Utilice StorageGRID

StorageGRID software

NetApp
January 14, 2026

Tabla de contenidos

Utilizar clientes y inquilinos de StorageGRID

Usar una cuenta de inquilino

Usar una cuenta de inquilino

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

¿Qué es una cuenta de inquilino?

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

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

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

  > Si utiliza el protocolo 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"Bloques de S3 y políticas de bloques" Para más información.

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

Cómo crear una cuenta de inquilino

Las cuentas de arrendatario las crea un "El administrador de grid de StorageGRID que utiliza Grid Manager". Al crear una cuenta de inquilino, el administrador de grid especifica lo siguiente:

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

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

Configure los inquilinos S3

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

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

Aunque puede crear y administrar buckets S3 con el Gestor de inquilinos, debe usar un "Cliente S3" OR "S3 Consola" para ingerir y gestionar objetos.

Cómo iniciar sesión y salir

Inicie sesión en el Administrador de inquilinos

Para acceder al Gestor de Inquilinos, introduzca la URL del inquilino en la barra de direcciones de un "navegador web compatible".

Antes de empezar

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

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

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

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

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

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

Pasos

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

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

   No se utiliza SSO

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

   - La página de inicio de sesión de Grid Manager. Seleccione el enlace **Inscrito de inquilino**.
   - La página de inicio de sesión del administrador de inquilinos. Es posible que el campo **Cuenta** ya esté completado.
     i. Si no se muestra el ID de cuenta de 20 dígitos del arrendatario, seleccione el nombre de la cuenta de arrendatario si aparece en la lista de cuentas recientes o introduzca el ID de cuenta.
     ii. Introduzca su nombre de usuario y contraseña.
     iii. Seleccione **Iniciar sesión**.

     Aparece el panel de control del gestor de inquilinos.

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

   Uso de SSO

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

   - La página SSO de su organización.

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

   - La página de inicio de sesión SSO de inquilino Manager.
     i. Si no se muestra el ID de cuenta de 20 dígitos del arrendatario, seleccione el nombre de la cuenta de arrendatario si aparece en la lista de cuentas recientes o introduzca el ID de cuenta.
     ii. Seleccione **Iniciar sesión**.
     iii. Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

     Aparece el panel de control del gestor de inquilinos.

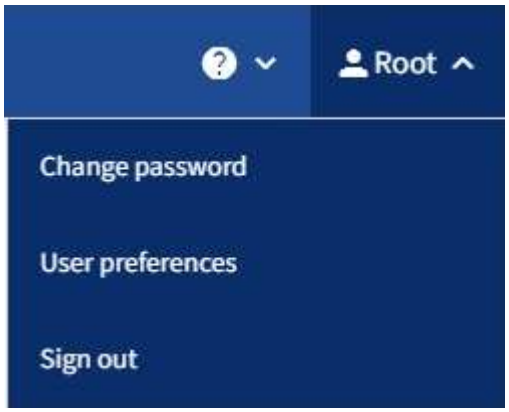
Cierre la sesión del responsable de inquilinos

Cuando haya terminado de trabajar con el Administrador de inquilinos, debe cerrar sesión para asegurarse de que los usuarios no autorizados no puedan acceder al

sistema StorageGRID. Es posible que cerrar el navegador no le cierre la sesión del sistema según la configuración de cookies del navegador.

Pasos

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



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

   - Si SSO no está en uso:

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

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

   - Si SSO está habilitado:

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

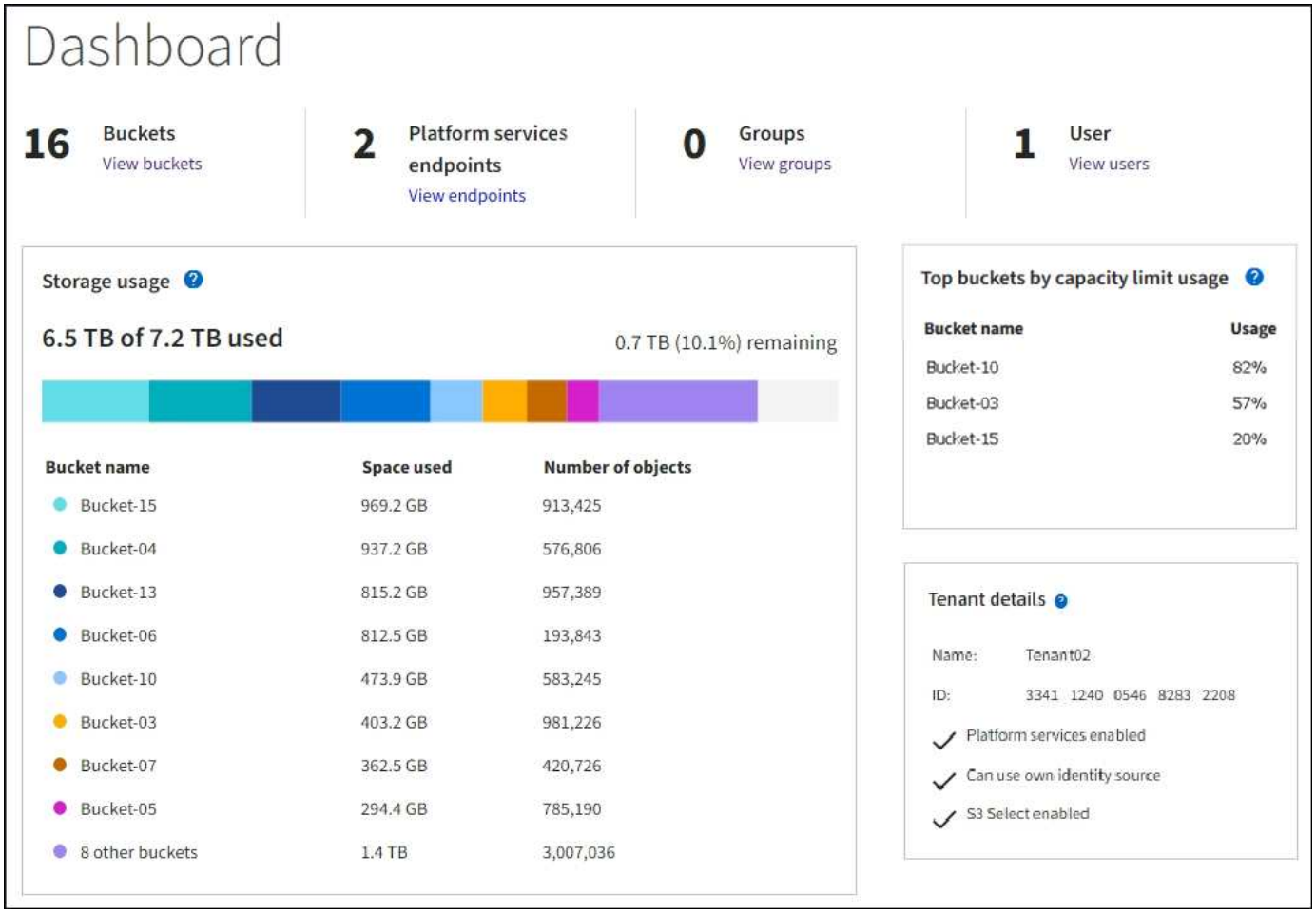
     Si SSO está activado y también ha iniciado sesión en Grid Manager, también debe cerrar sesión en Grid Manager para cerrar sesión en SSO.

Conozca la consola de tenant Manager

El panel de control del administrador de inquilinos 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 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.

El tamaño lógico de todos los objetos que pertenecen a este inquilino incluye cargas multiparte incompletas y en progreso. El tamaño no incluye el espacio físico adicional utilizado para las políticas de ILM. 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.

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



Información de la cuenta de inquilino

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

Según las "permisos de gestión de inquilinos"opciones que haya configurado, el resto de la consola muestra diferentes combinaciones de directrices, uso de almacenamiento, información del objeto y detalles de inquilinos.

Aprovechamiento del almacenamiento y de la cuota

El panel uso del almacenamiento contiene la siguiente información:

- La cantidad de datos de objeto para el inquilino.

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

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

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

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

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

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

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

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

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

Alertas de uso de cuotas

Si se han activado alertas de uso de cuotas en Grid Manager, estas alertas aparecerán en el gestor de inquilinos cuando la cuota sea baja o excedida, de la siguiente manera:

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

  Considere la posibilidad de solicitar al administrador de grid que aumente la cuota.

- Si excedes tu cuota, una notificación te indica que no puedes cargar nuevos objetos.

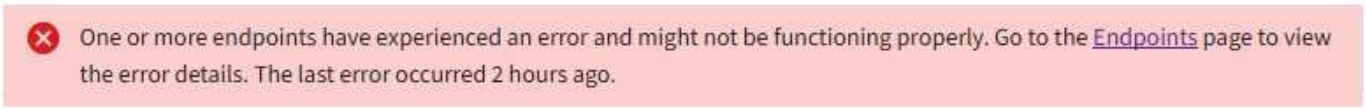
Límite de uso de la capacidad

Si ha establecido un límite de capacidad para sus bloques, la consola de tenant Manager muestra una lista de los bloques principales por 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 se alcanza esa cuota, no podrá ingerir más objetos independientemente del límite de capacidad restante en un bloque.

