *máximo*, que puede tener un valor de entre 1 día y 100 años, cuando el administrador de la red crea el inquilino. Cuando se establece un período de retención *predeterminado*, no puede exceder el valor establecido para el período de retención máximo. Si es necesario, solicite al administrador de su red que aumente o disminuya el período máximo de retención.

7. Seleccione **Guardar cambios**.

Configurar el uso compartido de recursos entre orígenes (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un bucket S3 si desea que ese bucket y los objetos que contiene sean accesibles para las aplicaciones web en otros dominios.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Para las solicitudes de configuración GET CORS, usted pertenece a un grupo de usuarios que tiene la"Administrar todos los depósitos o Ver todos los permisos de los depósitos" . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.
- Para las solicitudes de configuración PUT CORS, usted pertenece a un grupo de usuarios que tiene

la"Administrar todos los permisos de los buckets" . Este permiso anula la configuración de permisos en las políticas de grupo o de depósito.

- El"Permiso de acceso root" Proporciona acceso a todas las solicitudes de configuración de CORS.

Acerca de esta tarea

El uso compartido de recursos entre orígenes (CORS) es un mecanismo de seguridad que permite que las aplicaciones web cliente de un dominio accedan a recursos de un dominio diferente. Por ejemplo, supongamos que utiliza un depósito S3 llamado `Images` para almacenar gráficos. Al configurar CORS para el `Images` Cubo, puede permitir que las imágenes en ese cubo se muestren en el sitio web `http://www.example.com` .

Habilitar CORS para un bucket

Pasos

1. Utilice un editor de texto para crear el XML requerido. Este ejemplo muestra el XML utilizado para habilitar CORS para un bucket S3. Específicamente:
   - Permite que cualquier dominio envíe solicitudes GET al depósito
   - Sólo permite el `http://www.example.com` dominio para enviar solicitudes GET, POST y DELETE
   - Se permiten todos los encabezados de solicitud