Errores de punto final

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



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

API de gestión de inquilinos

Comprender la API de gestión de inquilinos

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

API de gestión de inquilinos:

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

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

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

Operaciones de API

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

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

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

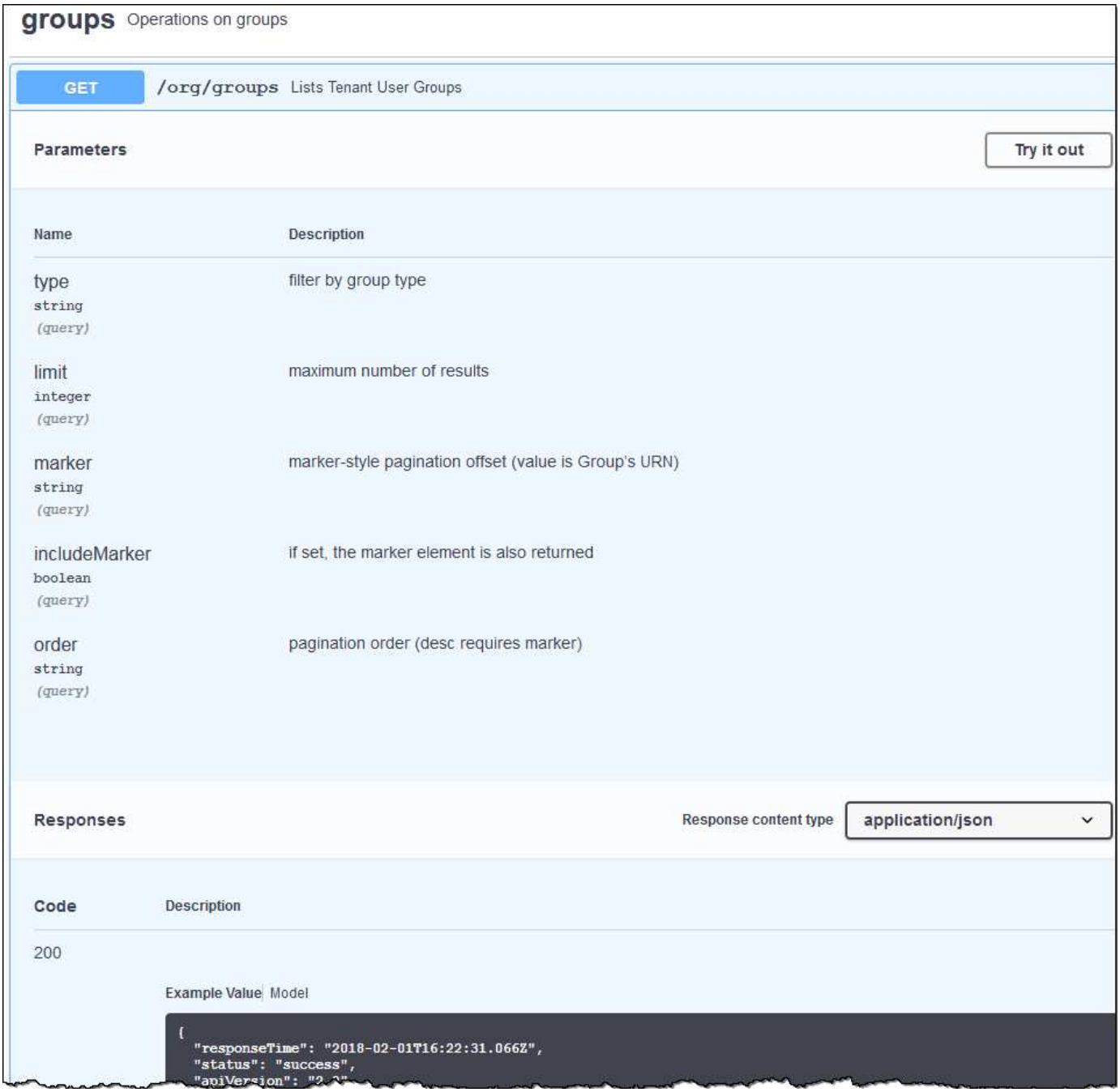
  Para obtener información sobre cómo mejorar la seguridad de autenticación, consulte "Protección contra falsificación de solicitudes entre sitios".

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

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

Detalles de la operación

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



Emita solicitudes API

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

Pasos

1. Seleccione la acción HTTP para ver los detalles de la solicitud.
2. Determine si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. A continuación, obtenga estos valores. Es posible que primero deba emitir una solicitud de API diferente para obtener la información que necesita.
3. Determine si necesita modificar el cuerpo de solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.

4. Seleccione **probar**.
5. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.
6. Seleccione **Ejecutar**.
7. Revise el código de respuesta para determinar si la solicitud se ha realizado correctamente.

Creación de versiones de la API de gestión de inquilinos

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

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

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

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

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

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

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

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

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

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

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

Determine qué versiones de API son compatibles con la versión actual

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

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

Especifique una versión API para una solicitud

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

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

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

Protección contra falsificación de solicitudes entre sitios (CSRF)

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

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

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

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

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

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

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

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

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

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

Utilizar conexiones de federación de grid

Clone los usuarios y los grupos de inquilinos

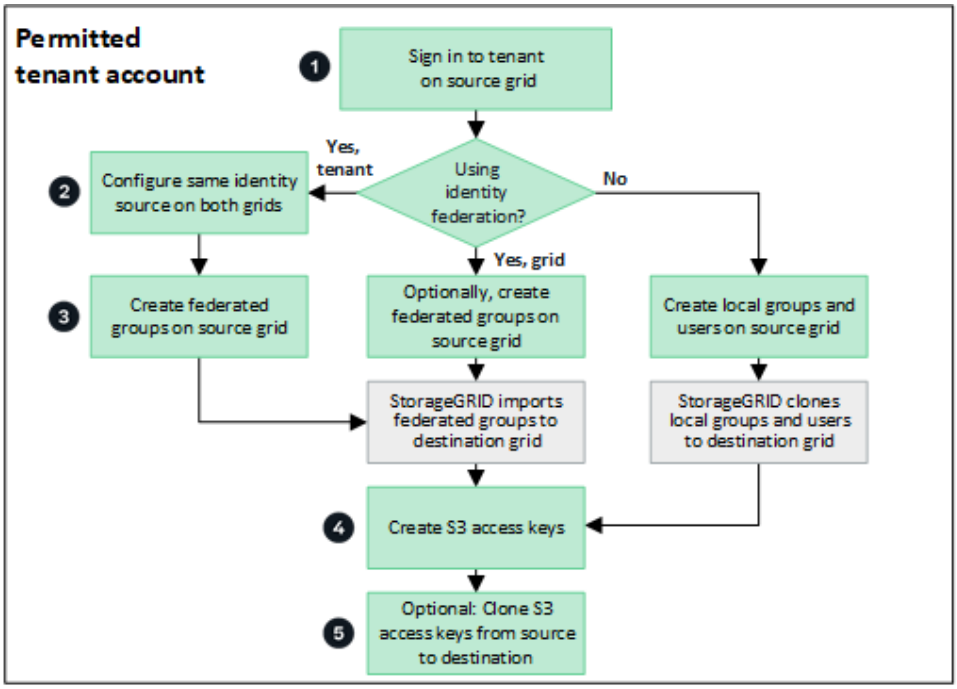
Si se creó o editó un inquilino para utilizar una conexión de federación de grid, ese inquilino se replica desde un sistema StorageGRID (el inquilino de origen) a otro sistema StorageGRID (el inquilino de réplica). Una vez que el inquilino se ha replicado, todos los grupos y usuarios agregados al inquilino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

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

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

Flujo de trabajo de inquilino para el clon de cuenta

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



Estos son los pasos principales del flujo de trabajo:

1 Inicie sesión en el inquilino

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

2 Opcionalmente, configure la federación de identidades

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

3 Crear grupos y usuarios

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

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

4 Crear claves de acceso S3

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

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

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

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

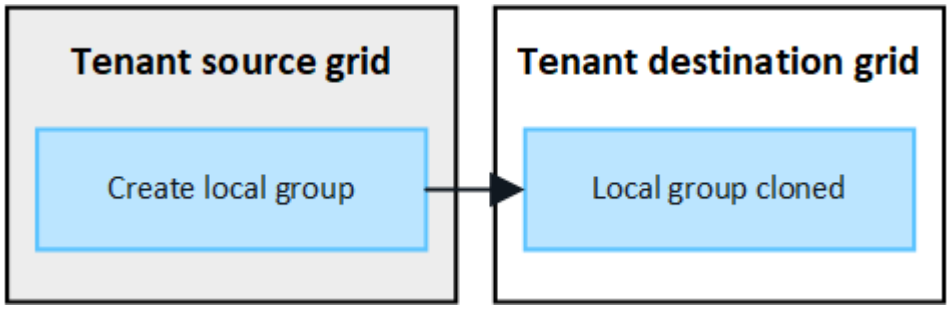
¿Cómo se clonan los grupos, los usuarios y las claves de acceso de S3?

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

Los grupos locales creados en la cuadrícula de origen se clonan

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

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

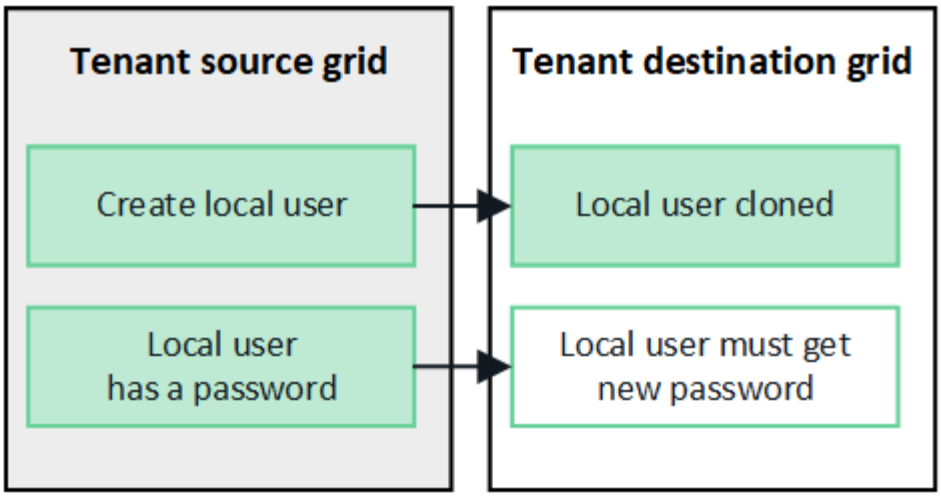


Los usuarios que seleccione al crear un grupo local en la cuadrícula de origen no se incluyen cuando el grupo se clona en la cuadrícula de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Los usuarios locales creados en la cuadrícula de origen se clonan

Cuando 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"Gestionar usuarios" .

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"Gestionar usuarios" .

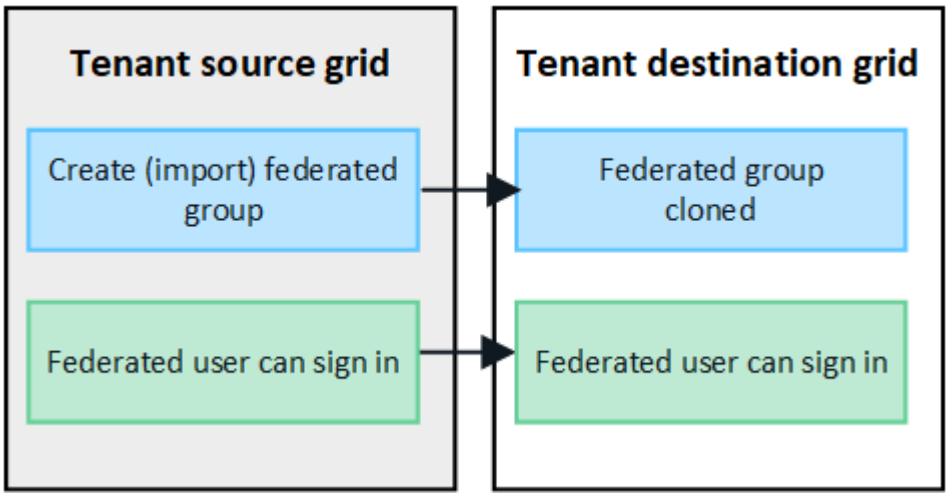


Los grupos federados creados en la cuadrícula de origen se clonan

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

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

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

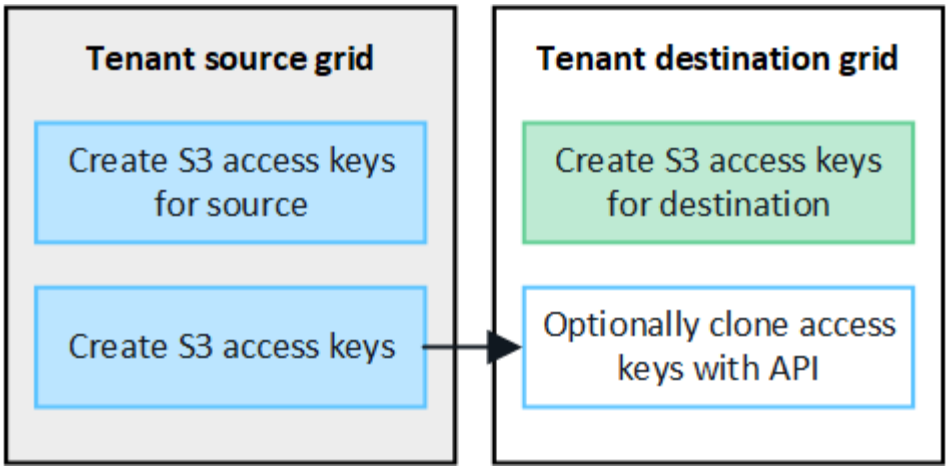


Las claves de acceso S3 se pueden clonar manualmente

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

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

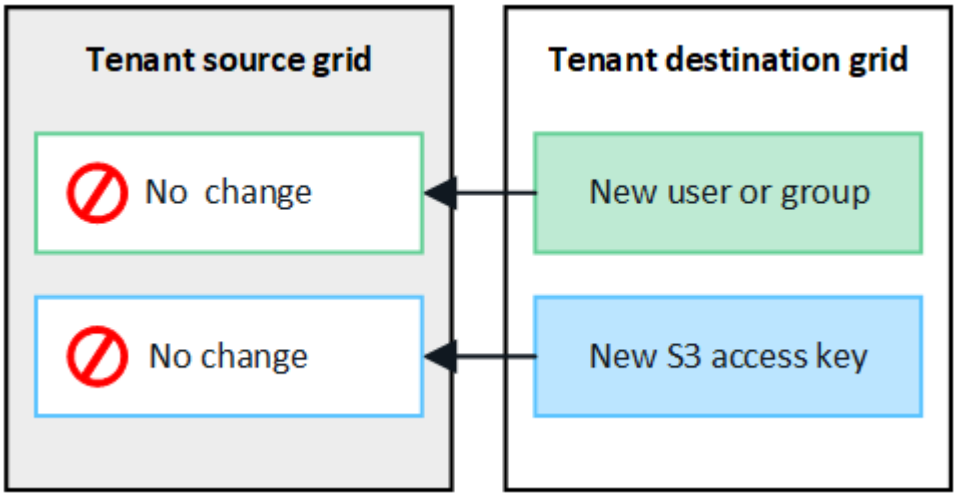
- Si no necesita utilizar las mismas claves para cada cuadrícula, puede hacerlo "cree sus propias claves de acceso" "crear claves de acceso de otro usuario"en cada cuadrícula.
- Si necesita utilizar las mismas claves en ambas cuadrículas, puede crear claves en la cuadrícula de origen y, a continuación,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



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

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

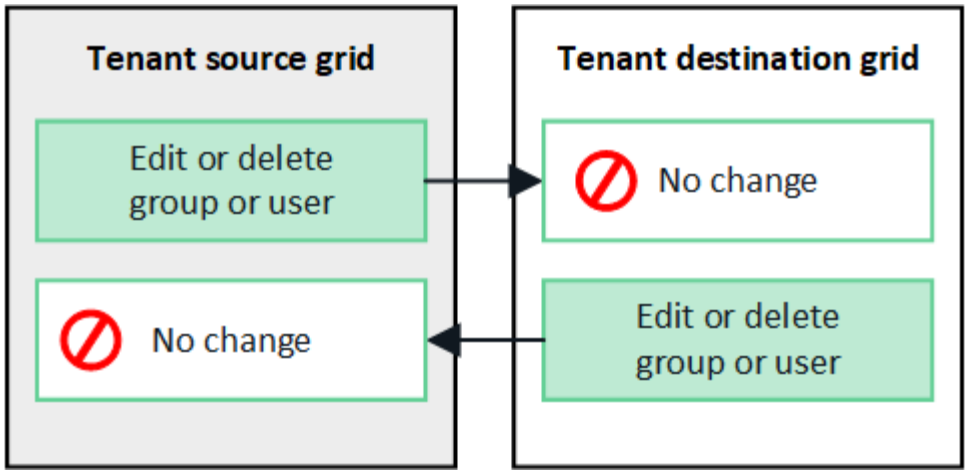
La clonación solo se produce desde la cuadrícula de origen del inquilino al grid de destino del inquilino. Si crea o importa grupos y usuarios en la cuadrícula de destino del inquilino, StorageGRID no clonará estos elementos de vuelta a la cuadrícula de origen del inquilino.



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

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

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



Clone las claves de acceso S3 mediante la API

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

Antes de empezar

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

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

Clone sus propias claves de acceso

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

Pasos

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

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

4. Seleccione **probar**.

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

   Asegúrese de conservar las comillas dobles alrededor de cada cadena.

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

Clonar las claves de acceso de otro usuario

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

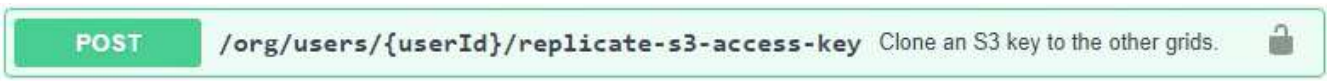
Pasos

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

      `GET /org/users`

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

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



5. Seleccione **probar**.

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

   Asegúrese de conservar las comillas dobles alrededor de la cadena.

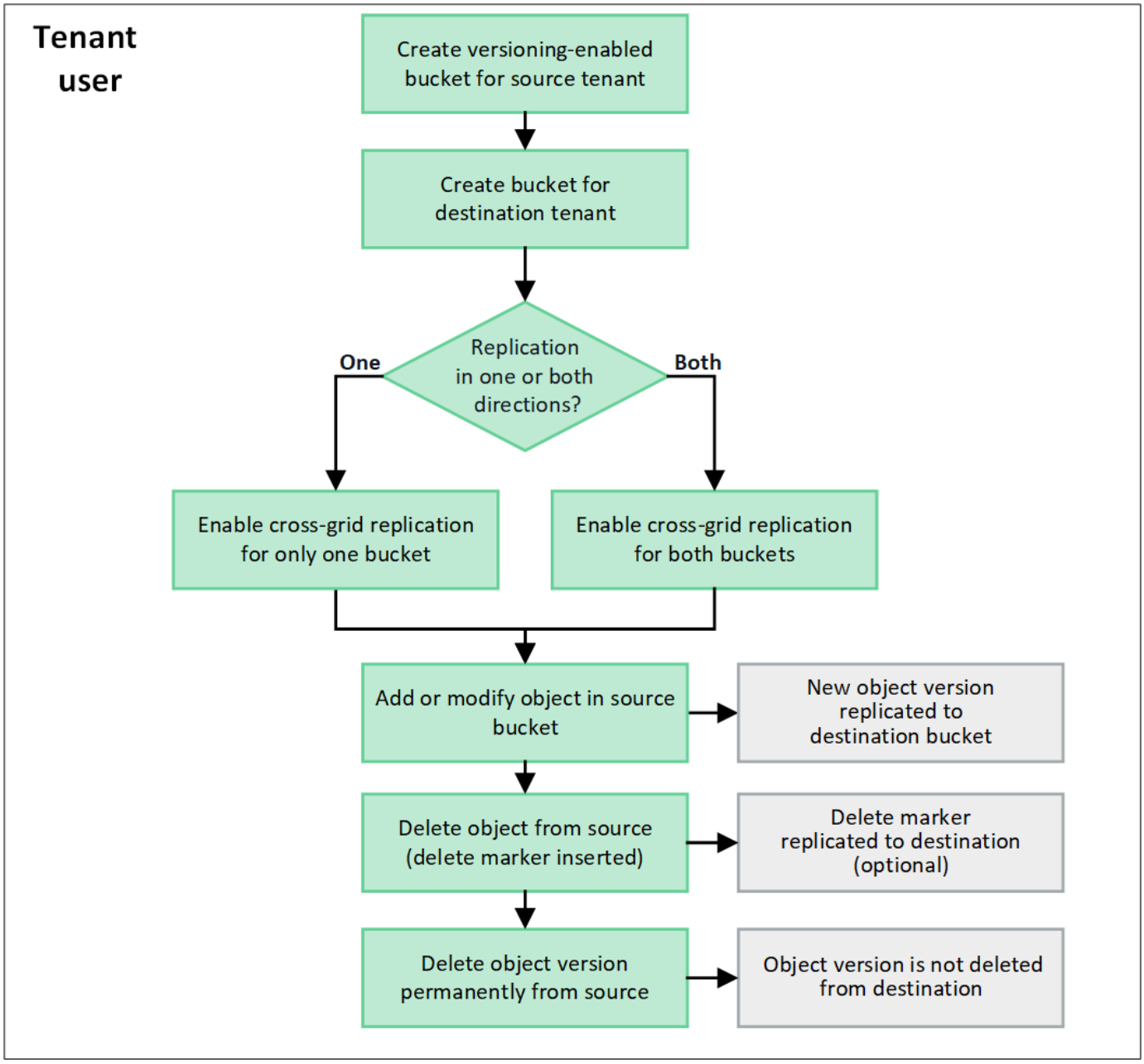
8. Si la clave caduca, reemplace la entrada de ejemplo para **Expires** con la fecha y hora de vencimiento como una cadena en formato ISO 8601 data-time (por ejemplo, `2023-02-28T22:46:33-08:00`). Si la clave no caduca, introduzca **null** como valor para la entrada **Expires** (o elimine la línea **Expires**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