   ```
   <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 sobre el XML de configuración de CORS, consulte "Documentación de Amazon Web Services (AWS): Guía del usuario de Amazon Simple Storage Service" .

2. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
3. Seleccione el nombre del depósito de la tabla.

   Aparece la página de detalles del depósito.

4. Desde la pestaña **Acceso al bucket**, seleccione el acordeón **Intercambio de recursos de origen cruzado (CORS)**.
5. Seleccione la casilla de verificación **Habilitar CORS**.

6. Pegue el XML de configuración de CORS en el cuadro de texto.
7. Seleccione **Guardar cambios**.

Modificar la configuración de CORS

Pasos

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

Deshabilitar la configuración CORS

Pasos

1. Desmarque la casilla de verificación **Habilitar CORS**.
2. Seleccione **Guardar cambios**.

Eliminar objetos en el depósito

Puede utilizar el Administrador de inquilinos para eliminar los objetos en 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 en cada depósito seleccionado de todos los nodos y sitios de su sistema StorageGRID . StorageGRID también elimina cualquier metadato de objeto relacionado. No podrás recuperar esta información.
- Eliminar todos los objetos de un depósito puede llevar minutos, días o incluso semanas, según la cantidad de objetos, copias de objetos y operaciones simultáneas.
- Si un cubo tiene"Bloqueo de objetos S3 habilitado" , podría permanecer en el estado **Eliminando objetos: solo lectura** durante *años*.

> Un depósito que utiliza S3 Object Lock permanecerá en el estado **Eliminando objetos: solo lectura** hasta que se alcance la fecha de retención para todos los objetos y se eliminen todas las retenciones legales.

- Mientras se eliminan objetos, el estado del depósito es **Eliminando objetos: solo lectura**. En este estado no se pueden agregar nuevos objetos al depósito.
- Cuando se hayan eliminado todos los objetos, el depósito permanecerá en estado de solo lectura. Puede realizar una de las siguientes acciones:
  - Devuelva el depósito al modo de escritura y reutilícelo para nuevos objetos
  - Eliminar el depósito
  - Mantenga el depósito en modo de solo lectura para reservar su nombre para uso futuro
- Si un bucket tiene habilitada la versión de objetos, los marcadores de eliminación que se crearon en StorageGRID 11.8 o posterior se pueden quitar mediante las operaciones Eliminar objetos en el bucket.
- Si un bucket tiene habilitada la versión de objetos, la operación de eliminación de objetos no eliminará los

marcadores de eliminación creados en StorageGRID 11.7 o anterior. Consulte información sobre cómo eliminar objetos en un depósito en"Cómo se eliminan los objetos versionados de S3" .

- Si utilizas"replicación entre redes" , tenga en cuenta lo siguiente:
  - Al utilizar esta opción no se elimina ningún objeto del depósito en la otra cuadrícula.
  - Si selecciona esta opción para el depósito de origen, se activará la alerta **Error de replicación entre cuadrículas** si agrega objetos al depósito de destino en la otra cuadrícula. Si no puede garantizar que nadie agregará objetos al contenedor en la otra cuadrícula,"Deshabilitar la replicación entre redes" para ese depósito antes de eliminar todos los objetos del depósito.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Permiso de acceso root" . Este permiso anula la configuración de permisos en las políticas de grupo o de depósito.

Pasos

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

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

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

   Menú de acciones

   a. Seleccione la casilla de verificación para cada depósito del que desee eliminar objetos.

   b. Seleccione **Acciones** > **Eliminar objetos en el depósito**.

   Página de detalles

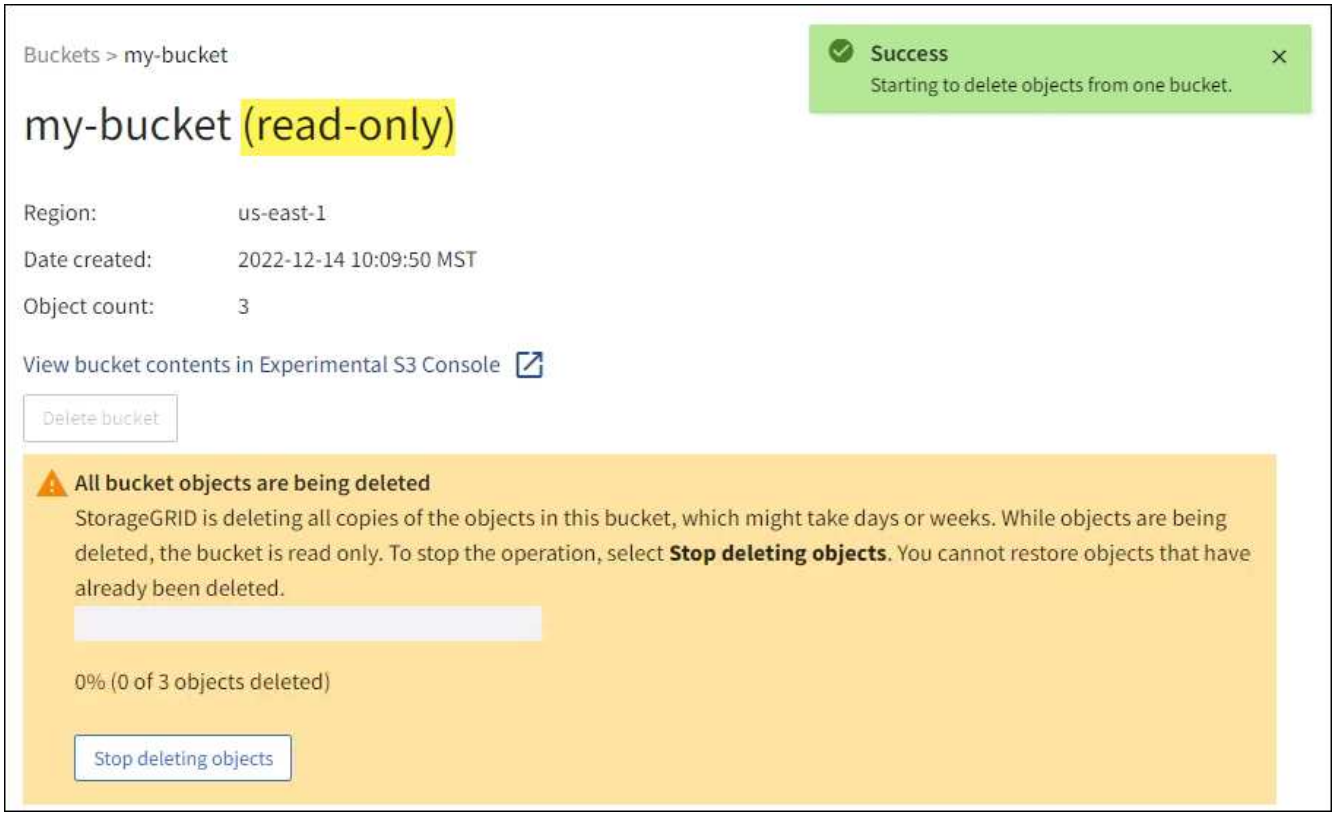
   a. Seleccione un nombre de depósito para mostrar sus detalles.

   b. Seleccione **Eliminar objetos del depósito**.

3. Cuando aparezca el cuadro de diálogo de confirmación, revise los detalles, ingrese **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 qué porcentaje de objetos se han eliminado.
   - **(solo lectura)** aparece después del nombre del depósito en la página de detalles del depósito.
   - **(Eliminar objetos: solo lectura)** aparece junto al nombre del depósito en la página Depósitos.

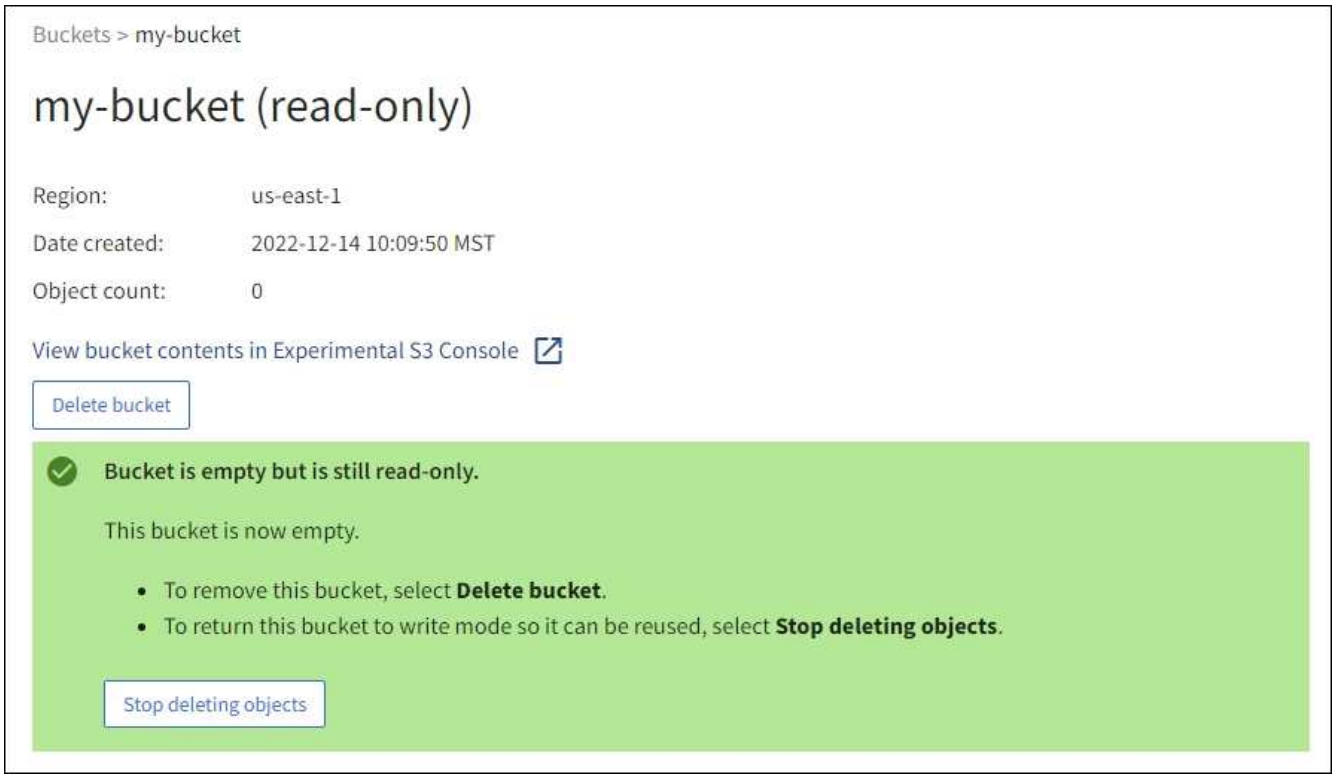


5. Según sea necesario mientras la operación se esté ejecutando, seleccione **Detener la eliminación de objetos** para detener el proceso. Luego, opcionalmente, seleccione **Eliminar objetos en el depósito** para reanudar el proceso.

   Cuando selecciona **Detener eliminación de 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, el banner de estado se actualiza, pero el depósito permanece como de solo lectura.



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

     Si no puede eliminar un depósito versionado después de eliminar todos los objetos, es posible que queden marcadores de eliminación. Para eliminar el depósito, debes quitar todos los marcadores de eliminación restantes.

   - Devuelve el depósito al modo de escritura y, opcionalmente, reutilízalo para nuevos objetos. Puede seleccionar **Detener la eliminación de objetos** para un solo depósito o regresar a la página Depósitos y seleccionar **Acción** > **Detener la eliminación de objetos** para más de un depósito.

Eliminar el depósito S3

Puede utilizar el Administrador de inquilinos para eliminar uno o más depósitos S3 que estén vacíos.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.
- Los depósitos que deseas eliminar están vacíos. Si los depósitos que desea eliminar no están vacíos,"eliminar objetos del depósito" .

Acerca de esta tarea

Estas instrucciones describen cómo eliminar un depósito S3 mediante el Administrador de inquilinos. También

puedes eliminar depósitos S3 usando el"API de gestión de inquilinos" o el"API REST de S3" .

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

Pasos

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

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

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

   Menú de acciones

   a. Seleccione la casilla de verificación para cada depósito que desee eliminar.

   b. Seleccione **Acciones** > **Eliminar depósitos**.

   Página de detalles

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

   b. Seleccione **Eliminar depósito**.

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

   StorageGRID confirma que cada depósito está vacío y luego elimina cada uno de ellos. Esta operación puede tardar unos minutos.

   Si un depósito no está vacío, aparece un mensaje de error. Usted debe"eliminar todos los objetos y cualquier marcador de eliminación en el depósito" antes de poder eliminar el depósito.

Usar la consola S3

Puede utilizar la Consola S3 para ver y administrar los objetos en un bucket S3.

La consola S3 le permite:

- Cargar, descargar, renombrar, copiar, mover y eliminar objetos
- Ver, revertir, descargar y eliminar versiones de objetos
- Buscar objetos por prefijo
- Administrar etiquetas de objetos
- Ver metadatos del objeto
- Ver, crear, renombrar, copiar, mover y eliminar carpetas

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

Si el uso de la consola S3 hace que las operaciones tarden demasiado tiempo (por ejemplo, minutos u horas), considere lo siguiente:

- Reducir el número de objetos seleccionados
- Usar métodos no gráficos (API o CLI) para acceder a sus datos

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Si desea administrar objetos, pertenece a un grupo de usuarios que tenga permiso de acceso Root. Como alternativa, pertenece a un grupo de usuarios que tiene el permiso de la pestaña Usar consola S3 y el permiso Ver todos los depósitos o el permiso Administrar todos los depósitos. Ver "Permisos de gestión de inquilinos" .
- Se ha configurado una política de grupo o bucket S3 para el usuario. Ver "Utilice políticas de acceso a grupos y buckets" .
- Conoces el ID de la clave de acceso del usuario y la clave de acceso secreta. Opcionalmente, tienes un `.csv` archivo que contiene esta información. Ver el"instrucciones para crear claves de acceso" .

Pasos

1. Seleccione **ALMACENAMIENTO** > **Cubos** > ***nombre del cubo***.
2. Seleccione la pestaña Consola S3.
3. Pegue el ID de la clave de acceso y la clave de acceso secreta en los campos. De lo contrario, seleccione **Cargar claves de acceso** y seleccione su `.csv` archivo.
4. Seleccionar * Sign in*.
5. Aparece la tabla de objetos del bucket. Puede administrar objetos según sea necesario.

Información adicional

- **Buscar por prefijo**: La función de búsqueda por 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 están dentro del `folder1/folder2/` carpeta y comenzar con la palabra `somefile-` .
- **Arrastrar y soltar**: puedes arrastrar y soltar archivos desde el administrador de archivos de tu computadora a la Consola S3. Sin embargo, no es posible cargar carpetas.
- **Operaciones en carpetas**: cuando mueves, copias o renombras una carpeta, todos los objetos en la carpeta se actualizan uno a la vez, lo que puede llevar tiempo.
- **Eliminación permanente cuando el control de versiones del depósito está deshabilitado**: cuando sobrescribe o elimina un objeto en un depósito con el control de versiones deshabilitado, la operación es permanente. Ver "Cambiar la versión de un objeto para un bucket" .

Administrar los servicios de la plataforma S3

Servicios de la plataforma S3

Descripción general y consideraciones sobre los servicios de la plataforma

Antes de implementar los servicios de la plataforma, revise la descripción general y las consideraciones para el uso de estos servicios.

Para obtener información sobre S3, consulte"Utilice la API REST de S3" .

Descripción general de los servicios de la plataforma

Los servicios de la plataforma StorageGRID pueden ayudarlo a implementar una estrategia de nube híbrida al permitirle enviar notificaciones de eventos y copias de objetos S3 y metadatos de objetos a destinos externos.

Dado que la ubicación de destino de los servicios de plataforma generalmente es externa a su implementación de StorageGRID , los servicios de plataforma le brindan la potencia y la flexibilidad que brinda el uso de recursos de almacenamiento externos, servicios de notificación y servicios de búsqueda o análisis para sus datos.

Se puede configurar cualquier combinación de servicios de plataforma para un único bucket S3. Por ejemplo, puede configurar tanto el"Servicio CloudMirror" y"notificaciones" en un bucket S3 de StorageGRID para que pueda reflejar objetos específicos en Amazon Simple Storage Service (S3) y, al mismo tiempo, enviar una notificación sobre cada uno de esos objetos a una aplicación de monitoreo de terceros para ayudarlo a realizar un seguimiento de sus gastos de AWS.

El uso de los servicios de la plataforma debe ser habilitado para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o la API de administración de Grid.

Cómo se configuran los servicios de la plataforma

Los servicios de plataforma se comunican con puntos finales externos que usted configura mediante el"Administrador de inquilinos" o el"API de gestión de inquilinos" . Cada punto final representa un destino externo, como un bucket S3 de StorageGRID , un bucket 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 habilitar un servicio de plataforma para un depósito agregando una configuración XML al depósito. La configuración XML identifica los objetos sobre los que debe actuar el depósito, la acción que debe realizar el depósito y el punto final que debe utilizar el depósito para el servicio.

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

- Si desea todos los objetos cuyas claves comiencen con `/images` Para replicarlo en un bucket de Amazon S3, debe agregar una configuración de replicación al bucket de origen.
- Si también desea enviar notificaciones cuando estos objetos se almacenan en el depósito, debe agregar una configuración de notificaciones.
- Si desea indexar los metadatos de estos objetos, debe agregar la configuración de notificación de metadatos que se utiliza para implementar la integración de búsqueda.

El formato del XML de configuración está regido por las API REST de S3 utilizadas para implementar los servicios de la plataforma StorageGRID :

Servicio de plataforma	API REST de S3	Referirse a
Replicación de CloudMirror	• Obtener réplica de cubo • Replicación de PutBucket	• "Replicación de CloudMirror" • "Operaciones en buckets"
Notificaciones	• Configuración de GetBucketNotification • Configuración de notificación de PutBucket	• "Notificaciones" • "Operaciones en buckets"
Integración de búsqueda	• Configuración de notificación de metadatos del depósito GET • Configuración de notificación de metadatos del depósito PUT	• "Integración de búsqueda" • "Operaciones personalizadas de StorageGRID"

Consideraciones para el uso de servicios de plataforma

Consideración	Detalles
Monitoreo de puntos finales de destino	Debes supervisar la disponibilidad de cada punto final de destino. Si se pierde la conectividad con el punto final de destino durante un período prolongado y existe una gran acumulación de solicitudes, las solicitudes de cliente adicionales (como las solicitudes PUT) a StorageGRID fallarán. Debes volver a intentar estas solicitudes fallidas cuando el punto final sea accesible.
Limitación del punto final de destino	El software StorageGRID puede limitar las solicitudes S3 entrantes para un bucket si la velocidad a la que se envían las solicitudes excede la velocidad a la que el punto final de destino puede recibirlas. La limitación solo se produce cuando hay una acumulación de solicitudes en espera de ser enviadas al punto final de destino. El único efecto visible es que las solicitudes S3 entrantes tardarán más en ejecutarse. Si comienza a detectar un rendimiento significativamente más lento, debe reducir la tasa de ingesta o utilizar un punto final con mayor capacidad. Si la acumulación de solicitudes continúa creciendo, las operaciones S3 del cliente (como las solicitudes PUT) eventualmente fallarán. Es más probable que las solicitudes de CloudMirror se vean afectadas por el rendimiento del punto final de destino porque estas solicitudes generalmente implican más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.

Consideración	Detalles
Garantías de pedidos	StorageGRID garantiza el orden de las operaciones en un objeto dentro de un sitio. Siempre que todas las operaciones contra un objeto se realicen dentro del mismo sitio, el estado final del objeto (para la replicación) siempre será igual al estado en StorageGRID. StorageGRID hace todo lo posible para ordenar las solicitudes cuando se realizan operaciones en los sitios de StorageGRID . Por ejemplo, si escribe un objeto inicialmente en el sitio A y luego sobrescribe el mismo objeto en el sitio B, no se garantiza que el objeto final replicado por CloudMirror en el depósito de destino sea el objeto más nuevo.
Eliminaciones de objetos impulsadas por ILM	Para que coincida con el comportamiento de eliminación de AWS CRR y Amazon Simple Notification Service, las solicitudes de notificación de eventos y CloudMirror no se envían cuando se elimina un objeto en el bucket de origen debido a las reglas ILM de StorageGRID . Por ejemplo, no se envían solicitudes de notificaciones de eventos ni de CloudMirror si una regla ILM elimina un objeto después de 14 días. Por el contrario, las solicitudes de integración de búsqueda se envían cuando se eliminan objetos debido a ILM.
Uso de puntos finales de Kafka	Para los puntos finales de Kafka, no se admite TLS mutuo. Como resultado, si tienes `ssl.client.auth` empezar a `required` en la configuración de su agente de Kafka, podría causar problemas de configuración del punto final de Kafka. La autenticación de los puntos finales de Kafka utiliza los siguientes tipos de autenticación. Estos tipos son diferentes de los que se utilizan para la autenticación de otros puntos finales, como Amazon SNS, y requieren credenciales de nombre de usuario y contraseña. • SASL/LLANO • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Nota:** Las configuraciones del proxy de almacenamiento configuradas no se aplican a los puntos finales de los servicios de la plataforma Kafka.

Consideraciones para utilizar el servicio de replicación CloudMirror

Consideración	Detalles
Estado de replicación	StorageGRID no es compatible con `x-amz-replication-status` encabezamiento.

Consideración	Detalles
Tamaño del objeto	El tamaño máximo de los objetos que el servicio de replicación CloudMirror puede replicar en un depósito de destino es de 5 TiB, que es el mismo que el tamaño máximo de objeto *compatible*. **Nota**: El tamaño máximo *recomendado* para una sola operación PutObject es 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice la carga multiparte en su lugar.
Control de versiones de bucket e ID de versiones	Si el depósito S3 de origen en StorageGRID tiene habilitada la gestión de versiones, también debe habilitarla para el depósito de destino. Al utilizar versiones, tenga en cuenta que el orden de las versiones de los objetos en el depósito de destino es el máximo esfuerzo y no está garantizado por el servicio CloudMirror, debido a las limitaciones del protocolo S3. **Nota**: Los ID de versión del depósito de origen en StorageGRID no están relacionados con los ID de versión del depósito de destino.
Etiquetado de versiones de objetos	El servicio CloudMirror no replica ninguna solicitud PutObjectTagging o DeleteObjectTagging que proporcione un ID de versión, debido a limitaciones en el 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 a un ID de versión específico. Por el contrario, el servicio CloudMirror replica solicitudes PutObjectTagging o DeleteObjectTagging que no especifican un ID de versión. Estas solicitudes actualizan las etiquetas para la última clave (o la última versión si el depósito tiene versión). Las ingestas normales con etiquetas (no actualizaciones de etiquetas) también se replican.
Cargas multiparte y `ETag` valores	Al reflejar objetos que se cargaron mediante una carga multiparte, el servicio CloudMirror no conserva las partes. Como resultado, la `ETag` El valor del objeto reflejado será diferente al `ETag` valor del objeto original.
Objetos cifrados con SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente)	El servicio CloudMirror no admite objetos cifrados con SSE-C. Si intenta ingerir un objeto en el bucket de origen para la replicación de CloudMirror y la solicitud incluye los encabezados de solicitud SSE-C, la operación fallará.
Cubo con bloqueo de objetos S3 habilitado	La replicación no es compatible con los depósitos de origen o destino que tengan el bloqueo de objetos S3 habilitado.

Comprender el servicio de replicación CloudMirror

Puede habilitar la replicación de CloudMirror para un bucket S3 si desea que StorageGRID replique objetos específicos agregados al bucket en uno o más buckets de destino externos.

Por ejemplo, puede utilizar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y luego aprovechar los servicios de AWS para realizar análisis de sus datos.

> La replicación de CloudMirror no es compatible si el depósito de origen tiene habilitado el bloqueo de objetos S3.

CloudMirror e ILM

La replicación de CloudMirror funciona independientemente de las políticas ILM activas de la red. El servicio CloudMirror replica los objetos a medida que se almacenan en el depósito de origen y los envía al depósito de destino lo antes posible. La entrega de objetos replicados se activa cuando la ingesta del objeto se realiza correctamente.

CloudMirror y replicación entre redes

La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre redes. Consulte "Comparar la replicación entre redes y la replicación de CloudMirror" .

Cubos de CloudMirror y S3

La replicación de CloudMirror normalmente está configurada para utilizar un depósito S3 externo como destino. Sin embargo, también puede configurar la replicación para utilizar otra implementación de StorageGRID o cualquier servicio compatible con S3.

Cubos existentes

Cuando habilita la replicación de CloudMirror para un depósito existente, solo se replican los nuevos objetos agregados a ese depósito. Cualquier objeto existente en el depósito no se replica. Para forzar la replicación de objetos existentes, puede actualizar los metadatos del objeto existente realizando una copia del 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 a 2 KB, ese objeto no se replicará.