Gestionar la replicación entre grid

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

Flujo de trabajo de replicación entre grid

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



Configurar la replicación entre grid

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

Antes de empezar

- Has revisado los requisitos para la replicación entre redes. Consulte "Qué es la replicación entre grid" .
- 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. Consulte "Gestione los inquilinos permitidos para la conexión de federación de grid" .
- El usuario inquilino con el que está iniciando sesión ya existe en ambas redes y pertenece a un grupo de usuarios que tiene la"Permiso de acceso raíz" .

- Si inicia 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

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

Pasos

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

      Si no puede iniciar sesión en la 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 "Cree un bucket de S3".

      Los nombres de los depósitos y las regiones pueden ser diferentes en cada cuadrícula.

   c. En la pestaña **Administrar configuración de objetos**, selecciona **Activar control de versiones de objetos**.
   d. Si el bloqueo de objetos S3 está habilitado para su sistema StorageGRID , consulte"Replicación entre cuadrículas con S3 Object Lock" .
   e. Seleccione **Crear cucharón**.
   f. Seleccione **Finalizar**.
2. Repita estos pasos para crear un depósito para la misma cuenta de inquilino en la otra red en la conexión de federación de red.

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

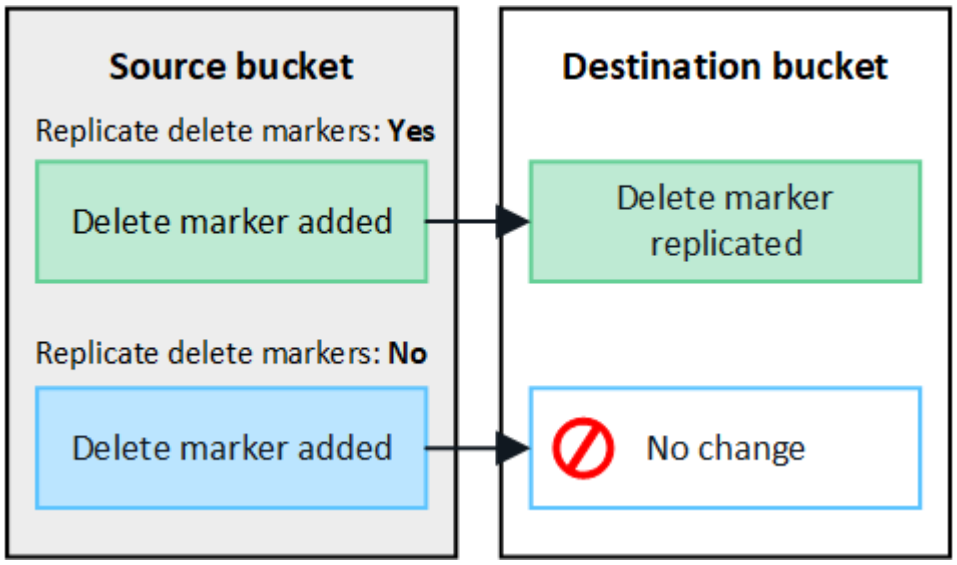
Habilite la replicación entre grid

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

Pasos

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

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

Referirse a"Qué es la replicación entre grid" Para más detalles.

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

   Después de unos momentos, aparece un mensaje de éxito. Los objetos agregados a este depósito ahora se replican 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 cucharón correspondiente en la otra cuadrícula y "permita la replicación entre grid en ambas direcciones".

Probar la replicación entre grids

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

Antes de empezar

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

Pasos

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

   Si la conexión es 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 más detalles, consulte"Solucionar errores de federación de grid" .

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

Desactive la replicación entre grid

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

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

- 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 activó la replicación entre grid para cada uno de los buckets (es decir, si la replicación se produce en ambas direcciones), puede deshabilitar la replicación entre grid para uno o ambos buckets. Por ejemplo, puede que desee desactivar la replicación de objetos de `my-bucket` Grid 1 a `my-bucket` Grid 2, mientras continúa replicando objetos de `my-bucket` Grid 2 a Grid `my-bucket` 1.
- Debe deshabilitar la replicación entre redes antes de poder quitar el permiso de un inquilino para usar la conexión de federación de red. Consulte "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 puede volver a activar la replicación a menos que ambos buckets estén vacíos.

Antes de empezar

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

Pasos

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

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

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

e. Seleccione **Desactivar replicación**.

f. Si está seguro de que desea deshabilitar la replicación entre redes para este 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 el otro grid. **La replicación entre redes** ya no se muestra como una característica habilitada en la página Buckets.

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

Ver conexiones de federación de grid

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

Antes de empezar

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

Pasos

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

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

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

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

Borrar el último error

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

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

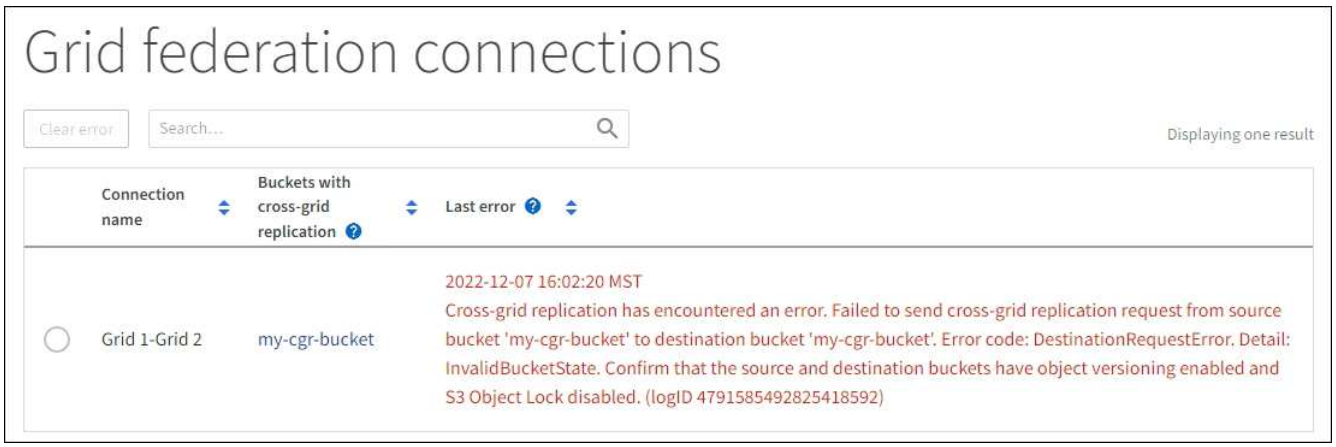
- Se ha suprimido el depósito de destino.
- Una cuenta diferente ha vuelto a crear el bloque de destino.
- Se ha suspendido el control de versiones del bloque de destino.
- La misma cuenta ha vuelto a crear el depósito de destino, pero ahora no tiene versiones.

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

Pasos

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

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



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

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

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

Gestionar grupos y usuarios

Usar la federación de identidades

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

utilizando credenciales conocidas.

Configurar la federación de identidades para el Administrador de inquilinos

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

Antes de empezar

- Has iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Está utilizando Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server como proveedor de identidad.