Cubos de destino múltiples

Para replicar objetos de un solo depósito en varios depósitos de destino, especifique el destino de cada regla en el XML de configuración de replicación. No es posible replicar un objeto en más de un bucket al mismo tiempo.

Cubos versionados o no versionados

Puede configurar la replicación de CloudMirror en depósitos versionados o no versionados. Los depósitos de destino pueden tener versiones o no. Puede utilizar cualquier combinación de depósitos versionados y no versionados. Por ejemplo, puede especificar un depósito versionado como destino para un depósito de origen no versionado, o viceversa. También puedes replicar entre depósitos sin versiones.

Eliminación, bucles de replicación y eventos

Comportamiento de eliminación

Es lo mismo que el comportamiento de eliminación del servicio Amazon S3, Replicación entre regiones (CRR). Eliminar un objeto en un depósito de origen nunca elimina un objeto replicado en el destino. Si tanto el depósito de origen como el de destino tienen versiones, se replica el marcador de eliminación. Si el depósito de destino no tiene versión, eliminar un objeto en el depósito de origen no replica el marcador de

eliminación en el depósito de destino ni elimina el objeto de destino.

Protección contra bucles de replicación

A medida que los objetos se replican en el depósito de destino, StorageGRID los marca como "réplicas". Un depósito StorageGRID de destino no volverá a replicar objetos marcados como réplicas, lo que lo protege de bucles de replicación accidentales. Esta marca de réplica es interna a StorageGRID y no le impide aprovechar AWS CRR cuando usa un bucket de Amazon S3 como destino.

> ⓘ El encabezado personalizado utilizado para marcar una réplica es `x-ntap-sg-replica` . Esta marca evita que se forme un espejo en cascada. StorageGRID admite un CloudMirror bidireccional entre dos redes.

Eventos en el bucket de destino

No se garantiza la singularidad ni el orden de los eventos en el depósito de destino. Es posible que se entregue más de una copia idéntica de un objeto de origen al destino como resultado de las operaciones realizadas para garantizar el éxito de la entrega. En casos excepcionales, cuando el mismo objeto se actualiza simultáneamente desde dos o más sitios StorageGRID diferentes, el orden de las operaciones en el depósito de destino podría no coincidir con el orden de los eventos en el depósito de origen.

Comprender las notificaciones de los buckets

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

Por ejemplo, puede configurar alertas para que se envíen a los administradores sobre cada objeto agregado a un depósito, donde los objetos representan archivos de registro asociados con un evento crítico del sistema.

Las notificaciones de eventos se crean en el depósito de origen según lo especificado en la configuración de notificación y se envían al destino. Si un evento asociado con un objeto tiene éxito, se crea una notificación sobre ese evento y se pone en cola para su entrega.

No se garantiza la singularidad ni el orden de las notificaciones. Es posible que se envíe más de una notificación de un evento al destino como resultado de las operaciones realizadas para garantizar el éxito de la entrega. Y debido a que la entrega es asincrónica, no se garantiza que el orden temporal de las notificaciones en el destino coincida con el orden de los eventos en el depósito de origen, en particular para las operaciones que se originan en diferentes sitios de StorageGRID . Puedes utilizar el `sequencer` Introduzca la clave en el mensaje de evento para determinar el orden de los eventos para un objeto en particular, como se describe en la documentación de Amazon S3.

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

- Se admiten los siguientes tipos de eventos:
  - s3:ObjetoCreado:
  - s3:ObjetoCreado:Poner
  - s3:ObjetoCreado:Publicación
  - s3:ObjetoCreado:Copiar
  - s3:Objeto creado:Carga multiparte completa
  - s3:Objeto eliminado:
  - s3:ObjetoEliminado:Eliminar

- s3:Objeto eliminado:Eliminar marcador creado
- s3:Restaurar objeto:Publicar

- Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar, pero no incluyen algunas claves y utilizan valores específicos para otras, como se muestra en la tabla:

Nombre de la clave	Valor de StorageGRID
Fuente del evento	`sgws:s3`
Región de AWS	*no incluido*
x-amz-id-2	*no incluido*
arn	`urn:sgws:s3:::bucket_name`

Comprender el servicio de integración de búsqueda

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

El servicio de integración de búsqueda es un servicio StorageGRID personalizado que envía de forma automática y asincrónica metadatos de objetos S3 a un punto final de destino cada vez que se crea o elimina un objeto, o se actualizan sus metadatos o etiquetas. Luego, puede utilizar herramientas sofisticadas de búsqueda, análisis de datos, visualización o aprendizaje automático proporcionadas por el servicio de destino para buscar, analizar y obtener información de los datos de sus objetos.

Por ejemplo, puede configurar sus depósitos para enviar metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, puede usar Elasticsearch para realizar búsquedas en diferentes grupos y realizar análisis sofisticados de patrones presentes en los metadatos de sus objetos.

Si bien la integración de Elasticsearch se puede configurar en un bucket con S3 Object Lock habilitado, los metadatos de S3 Object Lock (incluidos Conservar hasta la fecha y el estado de Retención legal) de los objetos no se incluirán en los metadatos enviados a Elasticsearch.

> Debido a que el servicio de integración de búsqueda hace que se envíen metadatos de objetos a un destino, su XML de configuración se denomina "XML de configuración de notificación *metadata*". Este XML de configuración es diferente del "XML de configuración de notificación" utilizado para habilitar las notificaciones de *eventos*.

Integración de búsquedas y buckets S3

Puede habilitar el servicio de integración de búsqueda para cualquier depósito con o sin versión. La integración de búsqueda se configura asociando el XML de configuración de notificación de metadatos con el depósito que especifica sobre qué objetos actuar y el destino de los metadatos del objeto.

Las notificaciones de metadatos se generan en forma de un documento JSON cuyo nombre incluye el nombre del depósito, el nombre del objeto y el ID de la versión, si corresponde. 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 del usuario, StorageGRID pasa fechas y números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para que interprete estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para el mapeo de campos dinámicos y para el mapeo de formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indexado un documento, no es posible editar los tipos de campos del documento en el índice.

Notificaciones de búsqueda

Las notificaciones de metadatos 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 de la operación de la política ILM de la red.
- Se agregan, actualizan o eliminan metadatos o etiquetas de objetos. Al actualizar, siempre se envía el conjunto completo de metadatos y etiquetas, no solo los valores modificados.

Después de agregar XML de configuración de notificación de metadatos a un bucket, se envían notificaciones para cualquier objeto nuevo que cree y para cualquier objeto que modifique actualizando sus datos, metadatos de usuario o etiquetas. Sin embargo, no se envían notificaciones para ningún objeto que ya estuviera en el depósito. Para garantizar que los metadatos de todos los objetos del depósito se envíen al destino, debe realizar una de las siguientes acciones:

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

Servicio de integración de búsqueda y Elasticsearch

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

Administrar puntos finales de servicios de la plataforma

Configurar puntos finales de servicios de la plataforma

Antes de poder configurar un servicio de plataforma para un bucket, debe configurar al menos un punto final para que sea el destino del servicio de plataforma.

El acceso a los servicios de la plataforma lo habilita un administrador de StorageGRID por inquilino. Para crear o usar un punto final de servicios de plataforma, debe ser un usuario inquilino con permiso de acceso Administrar puntos finales o Raíz, en una red cuya red haya sido configurada para permitir que los nodos de almacenamiento accedan a recursos de puntos finales externos. Para un solo inquilino, puede configurar un máximo de 500 puntos finales de servicios de plataforma. Comuníquese con su administrador de StorageGRID para obtener más información.

¿Qué es un punto final de servicios de plataforma?

Un punto final de servicios de plataforma especifica la información que StorageGRID necesita para acceder al destino externo.

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

Cada tipo de servicio de plataforma requiere su propio punto final, por lo que debe configurar al menos un punto final para cada servicio de plataforma que planea utilizar. Después de definir un punto final de servicios de plataforma, utilice el URN del punto final como destino en el XML de configuración utilizado para habilitar el servicio.

Puede utilizar el mismo punto final como destino para más de un depósito de origen. Por ejemplo, puede configurar varios depósitos de origen para enviar metadatos de objetos al mismo punto final de integración de búsqueda para poder realizar búsquedas en varios depósitos. También puede configurar un bucket de origen para usar más de un punto final como destino, lo que le 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.

Puntos finales para la replicación de CloudMirror

StorageGRID admite puntos finales de replicación que representan depósitos S3. Estos depósitos pueden estar alojados en Amazon Web Services, en el mismo StorageGRID o en una implementación remota del mismo, o en otro servicio.

Puntos finales para notificaciones

StorageGRID admite puntos finales de Amazon SNS y Kafka. No se admiten los puntos finales de Simple Queue Service (SQS) ni de AWS Lambda.

Para los puntos finales de Kafka, no se admite TLS mutuo. Como resultado, si tienes `ssl.client.auth` empezar a `required` en la configuración de su agente de Kafka, podría causar problemas de configuración del punto final de Kafka.

Puntos finales para el servicio de integración de búsqueda

StorageGRID admite puntos finales de integración de búsqueda que representan clústeres de Elasticsearch. Estos clústeres de Elasticsearch pueden estar en un centro de datos local o alojados en una nube de AWS o en otro lugar.

El punto final de integración de búsqueda hace referencia a un índice y tipo de Elasticsearch específicos. Debe crear el índice en Elasticsearch antes de crear el punto final en StorageGRID, de lo contrario la creación del punto final fallará. No es necesario crear el tipo antes de crear el punto final. StorageGRID creará el tipo si es necesario cuando envíe metadatos del objeto al punto final.

Información relacionada

"Administrar StorageGRID"

Especificar URN para el punto final de los servicios de la plataforma

Cuando crea un punto final de servicios de plataforma, debe especificar un nombre de recurso único (URN). Utilizará la URN para hacer referencia al punto final cuando cree

un XML de configuración para el servicio de la plataforma. La URN de cada punto final debe ser única.

StorageGRID valida los puntos finales de los servicios de la plataforma a medida que los crea. Antes de crear un punto final de servicios de plataforma, confirme que el recurso especificado en el punto final exista y que se pueda acceder a él.

Elementos URN

El URN para un punto final de servicios de plataforma debe comenzar con `arn:aws` o `urn:mysite` , de la siguiente manera:

- 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 está alojado localmente, utilice `urn:mysite`

Por ejemplo, si está especificando el URN para un punto final de CloudMirror alojado en StorageGRID, el URN podría comenzar con `urn:sgws` .

El siguiente elemento de la URN especifica el tipo de servicio de plataforma, de la siguiente manera:

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

Por ejemplo, para continuar especificando el URN para un punto final de CloudMirror alojado en StorageGRID, agregaría `s3` Llegar `urn:sgws:s3` .

El elemento final de la URN identifica el recurso de destino específico en la 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 **no** está configurado para crear índices automáticamente, debe crear el índice manualmente antes de crear el punto final.

URN para servicios alojados en AWS y GCP

Para las entidades de AWS y GCP, el URN completo es un ARN de AWS 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 punto final de integración de búsqueda de AWS, el `domain-name` debe incluir la cadena literal `domain/` , como se muestra aquí.

URN para servicios alojados localmente

Al utilizar servicios alojados localmente en lugar de servicios en la nube, puede especificar el URN de cualquier forma que cree un URN válido y único, siempre que el URN incluya los elementos requeridos 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 la URN sea única. Por ejemplo:

- Replicación de CloudMirror:

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

  Para un punto final de CloudMirror alojado en StorageGRID, puede especificar un URN válido que comience con `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 de 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 puntos finales de integración de búsqueda alojados localmente, el `domain-name` El elemento puede ser cualquier cadena siempre que la URN del punto final sea única.

Crear punto final de servicios de plataforma

Debe crear al menos un punto final del tipo correcto antes de 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 habilitó los servicios de plataforma para su cuenta de inquilino.
- Perteneces a un grupo de usuarios que tiene la"Administrar puntos finales o permisos de acceso raíz" .
- Se han creado los recursos a los que hace referencia el punto final de servicios de la plataforma:
  - Replicación de CloudMirror: depósito S3
  - Notificación de eventos: Amazon Simple Notification Service (Amazon SNS) o tema de Kafka
  - Notificación de búsqueda: índice de Elasticsearch, si el clúster de destino no está configurado para crear índices automáticamente.
- Tienes la información sobre el recurso de destino:
  - Host y puerto para el Identificador uniforme de recursos (URI)

    > Si planea utilizar un depósito alojado en un sistema StorageGRID como punto final para la replicación de CloudMirror, comuníquese con el administrador de la red para determinar los valores que debe ingresar.

  - Nombre único de recurso (URN)

    "Especificar URN para el punto final de los servicios de la plataforma"

  - Credenciales de autenticación (si es necesario):

Puntos finales de integración de búsqueda

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

- Clave de acceso: ID de clave de acceso y clave de acceso secreta
- HTTP básico: Nombre de usuario y contraseña

Puntos finales de replicación de CloudMirror

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

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

Puntos finales de Amazon SNS

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

- Clave de acceso: ID de clave de acceso y clave de acceso secreta

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 CA personalizado)

- Si las funciones de seguridad de Elasticsearch están habilitadas, tiene el privilegio de clúster de monitorización para realizar pruebas de conectividad y el privilegio de escritura de índice o los privilegios de índice y eliminación de índice para las actualizaciones de documentos.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Puntos finales de servicios de plataforma**. Aparece la página de puntos finales de servicios de la plataforma.
2. Seleccione **Crear punto final**.
3. Ingrese un nombre para mostrar para describir brevemente el punto final y su propósito.

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

4. En el campo **URI**, especifique el Identificador único de recurso (URI) del punto final.

   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 (la mayoría de los puntos finales)
- Puerto 9092 para HTTPS y URI HTTP (solo puntos finales de Kafka)

Por ejemplo, el URI de un depósito 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 punto final del balanceador 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 falla.

De manera similar, el URI de un bucket alojado en AWS podría ser:

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

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

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

> No se puede cambiar el URN de un punto final una vez creado el punto final.

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

Puntos finales de integración de búsqueda

Ingrese o cargue las credenciales para un punto final de integración de búsqueda.

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

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
Tecla de acceso	Utiliza credenciales de estilo AWS para autenticar las 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 • Password

Puntos finales de replicación de CloudMirror

Ingrese o cargue las credenciales para un punto final de replicación de CloudMirror.

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

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
Tecla de acceso	Utiliza credenciales de estilo AWS para autenticar las conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta

Tipo de autenticación	Descripción	Cartas credenciales
CAP (Portal de acceso C2S)	Utiliza certificados y claves para autenticar las conexiones al destino.	• URL de credenciales temporales • Certificado de CA del servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada del cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada sin cifrar) • Frase de contraseña de la clave privada del cliente (opcional)

Puntos finales de Amazon SNS

Ingrese o cargue las credenciales para un punto final de Amazon SNS.

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

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
Tecla de acceso	Utiliza credenciales de estilo AWS para autenticar las conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta

Puntos finales de Kafka

Ingrese 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	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
SASL/LLANO	Utiliza un nombre de usuario y una contraseña con texto sin formato para autenticar las conexiones al destino.	• Nombre de usuario • Password

Tipo de autenticación	Descripción	Cartas credenciales
SASL/SCRAM-SHA-256	Utiliza un nombre de usuario y una contraseña mediante un protocolo de desafío-respuesta y hash SHA-256 para autenticar las conexiones al destino.	• Nombre de usuario • Password
SASL/SCRAM-SHA-512	Utiliza un nombre de usuario y una contraseña mediante un protocolo de desafío-respuesta y hash SHA-512 para autenticar las conexiones al destino.	• Nombre de usuario • Password

Seleccione **Usar autenticación mediante delegación** si el nombre de usuario y la contraseña se derivan de un token de delegación obtenido 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 al punto final.

Tipo de verificación del certificado	Descripción
Utilice un certificado CA personalizado	Utilice un certificado de seguridad personalizado. Si selecciona esta configuración, copie y pegue el certificado de seguridad personalizado en el cuadro de texto **Certificado CA**.
Utilice el certificado CA del sistema operativo	Utilice el certificado CA de Grid predeterminado instalado en el sistema operativo para proteger las conexiones.
No verificar el certificado	El certificado utilizado para la conexión TLS no está verificado. Esta opción no es segura.

10. Seleccione **Probar y crear punto final**.
    - Aparece un mensaje de éxito si se puede acceder al punto final utilizando las credenciales especificadas. La conexión al punto final se valida desde un nodo en cada sitio.
    - Aparece un mensaje de error si falla la validación del punto final. Si necesita modificar el punto final para corregir el error, seleccione **Regresar a los detalles del punto final** y actualice la información. Luego, seleccione **Probar y crear punto final**.

> ⓘ La creación de puntos finales falla si los servicios de la plataforma no están habilitados para su cuenta de inquilino. Comuníquese con su administrador de StorageGRID .