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

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

Acerca de esta tarea

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

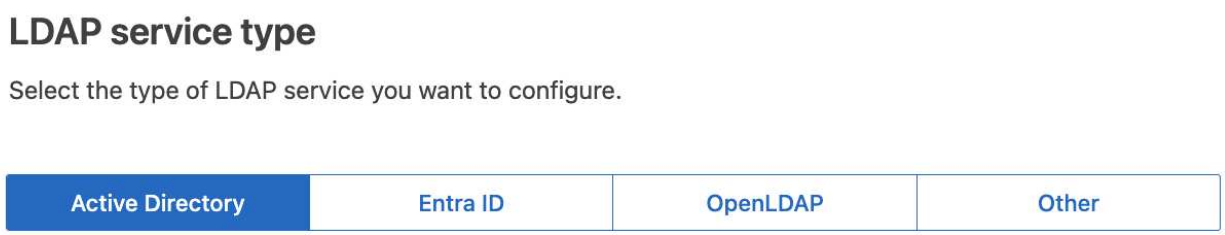
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Introducir configuración

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

Pasos

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



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

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

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

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

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

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

     - `sAMAccountName` o. `uid`

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

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

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

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

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

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

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

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

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

Introduzca uno de estos patrones:

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

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

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

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

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

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

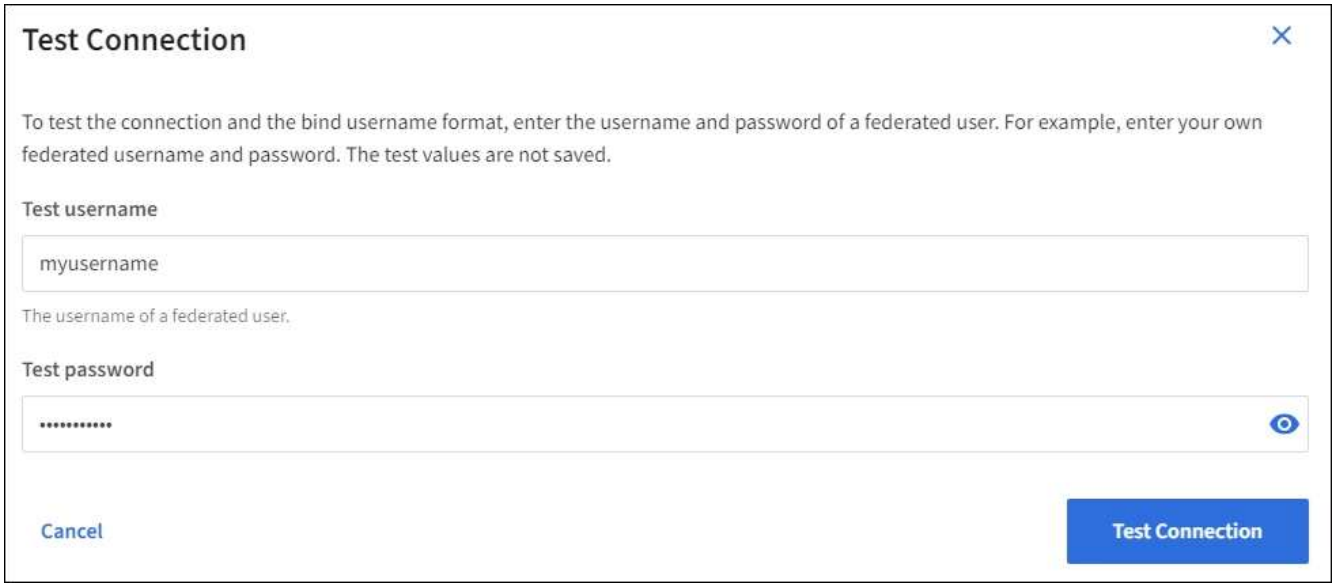
Pruebe la conexión y guarde la configuración

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

Pasos

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

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



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

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

Forzar la sincronización con el origen de identidades

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

Pasos

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

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

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

Deshabilitar la federación de identidades

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

Acerca de esta tarea

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

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

Pasos

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

Instrucciones para configurar el servidor OpenLDAP

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

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

Revestimientos memberOf y reft

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

Indización

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

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

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

Consulte la información sobre el mantenimiento inverso de miembros de grupo en la "Documentación de OpenLDAP: Guía del administrador de la versión 2.4".

Gestionar grupos de inquilinos

Cree grupos para un inquilino de S3

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

Antes de empezar

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

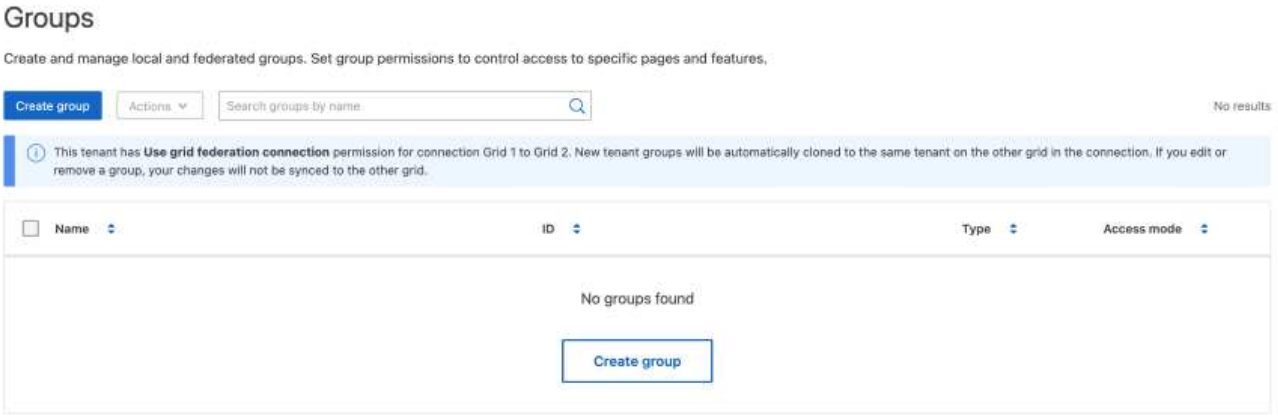
Acceda al asistente Crear grupo

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

Pasos

1. Seleccione **Administración de acceso** > **Grupos**.
2. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, confirme que aparece un

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



3. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

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

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

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

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

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

Administrar permisos de grupo

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

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:

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

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

2. Seleccione uno o más permisos para este grupo.

   Consulte "Permisos de gestión de inquilinos".

3. Seleccione **continuar**.

Establezca la política de grupo S3

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

Pasos

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

Política de grupo	Descripción
Sin acceso S3	Predeterminado. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que el acceso se conceda con una política de bloque. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3.
Acceso de sólo lectura	Los usuarios de este grupo tienen acceso de solo lectura a los recursos de S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puede editar esta cadena.
Acceso total	Los usuarios de este grupo tienen acceso completo a recursos de S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena.
Mitigación del ransomware	Esta política de ejemplo se aplica a todos los depósitos de este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden suprimir de forma permanente objetos de los bloques que tienen activado el control de versiones de objetos. Los usuarios del administrador de inquilinos que tienen el permiso **Administrar todos los cubos** pueden anular esta política de grupo. Limite el permiso Gestionar todos los buckets a usuarios de confianza y use la autenticación multifactor (MFA) cuando esté disponible.

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

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

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

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

Añadir usuarios (sólo grupos locales)

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

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

Pasos

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

   El grupo creado aparece en la lista de grupos.

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

Permisos de gestión de inquilinos

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

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

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

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

relacionadas.

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

Puede asignar los siguientes permisos a un grupo.

Permiso	Descripción	Detalles
Acceso raíz	Proporciona acceso completo al administrador de inquilinos y a la API de gestión de inquilinos.	
Gestione sus propias credenciales de S3	Permite a los usuarios crear y eliminar sus propias claves de acceso S3.	Los usuarios que no tienen este permiso no ven la opción de menú **STORAGE (S3)** > **My S3 access keys**.
Ver todos los cubos	Permite a los usuarios ver todos los depósitos y sus configuraciones.	Los usuarios que no tienen el permiso Ver todos los cubos o Gestionar todos los cubos no ven la opción de menú **Buckets**. Este permiso 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.
Gestionar todos los cucharones	Permite a los usuarios utilizar 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 de inquilino, independientemente de las políticas de grupo o depósito S3.	Los usuarios que no tienen el permiso Ver todos los cubos o Gestionar todos los cubos no ven la opción de menú **Buckets**. Este permiso 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.
Gestionar puntos finales	Permite a los usuarios utilizar el Gestor de inquilinos o la API de gestión de inquilinos para crear o editar puntos finales de servicio de plataforma, que se utilizan como destino para los servicios de plataforma de StorageGRID.	Los usuarios que no tienen este permiso no ven la opción de menú **Platform services endpoints**.
Utilice la pestaña Consola de S3	Cuando se combina con el permiso Ver todos los cubos o Gestionar todos los cubos, permite a los usuarios ver y gestionar objetos desde la pestaña Consola de S3 en la página de detalles de un bloque.	

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

Antes de empezar

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

Ver o editar grupo

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

Pasos

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

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

   - Un mensaje de banner indica que si edita o elimina un grupo, los cambios no se sincronizarán con la otra cuadrícula.
   - Según sea necesario, un mensaje de banner indica si los grupos no se clonaron en el inquilino en la cuadrícula de destino. Usted puede volver a intentar un clon de grupo que falló.
3. Si desea cambiar el nombre del grupo:
   a. Seleccione la casilla de verificación para el grupo.
   b. Seleccione **acciones** > **Editar nombre de grupo**.
   c. Introduzca el nuevo nombre.
   d. Selecciona **Guardar cambios.**
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre del grupo.
   - Selecciona la casilla de verificación del grupo y selecciona **Acciones** > **Ver detalles del grupo**.
5. Revise la sección Visión General, que muestra la siguiente información para cada grupo:
   - Nombre para mostrar
   - Nombre exclusivo
   - Tipo
   - Modo de acceso
   - Permisos
   - S3 Política
   - Número de usuarios en este grupo
   - Campos adicionales si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo el grupo en la cuadrícula de origen del inquilino:
     - Estado de clonación, ya sea **Success** o **Failure**

- Un banner azul que indica que si edita o elimina este grupo, los cambios no se sincronizarán con la otra cuadrícula.

6. Edite la configuración del grupo según sea necesario. Referirse a"Cree grupos para un inquilino de S3" para obtener detalles sobre qué ingresar.
   a. En la sección Descripción general, cambie el nombre mostrado seleccionando el nombre o el icono de edición .
   b. En la pestaña **Permisos de grupo**, actualice los permisos y seleccione **Guardar cambios**.
   c. En la pestaña **Política de grupo**, realice los cambios y seleccione **Guardar cambios**.

      Opcionalmente, seleccione una política de grupo S3 diferente o ingrese la cadena JSON para una política personalizada según sea necesario.

7. Para añadir uno o varios usuarios locales existentes al grupo:
   a. Seleccione la ficha Usuarios.

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

      Aparece un mensaje de éxito en la parte superior derecha.

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

      Aparece un mensaje de éxito en la parte superior derecha.

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

Grupo duplicado

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

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

Pasos

1. Seleccione **Administración de acceso** > **Grupos**.
2. Seleccione la casilla de control del grupo que desea duplicar.