Después de haber configurado un punto final, puede usar su URN para configurar un servicio de plataforma.

Información relacionada

- "Especificar URN para el punto final de los servicios de la plataforma"
- "Configurar la replicación de CloudMirror"
- "Configurar notificaciones de eventos"
- "Configurar el servicio de integración de búsqueda"

Conexión de prueba para el punto final de servicios de la plataforma

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

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Administrar puntos finales o permisos de acceso raíz" .

Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Puntos finales de servicios de plataforma**.

   Aparece la página Puntos finales de servicios de la plataforma y muestra la lista de puntos finales de servicios de la plataforma que ya se han configurado.

2. Seleccione el punto final cuya conexión desea probar.

   Aparece la página de detalles del punto final.

3. Seleccione **Probar conexión**.
   - Aparece un mensaje de éxito si se puede acceder al punto final utilizando las credenciales especificadas. La conexión al punto final se valida desde un nodo en cada sitio.
   - Aparece un mensaje de error si falla la validación del punto final. Si necesita modificar el punto final para corregir el error, seleccione **Configuración** y actualice la información. Luego, seleccione **Probar y guardar cambios**.

Editar el punto final de los servicios de la plataforma

Puede editar la configuración de un punto final de servicios de la plataforma para cambiar su nombre, URI u otros detalles. Por ejemplo, es posible que necesite actualizar credenciales vencidas o cambiar la URI para que apunte a un índice de Elasticsearch de respaldo para conmutación por error. No se puede cambiar el URN de un punto final de servicios de plataforma.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Administrar puntos finales o permisos de acceso raíz" .

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Puntos finales de servicios de plataforma**.

   Aparece la página Puntos finales de servicios de la plataforma y muestra la lista de puntos finales de servicios de la plataforma que ya se han configurado.

2. Seleccione el punto final que desea editar.

   Aparece la página de detalles del punto final.

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

   > No se puede cambiar el URN de un punto final una vez creado el punto final.

   a. Para cambiar el nombre para mostrar del punto final, seleccione el ícono de edición .
   b. Según sea necesario, cambie la 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 una nueva ID de clave de acceso y una clave de acceso secreta. Si necesita cancelar sus cambios, seleccione **Revertir edición de clave S3**.
      - Para la autenticación CAP (Portal de acceso C2S), 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 clave según sea necesario.

        > La clave privada del cliente debe estar en formato cifrado OpenSSL o en formato de clave privada sin cifrar.

   d. Según sea necesario, cambie el método para verificar el servidor.
5. Seleccione **Probar y guardar cambios**.
   - Aparece un mensaje de éxito si se puede acceder al punto final utilizando las credenciales especificadas. La conexión al punto final se verifica desde un nodo en cada sitio.
   - Aparece un mensaje de error si falla la validación del punto final. Modifique el punto final para corregir el error y luego seleccione **Probar y guardar cambios**.

Eliminar el punto final de los servicios de la plataforma

Puede eliminar un punto final 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" .
- Perteneces a un grupo de usuarios que tiene la"Administrar puntos finales o permisos de acceso raíz" .

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Puntos finales de servicios de plataforma**.

   Aparece la página Puntos finales de servicios de la plataforma y muestra la lista de puntos finales de servicios de la plataforma que ya se han configurado.

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

Si elimina un punto final de servicios de plataforma que está en uso, el servicio de plataforma asociado se deshabilitará para cualquier depósito que use el punto final. Cualquier solicitud que aún no se haya completado será descartada. Se seguirán generando nuevas solicitudes hasta que usted cambie la configuración de su depósito para que ya no haga referencia al URN eliminado. StorageGRID informará estas solicitudes como errores irrecuperables.

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

   Aparece un mensaje de confirmación.

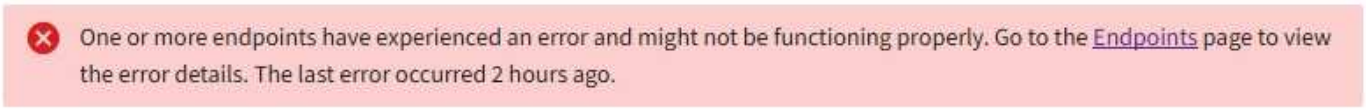
4. Seleccione **Eliminar punto final**.

Solucionar errores de puntos finales de servicios de la plataforma

Si se produce un error cuando StorageGRID intenta comunicarse con un punto final de servicios de la plataforma, se muestra un mensaje en el panel. En la página de puntos finales de servicios de la plataforma, la columna Último error indica cuánto tiempo hace que ocurrió el error. No se muestra ningún error si los permisos asociados con las credenciales de un punto final son incorrectos.

Determinar si se ha producido un error

Si se produjo algún error en los puntos finales de los servicios de la plataforma en los últimos 7 días, el panel del Administrador de inquilinos muestra un mensaje de alerta. Puede ir a la página de puntos finales de servicios de la plataforma para ver más detalles sobre el error.



El mismo error que aparece en el panel también aparece en la parte superior de la página de puntos finales de los servicios de la plataforma. Para ver un mensaje de error más detallado:

Pasos

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

Comprobar si el error sigue vigente

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

Pasos

1. Seleccione el punto final.

   Aparece la página de detalles del punto final.

2. Seleccione **Conexión** > **Probar conexión**.

Al seleccionar **Probar conexión**, StorageGRID valida que el punto final de servicios de la plataforma existe y que se puede acceder a él con las credenciales actuales. La conexión al punto final se valida desde un nodo en cada sitio.

Resolver errores de puntos finales

Puede utilizar el mensaje **Último error** en la página de detalles del punto final para ayudar a determinar qué está causando el error. Algunos errores podrían requerir que edites el punto final para resolver el problema. Por ejemplo, puede ocurrir un error de CloudMirroring si StorageGRID no puede acceder al bucket S3 de destino porque no tiene los permisos de acceso correctos o la clave de acceso ha expirado. El mensaje es "Es necesario actualizar las credenciales del punto final o el acceso al destino" y los detalles son "Acceso denegado" o "InvalidAccessKeyId".

Si necesita editar el punto final para resolver un error, seleccionar **Probar y guardar cambios** hace que StorageGRID valide el punto final actualizado y confirme que se puede acceder a él con las credenciales actuales. La conexión al punto final se valida desde un nodo en cada sitio.

Pasos

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

Credenciales de punto final con permisos insuficientes

Cuando StorageGRID valida un punto final de servicios de plataforma, confirma que las credenciales del punto final se pueden usar para contactar al recurso de destino y realiza una verificación de permisos básica. Sin embargo, StorageGRID no valida todos los permisos necesarios para ciertas operaciones de servicios de la plataforma. Por este motivo, si recibe un error al intentar utilizar un servicio de la plataforma (como "403 Prohibido"), verifique los permisos asociados con las credenciales del punto final.

Información relacionada

- **Administrar StorageGRID › Solucionar problemas de servicios de la plataforma**
- "Crear punto final de servicios de plataforma"
- "Conexión de prueba para el punto final de servicios de la plataforma"
- "Editar el punto final de los servicios de la plataforma"

Configurar la replicación de CloudMirror

Para habilitar la replicación de CloudMirror para un depósito, debe crear y aplicar un XML de configuración de replicación de depósito válido.

Antes de empezar

- Un administrador de StorageGRID habilitó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un depósito para que actúe como fuente de replicación.
- El punto final que desea utilizar como destino para la replicación de CloudMirror ya existe y tiene su URN.
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan las configuraciones de permisos en las políticas de grupo o de depósito cuando se configura el depósito mediante el Administrador de inquilinos.

Acerca de esta tarea

La replicación de CloudMirror copia objetos de un depósito de origen a un depósito de destino que se especifica en un punto final.

Para obtener información general sobre la replicación de buckets 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 la"Operaciones en buckets" .

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

Tenga en cuenta los siguientes requisitos y características al configurar la replicación de CloudMirror:

- Cuando crea y aplica un XML de configuración de replicación de bucket válido, debe utilizar el URN de un punto final de bucket S3 para cada destino.
- La replicación no es compatible con los depósitos de origen o destino que tengan el bloqueo de objetos S3 habilitado.
- Si habilita la replicación de CloudMirror en un depósito que contiene objetos, los objetos nuevos agregados al depósito se replican, pero los objetos existentes en el depósito no se replican. Debe actualizar los objetos existentes para activar la replicación.
- Si especifica una clase de almacenamiento en el XML de configuración de replicación, StorageGRID utiliza esa clase al realizar operaciones contra el punto final S3 de destino. El punto final de destino también debe admitir la clase de almacenamiento especificada. Asegúrese de seguir todas las recomendaciones proporcionadas por el proveedor del sistema de destino.

Pasos

1. Habilite la replicación para su depósito de origen:
   - Utilice un editor de texto para crear el XML de configuración de replicación necesario para habilitar la replicación, como se especifica en la API de replicación S3.
   - Al configurar el XML:
     - Tenga en cuenta que StorageGRID solo admite la versión 1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de `Filter` elemento para reglas y sigue las convenciones V1 para la eliminación de versiones de objetos. Consulte la documentación de Amazon sobre la configuración de replicación para obtener más detalles.
     - Utilice la URN de un punto final del bucket S3 como destino.
     - Opcionalmente agregue el `<StorageClass>` elemento y especifique uno de los siguientes:
       - `STANDARD`:La clase de almacenamiento predeterminada. Si no especifica una clase de almacenamiento cuando carga un objeto, el `STANDARD` Se utiliza la clase de almacenamiento.
       - `STANDARD_IA`:(Estándar - acceso poco frecuente). Utilice esta clase de almacenamiento para datos a los que se accede con menos frecuencia, pero que aún requieren 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 la `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 depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
3. Seleccione el nombre del depósito de origen.

   Aparece la página de detalles del depósito.

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**.

   > Los servicios de la plataforma deben ser habilitados para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o Grid Management API. Comuníquese con su administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Verifique que la replicación esté configurada correctamente:
   a. Agregue un objeto al depósito de origen que cumpla con los requisitos de replicación según lo especificado en la configuración de replicación.

      En el ejemplo mostrado anteriormente, se replican los objetos que coinciden con el prefijo "2020".

   b. Confirme que el objeto se haya replicado en el depósito de destino.

      Para objetos pequeños, la replicación ocurre rápidamente.

Información relacionada

"Crear punto final de servicios de plataforma"

Configurar notificaciones de eventos

Puede habilitar las notificaciones para un depósito creando un XML de configuración de notificaciones y utilizando el Administrador de inquilinos para aplicar el XML a un depósito.

Antes de empezar

- Un administrador de StorageGRID habilitó los servicios de plataforma para su cuenta de inquilino.

- Ya has creado un depósito que actuará como fuente de notificaciones.
- El punto final que desea utilizar como destino para las notificaciones de eventos ya existe y tiene su URN.
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan las configuraciones de permisos en las políticas de grupo o de depósito cuando se configura el depósito mediante el Administrador de inquilinos.

Acerca de esta tarea

Puede configurar las notificaciones de eventos asociando el XML de configuración de notificaciones con un depósito de origen. El XML de configuración de notificaciones sigue las convenciones S3 para configurar notificaciones de bucket, con el tema de destino de Kafka o Amazon SNS especificado como el URN de un punto final.

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 notificaciones de bucket S3, consulte"Instrucciones para implementar aplicaciones cliente S3" .

Tenga en cuenta los siguientes requisitos y características al configurar las notificaciones de eventos para un bucket:

- Cuando crea y aplica un XML de configuración de notificación válido, debe utilizar el URN de un punto final de notificaciones de eventos para cada destino.
- Si bien la notificación de eventos se puede configurar en un bucket con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluidos la fecha de retención y el estado de retención legal) de los objetos no se incluirán en los mensajes de notificación.
- Después de configurar las notificaciones de eventos, cada vez que ocurre un evento específico para un objeto en el bucket de origen, se genera una notificación y se envía al tema de Amazon SNS o Kafka utilizado como punto final de destino.
- Si habilita las notificaciones de eventos para un depósito que contiene objetos, las notificaciones se envían solo para las acciones que se realizan después de guardar la configuración de notificación.

Pasos

1. Habilitar notificaciones para su depósito de origen:
    - Utilice un editor de texto para crear el XML de configuración de notificación necesario para habilitar las notificaciones de eventos, como se especifica en la API de notificación S3.
    - Al configurar el XML, utilice la URN de un punto final 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)** > **Cubos**.
3. Seleccione el nombre del depósito de origen.

   Aparece la página de detalles del depósito.

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**.

   > Los servicios de la plataforma deben ser habilitados para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o Grid Management API. Comuníquese con su administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Verifique que las notificaciones de eventos estén configuradas correctamente:

   a. Realizar una acción en un objeto en el depósito de origen que cumpla con los requisitos para activar una notificación según lo 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 enviado 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 la notificación se recibe en el tema de destino, ha configurado correctamente su depósito de origen para las notificaciones de StorageGRID .

Información relacionada

"Comprender las notificaciones de los buckets"

"Utilice la API REST de S3"

"Crear punto final de servicios de plataforma"

Configurar el servicio de integración de búsqueda

Puede habilitar la integración de búsqueda para un depósito creando un XML de integración de búsqueda y utilizando el Administrador de inquilinos para aplicar el XML al depósito.

Antes de empezar

- Un administrador de StorageGRID habilitó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket S3 cuyo contenido desea indexar.
- El punto final que desea utilizar como destino para el servicio de integración de búsqueda ya existe y tiene su URN.
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan las configuraciones de permisos en las políticas de grupo o de depósito cuando se configura el depósito mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar el servicio de integración de búsqueda para un depósito de origen, la creación de un objeto o la actualización de los metadatos o las etiquetas de un objeto activa el envío de metadatos del objeto al punto final 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. Actualice estos objetos existentes para garantizar que sus metadatos se agreguen al índice de búsqueda de destino.

Pasos

1. Habilitar la integración de búsqueda para un depósito:
    - Utilice un editor de texto para crear el XML de notificación de metadatos necesario para habilitar la integración de búsqueda.
    - Al configurar el XML, utilice la URN de un punto final de integración de búsqueda como destino.

      Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, podría enviar metadatos para objetos con el prefijo `images` a un destino y metadatos para 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.

      Según sea necesario, consulte laEjemplos para la configuración de metadatos XML .

      ```
      <MetadataNotificationConfiguration>
       <Rule>
          <Status>Enabled</Status>
          <Prefix></Prefix>
          <Destination>
             <Urn>/Urn>
             </Destination>
       </Rule>
      </MetadataNotificationConfiguration>
      ```

Elementos en el XML de configuración de notificación de metadatos:

Nombre	Descripción	Requerido
Configuración de notificación de metadatos	Etiqueta contenedora para reglas utilizadas para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos de regla.	Sí
Regla	Etiqueta contenedora para una regla que identifica los objetos cuyos metadatos deben agregarse a un índice específico. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
IDENTIFICACIÓN	Identificador único de la regla. Incluido en el elemento Regla.	No
Estado	El estado puede ser 'Habilitado' o 'Deshabilitado'. No se realiza ninguna acción para las reglas que están deshabilitadas. 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 que coincida con 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

Nombre	Descripción	Requerido
Urna	URN del destino donde se envían los metadatos del objeto. Debe ser la URN de un punto final de StorageGRID con las siguientes propiedades: • `es`Debe ser el tercer elemento. • La URN debe terminar con el índice y tipo donde se almacenan los metadatos, en el formato `domain-name/myindex/mytype` . Los puntos finales se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Toman la siguiente forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe configurarse antes de enviar el XML de configuración; de lo contrario, la configuración fallará con un error 404. URN está incluido en el elemento Destino.	Sí

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

   Aparece la página de detalles del depósito.

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**.

   Los servicios de plataforma deben ser habilitados para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o la API de administración. Comuníquese con su administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Verifique que el servicio de integración de búsqueda esté configurado correctamente:
   a. Agregue un objeto al depósito de origen que cumpla con los requisitos para activar una notificación de metadatos según lo especificado en el XML de configuración.

      En el ejemplo mostrado anteriormente, todos los objetos agregados al depósito activan una notificación de metadatos.

   b. Confirme que se agregó un documento JSON que contiene los metadatos y las etiquetas del objeto al índice de búsqueda especificado en el punto final.

Después de terminar

Según sea necesario, puede deshabilitar la integración de búsqueda para un depósito utilizando cualquiera de los siguientes métodos:

- Seleccione **ALMACENAMIENTO (S3)** > **Cubos** y desmarque la casilla **Habilitar integración de búsqueda**.
- Si está utilizando la API S3 directamente, utilice una solicitud de notificación de metadatos de DELETE Bucket. Consulte las instrucciones para implementar aplicaciones cliente S3.

Ejemplo: Configuración de notificación de metadatos que se aplica a todos los objetos

En este ejemplo, los metadatos 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>
```