3. Seleccione **acciones** > **Duplicar grupo**.
4. Ver"Cree grupos para un inquilino de S3" para obtener detalles sobre qué ingresar.
5. Seleccione **Crear grupo**.

Vuelva a intentar clonar el grupo

Para volver a intentar un clon que generó errores:

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

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

Elimine uno o más grupos

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

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

Pasos

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

   Se muestra un cuadro de diálogo de confirmación.

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

Configurar AssumeRole

Antes de empezar

Debe ser administrador para configurar AssumeRole.

Acerca de esta tarea

Para configurar AssumeRole, cree el grupo objetivo que se asumirá, si el grupo aún no existe. Edite la política S3 del grupo para especificar las acciones permitidas para asumir este grupo. Edite la política de confianza S3 del grupo para especificar los usuarios de confianza autorizados para asumir el grupo con la API AssumeRole.

Credenciales de seguridad temporales creadas asumiendo que este grupo es válido por un tiempo limitado. La sesión dura entre 15 minutos y 12 horas, y la sesión predeterminada es de 1 hora. Cuando se elimina al usuario de la política de confianza S3 del grupo, el usuario ya no podrá asumir este grupo.

Pasos

1. Seleccione **Administración de acceso** > **Grupos**.
2. Haga clic en el nombre del grupo.

3. Seleccione la pestaña **Política de confianza S3**.
4. Agregue su política de confianza S3, incluida una lista de usuarios que pueden realizar AssumeRole.
5. Seleccione **Guardar cambios**.
6. Seleccione la pestaña **Política de grupo S3**.
7. Edite la política S3 para especificar solo las acciones S3 requeridas para los usuarios de confianza agregados en la política de confianza S3 de este grupo.
8. Seleccione **Guardar cambios**.

Ejemplo de una política de confianza de AssumeRole S3

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

Una vez completada la configuración, los usuarios enumerados en la política de confianza de S3 pueden ejecutar AssumeRole y recibir credenciales. Los permisos finales están determinados por la política de grupo, la política de depósito y la política de sesión. Para más información, consulte "Utilizar políticas de acceso" .

Gestionar usuarios

Puede crear usuarios locales y asignarlos a grupos locales para determinar a qué funciones pueden acceder estos usuarios. También puedes importar usuarios federados. 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 el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el gestor de inquilinos o en la API de gestión de inquilinos, aunque pueden utilizar aplicaciones cliente para acceder a los recursos del inquilino, según los permisos del grupo.

Antes de empezar

- Ha iniciado sesión en el gestor de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, ha revisado el flujo de

trabajo y las consideraciones de "clonación de usuarios y grupos de inquilinos", y ha iniciado sesión en la cuadrícula de origen del inquilino.

Cree un usuario local

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

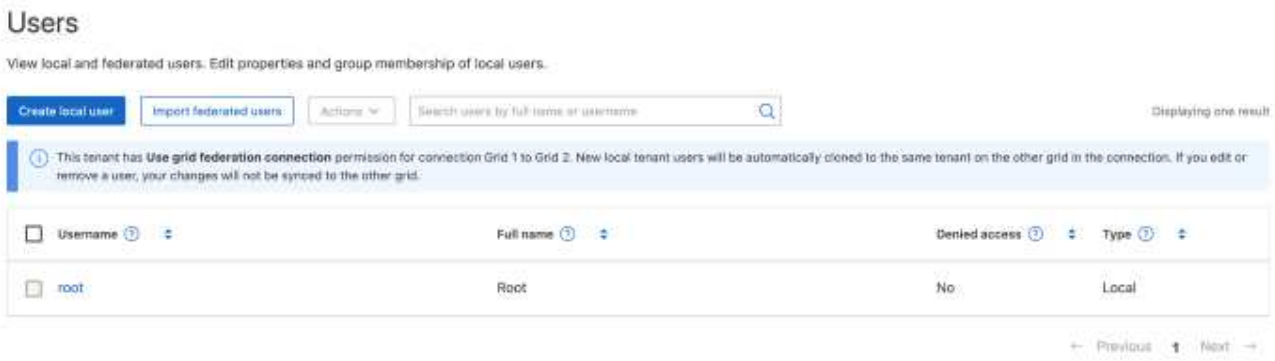
Los usuarios de S3 que no pertenecen a ningún grupo no tienen permisos de administración ni se les aplican S3 políticas de grupo. Es posible que estos usuarios tengan acceso a bloques de S3 otorgado a través de una política de bloques.

Acceda al asistente Crear usuario

Pasos

1. Seleccione **Administración de acceso** > **Usuarios**.

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



2. Seleccione **Crear usuario**.

Introduzca las credenciales

Pasos

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

Campo	Descripción
Nombre completo	El nombre completo de este usuario, por ejemplo, el nombre y apellidos de una persona o el nombre de una aplicación.
Nombre de usuario	Nombre que utilizará este usuario para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar. **Nota**: Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, se producirá un error de clonación si el mismo **Nombre de usuario** ya existe para el inquilino en la cuadrícula de destino.

Campo	Descripción
Contraseña y confirme la contraseña	La contraseña que el usuario utilizará inicialmente al iniciar sesión.
Denegar el acceso	Seleccione **Sí** para evitar que este usuario inicie sesión en la cuenta de inquilino, aunque todavía pertenezca a uno o más grupos. Por ejemplo, selecciona **Sí** para suspender temporalmente la capacidad de un usuario para iniciar sesión.

2. Seleccione **continuar**.

Asignar a grupos

Pasos

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

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

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

2. Seleccione **Crear usuario**.

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

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

Ver o editar usuario local

Pasos

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

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

   - Un mensaje de banner indica que si edita o elimina un usuario, los cambios no se sincronizarán con la otra cuadrícula.
   - Según sea necesario, un mensaje de banner indica si los usuarios no se clonaron en el inquilino en la cuadrícula de destino. Puede vuelva a intentar un clon de usuario que haya fallado.

3. Si desea cambiar el nombre completo del usuario:
   a. Seleccione la casilla de control para el usuario.
   b. Seleccione **acciones** > **Editar nombre completo**.

c. Introduzca el nuevo nombre.
d. Selecciona **Guardar cambios.**

4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre de usuario.
   - Selecciona la casilla de verificación para el usuario y selecciona **Acciones** > **Ver detalles de usuario**.
5. Revise la sección Visión General, que muestra la siguiente información para cada usuario:
   - Nombre completo
   - Nombre de usuario
   - Tipo de usuario
   - Acceso denegado
   - Modo de acceso
   - Pertenencia a grupos
   - Campos adicionales si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo al usuario en la cuadrícula de origen del inquilino:
     - Estado de clonación, ya sea **Success** o **Failure**
     - Un banner azul que indica que si edita este usuario, los cambios no se sincronizarán con la otra cuadrícula.
6. Edite la configuración del usuario según sea necesario. Consulte Crear usuario local para obtener más información acerca de lo que se debe introducir.
   a. En la sección Visión General, cambie el nombre completo seleccionando el nombre o el icono de edición .

      No puede cambiar el nombre de usuario.

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

Importar usuarios federados

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

Pasos

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

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

4. Seleccione **Importar**.

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

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

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

Usuario local duplicado

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

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

Pasos

1. Seleccione **Administración de acceso** > **Usuarios**.
2. Seleccione la casilla de control para el usuario que desea duplicar.
3. Seleccione **acciones** > **Duplicar usuario**.
4. Consulte Crear usuario local para obtener más información acerca de lo que se debe introducir.
5. Seleccione **Crear usuario**.

Reintente clonar el usuario

Para volver a intentar un clon que generó errores:

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

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

Elimine uno o varios usuarios locales

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

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

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

Pasos

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

   Se muestra un cuadro de diálogo de confirmación.

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

Gestión de claves de acceso de S3

Gestión de claves de acceso de S3

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

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

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

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

Cree sus propias claves de acceso S3

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

Antes de empezar

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

Acerca de esta tarea

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

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

- Establezca un tiempo de caducidad para sus llaves para limitar su acceso a un período de tiempo determinado. Establecer un tiempo de caducidad corto puede ayudar a reducir el riesgo si el ID de clave

de acceso y la clave de acceso secreta están expuestos accidentalmente. Las claves caducadas se eliminan automáticamente.

- Si el riesgo de seguridad en su entorno es bajo y no necesita crear periódicamente claves nuevas, no tiene que establecer un tiempo de caducidad para las claves. Si decide más tarde crear claves nuevas, elimine manualmente las claves antiguas.

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

Pasos

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

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

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

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

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

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

5. Copie el ID de la clave de acceso y la clave de acceso secreta a una ubicación segura, o seleccione **Descargar .csv** para guardar un archivo de hoja de cálculo que contenga el ID de clave de acceso y la clave de acceso secreta.

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

6. Seleccione **Finalizar**.

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

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

Consulte las claves de acceso de S3

Si está utilizando un inquilino de S3 y tiene el "permiso apropiado", puede ver una lista de las claves de acceso de S3. Puede ordenar la lista por tiempo de caducidad, de modo

que puede determinar qué claves caducarán pronto. Según sea necesario, puede "crear nuevas claves" o "teclas de eliminación" que ya no utilice.

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

Antes de empezar

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

Pasos

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

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

   Las claves caducadas se eliminan automáticamente.

Elimine sus propias claves de acceso de S3

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

Antes de empezar

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

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

Pasos

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

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

Cree las claves de acceso S3 de otro usuario

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

Pasos

1. Seleccione **Administración de acceso** > **Usuarios**.
2. Seleccione el usuario cuyas claves de acceso de S3 desee gestionar.

   Aparece la página de detalles del usuario.

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

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

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

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

6. Copie el ID de la clave de acceso y la clave de acceso secreta a una ubicación segura, o seleccione **Descargar .csv** para guardar un archivo de hoja de cálculo que contenga el ID de clave de acceso y la clave de acceso secreta.

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

7. Seleccione **Finalizar**.

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

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

Ver las claves de acceso S3 de otro usuario

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

Antes de empezar

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

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

Pasos

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

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

   Las claves caducadas se eliminan automáticamente.

Información relacionada

- "Cree las claves de acceso S3 de otro usuario"
- "Elimine las claves de acceso S3 de otro usuario"

Elimine las claves de acceso S3 de otro usuario

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

Antes de empezar

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

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

Pasos

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

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

Gestión de bloques S3

Cree un bloque de S3

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

Antes de empezar

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

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

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

- Si cada inquilino tendrá 5.000 buckets, cada nodo de almacenamiento del grid tiene un mínimo de 64 GB de RAM.

> Cada cuadrícula puede tener un máximo de 100.000 contenedores, incluidos"cubos de ramas" .

Acceda al asistente

Pasos

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

Introduzca los detalles

Pasos

1. Introduzca los detalles del cucharón.

Campo	Descripción
Nombre del bloque	Un nombre para el depósito que cumple con estas reglas: • Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino). • Debe ser compatible con DNS. • Debe 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 periodos en las solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor. Para obtener más información, consulte la "Documentación de Amazon Web Services (AWS) sobre reglas de nomenclatura de bloques". **Nota**: No puedes cambiar el nombre del cubo después de crear el cubo.
Región	La región del cubo. 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. Si la región predeterminada está configurada en una región distinta a `us-east-1` , esta otra región se selecciona inicialmente en el menú desplegable. **Nota**: No puedes cambiar la región después de crear el cubo.

2. Seleccione **continuar**.

Gestionar configuración

Pasos

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

   Habilite el control de versiones de objetos si desea almacenar cada versión de cada objeto en este bloque. A continuación, puede recuperar versiones anteriores de un objeto según sea necesario.

   Debe habilitar el control de versiones de objetos si:

   - El contenedor se utilizará para la replicación entre redes.
   - Quieres crear un"cubo de rama" de este cubo.

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

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

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

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

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

   > El administrador de grid debe darle permiso a "Utilice características específicas de S3 Object Lock".

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

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

Modo de retención predeterminado	Descripción
Gobernanza	• Los usuarios con `s3:BypassGovernanceRetention` permiso pueden utilizar `x-amz-bypass-governance-retention: true` la cabecera de solicitud para omitir la configuración de retención. • Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Modo de retención predeterminado	Descripción
Cumplimiento de normativas	• El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta. • La fecha de retención del objeto se puede aumentar, pero no se puede reducir. • No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha. **Nota**: Su administrador de grid debe permitirle usar el modo de cumplimiento.

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

   El **período de retención predeterminado** indica cuánto tiempo deben conservarse los nuevos objetos agregados a este depósito, a partir del momento en que se ingieren. Especifique un valor inferior o igual al período de retención máximo del inquilino, según lo establece el administrador de grid.

Un período de retención *maximum*, que puede ser un valor de 1 día a 100 años, se establece cuando el administrador de grid crea el inquilino. Cuando establece un período de retención *default*, no puede exceder el valor establecido para el período de retención máximo. Si es necesario, pida al administrador de grid que aumente o reduzca el período de retención máximo.

4. Opcionalmente, seleccione **Habilitar límite de capacidad**, ingrese un valor y seleccione la unidad de capacidad.

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

   Si no se establece ningún límite, la capacidad de este depósito es ilimitada. Consulte "Límite de uso de capacidad" si desea obtener más información.

5. Opcionalmente, seleccione **Habilitar límite de conteo de objetos**.

   El límite de conteo de objetos es la cantidad máxima de objetos que este depósito puede contener. Este valor representa una cantidad lógica (cantidad de objetos). Si no se establece ningún límite, el número de objetos es ilimitado.

6. Seleccione **Crear cucharón**.

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

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

También puedes"crear depósitos de ramas" según sea necesario.

Ver detalles del período

Puede ver los depósitos en su cuenta de inquilino.

Antes de empezar

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

Pasos

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

   Aparecerá la página Buckets.

2. Revise la tabla de resumen de cada segmento.

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

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

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

   Funciones activadas
   Lista de funciones activadas para el depósito.

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

   Esta columna sólo aparece si Bloqueo de objetos S3 está activado para la cuadrícula. Esta columna también muestra información para todos los segmentos compatibles anteriores.

   Región
   La región del cubo, que no se puede cambiar. Esta columna está oculta por defecto.

   Recuento de objetos
   Núm. De objetos en este depósito. Si los cubos tienen el control de versiones activado, se incluyen versiones de objetos no actuales en este valor.

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

   Espacio utilizado
   El tamaño lógico de todos los objetos del bloque. El tamaño lógico no incluye el espacio real necesario para las copias replicadas o con código de borrado o para los metadatos de objetos.

   Este valor puede tardar hasta 10 minutos en actualizarse.

   Uso
   El porcentaje utilizado del límite de capacidad del bloque, si se estableció uno.

   El valor de uso se basa en estimaciones internas y puede superarse en algunos casos. Por ejemplo, StorageGRID comprueba el límite de capacidad (si está configurado) cuando un inquilino comienza a

cargar objetos y rechaza entradas nuevas en este bloque si el inquilino ha superado el límite de capacidad. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha superado el límite de capacidad. Si se eliminan objetos, es posible que un inquilino no cargue temporalmente objetos nuevos en este depósito hasta que se vuelva a calcular el uso de 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 está configurado, el límite de capacidad para el cucharón.

Fecha de creación

La fecha y la hora en la que se creó el bloque. Esta columna está oculta por defecto.

3. Para ver los detalles de un cubo específico, seleccione el nombre del cubo en la tabla.
   a. Consulte la información de resumen en la parte superior de la página web para confirmar los detalles del depósito, como Región y Recuento de objetos.
   b. Vea las barras de uso del límite de capacidad y del límite de uso del recuento de objetos. 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 cubo** y **Eliminar cubo**.

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

      - "Eliminar todos los objetos de un depósito"
      - "Eliminar un cubo" (el cucharón 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 cubo. Para obtener más información, consulte "Utilice la consola S3".
      - **Opciones de cubo**: Ver o cambiar la configuración de las opciones. Algunas configuraciones, como Bloqueo de objetos S3, no se pueden cambiar después de crear el depósito.
        - "Gestione la coherencia de los bloques"
        - "Últimas actualizaciones de hora de acceso"
        - "Límite de capacidad"
        - "Límite de conteo de objetos"
        - "Control de versiones de objetos"
        - "Bloqueo de objetos de S3"
        - "Retención de cucharón por defecto"
        - "Gestionar la replicación entre grid" (si está permitido para el inquilino)
      - **Servicios de la plataforma**: "Gestione los servicios de la plataforma" (Si está permitido para el inquilino)
      - **Acceso a cubos**: Ver o cambiar la configuración de opciones. Debe tener permisos de acceso específicos.
        - Configurar"CORS para depósitos y objetos" De esta forma, el depósito y los objetos dentro del

depósito serán accesibles para las aplicaciones web en otros dominios.

    - "Controle el acceso de usuarios" Para un cubo S3 y objetos en ese cubo.
- **Ramas**: Ver la lista de ramas para el depósito. "Crear un nuevo depósito de ramas o administrar depósitos de ramas" .

¿Qué es un bucket de rama?

Un bucket de rama proporciona acceso a los objetos de un bucket tal como existían en un momento determinado.

Crea un bucket de rama a partir de un bucket existente. Después de crear un bucket de rama, el bucket original desde el cual se creó se denomina *bucket base*. Además, puedes crear un bucket de rama a partir de otro bucket de rama.

Un bucket de rama proporciona acceso a datos protegidos, pero no sirve como respaldo. Para continuar protegiendo los datos, utilice estas funciones en los depósitos base:

- "Bloqueo de objetos de S3"
- "Replicación entre grid"para cubos de base
- "Políticas de cubos"para que los depósitos versionados limpien versiones antiguas de objetos

Tenga en cuenta las siguientes características de los grupos de ramas:

- Puede acceder a los objetos en los depósitos de ramas mediante"Consola S3 para descargar objetos" .
- Cuando los clientes acceden a objetos en un depósito de rama, el depósito de rama"políticas de acceso" , en lugar de las políticas del depósito base, determinan si se concede o se deniega el acceso.
- Los objetos creados en un depósito base se evalúan en función de cómo"Reglas de ILM" aplicar al cubo base. Los objetos creados en un bucket de rama se evalúan en función de cómo se aplican las reglas de ILM al bucket de rama.
- La replicación entre redes no es compatible con los grupos de sucursales.
- Los servicios de plataforma no son compatibles con los grupos de sucursales.

Ejemplos de uso de depósitos de sucursales

- Puede utilizar un depósito de rama para eliminar objetos corruptos creando un depósito de rama desde un punto en el tiempo anterior a la ocurrencia de la corrupción y luego apuntando las aplicaciones al depósito de rama en lugar de al depósito base que contiene los objetos corruptos.
- Estás guardando datos en un depósito versionado. Hubo una vulnerabilidad accidental que provocó que se ingieran muchos objetos no deseados después del tiempo *T*. Puede crear un depósito de rama para el valor de tiempo anterior, *T*, y redirigir las operaciones del cliente a ese depósito de rama. Luego, solo los objetos ingeridos antes del tiempo anterior *T* se exponen a los clientes.