Ejemplo: Configuración de notificación 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 del objeto para 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>
```

Formato de notificación de metadatos

Cuando habilita el servicio de integración de búsqueda para un depósito, se genera un documento JSON y se envía al punto final de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas de objeto.

Este ejemplo muestra un ejemplo del JSON que podría generarse cuando un objeto con la clave `SGWS/Tagging.txt` se crea en un depósito llamado `test` . El `test` El bucket no tiene versión, por lo que `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"
  }
}
```

Campos incluidos en el documento JSON

El nombre del documento incluye el nombre del depósito, el nombre del objeto y el ID de la versión, si está presente.

Información de depósito y objeto

`bucket`: Nombre del bucket

`key`: Nombre de la clave del objeto

`versionID`:Versión del objeto, para objetos en depósitos versionados

`region`: Región del cubo, por ejemplo `us-east-1`

Metadatos del sistema

`size`:Tamaño del objeto (en bytes) tal como lo ve un cliente HTTP

`md5`: Hash de objeto

Metadatos del usuario

`metadata`:Todos los metadatos del usuario para el objeto, como pares clave-valor

`key:value`

Etiquetas

`tags`:Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor

`key:value`

Cómo ver resultados en Elasticsearch

Para las etiquetas y los metadatos del usuario, StorageGRID pasa fechas y números a Elasticsearch como

cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para que interprete estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para el mapeo de campos dinámicos y para el mapeo de formatos de fecha. Habilite las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indexado un documento, no es posible editar los tipos de campos del documento en el índice.

Información de copyright

Información de la marca comercial