Operaciones sobre objetos en depósitos de ramas

- Una operación PUT de objeto en un bucket de rama crea un objeto en la rama.
- Una operación GET de objeto en un bucket de rama recupera un objeto de la rama. Si el objeto no existe en el depósito de la rama, el objeto se recupera del depósito base.
- Las eliminaciones de objetos de los depósitos de ramas ocurren de la siguiente manera:

Funcionamiento	Objetivo	Resultado	Visibilidad de objetos en el depósito base	Visibilidad de objetos en el bucket de la rama
Eliminar sin ID de versión	Cubo base	El marcador de eliminación se crea solo para el depósito base	HEAD/GET devuelve El objeto no existe, pero aún se puede acceder a versiones específicas	HEAD/GET devuelve El objeto existe y aún se puede acceder a versiones específicas El marcador de eliminación se habría creado después del depósito de la rama. `beforeTime` .
Eliminar con ID de versión	Cubo base	Se elimina la versión de objeto específica tanto para el depósito base como para el de la rama	HEAD/GET devuelve La versión del objeto no existe	HEAD/GET devuelve La versión del objeto no existe
Eliminar sin ID de versión	Cubo de rama	El marcador de eliminación se crea solo para el depósito de la rama	HEAD/GET devuelve un objeto (el objeto del depósito base no se ve afectado)	HEAD/GET devuelve El objeto no existe
Eliminar con ID de versión	Cubo de rama	La versión de objeto específica se elimina solo para el depósito de la rama	HEAD/GET devuelve la versión específica del objeto (el objeto del bucket base no se ve afectado)	HEAD/GET devuelve La versión del objeto no existe

Consulte también"Cómo se eliminan los objetos con versiones de S3" .

Administrar grupos de sucursales

Utilice el Administrador de inquilinos para crear y ver detalles de las sucursales.

Antes de empezar

- Has iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Pertenece a un grupo de usuarios que tiene acceso root o"Permite gestionar todos los depósitos" . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.
- El depósito base desde el cual desea crear una rama tiene"control de versiones habilitado" .
- Eres el propietario del cubo base.

Acerca de esta tarea

Tenga en cuenta la siguiente información para los grupos de ramas:

- Los permisos para establecer las propiedades de bloqueo de objetos S3 de depósitos u objetos se pueden otorgar mediante"política de bloques o política de grupo" .
- Si suspende el control de versiones en el bucket base, el contenido del bucket base ya no será visible en

sus buckets de rama.

Después de configurar y crear un bucket de rama, no podrá cambiar la configuración.

Crear un depósito de ramas

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione el depósito desde el cual desea crear una rama (el "depósito base").
3. En la página de detalles del depósito, seleccione **Ramas** > **Crear depósito de ramas**.

   El botón **Crear rama de depósito** está deshabilitado si el depósito base no tiene habilitada la versión.

Introduzca los detalles

Pasos

1. Introduzca detalles para la sucursal.

Campo	Descripción
Nombre del depósito de la rama	Un nombre para la rama que cumple con estas reglas: • Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino). • Debe ser compatible con DNS. • Debe 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 periodos en las solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor. Para obtener más información, consulte la "Documentación de Amazon Web Services (AWS) sobre reglas de nomenclatura de bloques". **Nota**: No puedes cambiar el nombre después de crear la rama.
Región (no se puede modificar para los depósitos de sucursales)	Región del depósito de la rama. La región del depósito de la rama debe coincidir con la región del depósito base, por lo que este campo está deshabilitado para los depósitos de la rama.
Antes de tiempo	El tiempo límite para que las versiones de objetos creadas en el depósito base sean accesibles desde el depósito de la rama. El contenedor de ramas proporciona acceso a versiones de objetos creadas antes del tiempo anterior. Antes del tiempo debe haber una fecha y hora que haya pasado. No puede ser una fecha futura.

Campo	Descripción
Tipo de cubo de rama	• **Lectura y escritura**: puede agregar o eliminar objetos o versiones de objetos en el depósito de ramas. • **Solo lectura**: no puedes modificar objetos en el bucket de la rama. **Nota**: Puede configurar el tipo de depósito de la rama como de solo lectura únicamente si el depósito de la rama está vacío. Si el tipo de un depósito de rama existente está configurado como lectura y escritura y no ha escrito en él, puede cambiar el tipo a solo lectura.

2. Seleccione **continuar**.

Administrar la configuración de objetos (opcional)

Las configuraciones de objetos para un bucket de rama no afectan las versiones de objetos en el bucket base.

Pasos

1. Si la configuración global de Bloqueo de objetos S3 está habilitada, habilite opcionalmente el Bloqueo de objetos S3 para el depósito de ramas. Para habilitar el bloqueo de objetos S3, el depósito de la rama debe ser un depósito de lectura y escritura.

   Habilite el bloqueo de objetos S3 para un bucket de rama 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 al depósito de la rama que no se pueden modificar. Es posible que no puedas eliminar estos objetos ni la rama en sí.

2. Si seleccionó **Habilitar bloqueo de objetos S3**, habilite opcionalmente la **Retención predeterminada** para el depósito de la rama.

   > El administrador de grid debe darle permiso a "Utilice características específicas de S3 Object Lock".

   Cuando la **Retención predeterminada** está habilitada, los objetos nuevos agregados al depósito de la rama 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 de la rama.

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

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

   El **Período de retención predeterminado** indica durante cuánto tiempo se deben conservar los objetos nuevos agregados al depósito de la rama, 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.

Un período de retención *maximum*, que puede ser un valor de 1 día a 100 años, se establece cuando el administrador de grid crea el inquilino. Cuando establece un período de retención *default*, no puede exceder el valor establecido para el período de retención máximo. Si es necesario, pida al administrador de grid que aumente o reduzca el período de retención máximo.

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

   El límite de capacidad es la capacidad máxima disponible para el depósito de la sucursal. Este valor representa una cantidad lógica (tamaño del objeto), no una cantidad física (tamaño en disco).

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

   > Esta configuración se aplica solo a los objetos ingeridos directamente en el bucket de la rama, y no a los objetos que son visibles desde el bucket base a través del bucket de la rama.

4. Opcionalmente, seleccione **Habilitar límite de conteo de objetos**.

   El límite de recuento de objetos es la cantidad máxima de objetos que el depósito de la rama puede contener. Este valor representa una cantidad lógica (cantidad de objetos). Si no se establece ningún límite,

el número de objetos es ilimitado.

> Esta configuración se aplica solo a los objetos ingeridos directamente en el bucket de la rama, y no a los objetos que son visibles desde el bucket base a través del bucket de la rama.

5. Seleccione **Crear cucharón**.

   El depósito de ramas 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 de la rama" y realizar una configuración adicional.

   En la página de detalles del depósito, algunas opciones de configuración relacionadas con la modificación de objetos están deshabilitadas para los depósitos de solo lectura.

Aplique una etiqueta de política de ILM a un bloque

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

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

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

Antes de empezar

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

Pasos

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

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

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

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

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

3. En la pestaña Bucket options, expanda el acordeón de etiqueta de política de ILM. Este acordeón solo aparece si el administrador de grid ha habilitado el uso de etiquetas de política personalizadas.

4. Lea la descripción de cada etiqueta de política para determinar qué etiqueta se debe aplicar al depósito.

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

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

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

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

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

Gestione la política de bloques

Puede controlar el acceso de los usuarios a un bloque de S3 y los objetos de ese bloque.

Antes de empezar

- Ha iniciado sesión en el gestor de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz". Los permisos Ver todos los buckets y Gestionar todos los buckets sólo permiten la visualización.
- Verificó que el número necesario de nodos y sitios de almacenamiento está disponible. Si no hay dos o más nodos de almacenamiento disponibles en ningún sitio, o si no hay un sitio disponible, los cambios realizados en estos ajustes podrían no estar disponibles.

Pasos

1. Seleccione **Buckets**, luego seleccione el bucket que desea administrar.
2. En la página de detalles del cubo, selecciona **Acceso al cubo** > **Política del cubo**.
3. Debe realizar una de las siguientes acciones:
   - Introduzca una política de cubo seleccionando la casilla de verificación **Habilitar política**. A continuación, introduzca una cadena con formato JSON válida.

     Cada política de bloque tiene un límite de tamaño de 20.480 bytes.

   - Modifique una política existente editando la cadena.
   - Desactive una política desseleccionando **Habilitar política**.

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

Gestione la coherencia de los bloques

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

Antes de empezar

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

Directrices de coherencia de bloques

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

Cambie la consistencia del bloque

Si la consistencia de **Read-after-new-write** no cumple con los requisitos de la aplicación cliente, puede cambiar la consistencia configurando la consistencia del depósito o usando el `Consistency-Control` encabezado. El `Consistency-Control` cabezal anula la consistencia del cucharón.

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

Pasos

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

   Aparece la página de detalles bucket.

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

existen). No se admite para bloques de FabricPool S3.

5. Seleccione **Guardar cambios**.

Qué sucede cuando se cambia la configuración del bloque

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

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

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

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

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

- "Configuración de servicios de plataforma: Notificación, replicación o integración de búsqueda"
- "Configurar StorageGRID CORS para depósitos y objetos"
- Cambie la consistencia del cucharón

> 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 `Consistency-Control` la cabecera para "API REST DE S3"o mediante las `force` opciones o. `reducedConsistency`"API de gestión de inquilinos"

Activar o desactivar las actualizaciones de la hora del último acceso

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

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

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

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

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

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

Tipo de solicitud	Comportamiento si la hora del último acceso está desactivada (valor predeterminado)		Comportamiento si la hora del último acceso está activada	
	¿Hora de último acceso actualizada?	¿Objeto añadido a la cola de evaluación de ILM?	¿Hora de último acceso actualizada?	¿Objeto añadido a la cola de evaluación de ILM?

Solicitud para recuperar los metadatos de un objeto cuando se emite una operación HEAD	No	No	No	No
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
Solicitar la lista de objetos o versiones de objetos	No	No	No	No
Solicite copiar un objeto de un bloque a otro	• No, para la copia de origen • Sí, para la copia de destino	• No, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Pasos

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

   Aparece la página de detalles bucket.

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

Cambiar el control de versiones del objeto para un bloque

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

Antes de empezar

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

- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.
- Verificó que el número necesario de nodos y sitios de almacenamiento está disponible. Si no hay dos o más nodos de almacenamiento disponibles en ningún sitio, o si no hay un sitio disponible, los cambios realizados en estos ajustes podrían no estar disponibles.

Acerca de esta tarea

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

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

Para obtener más información, consulte lo siguiente:

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

Pasos

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

   Aparece la página de detalles bucket.

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

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

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

5. Seleccione **Guardar cambios**.

Utilice Bloqueo de objetos S3 para retener objetos

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

> Su administrador de grid debe darle permiso para usar características específicas de S3 Object Lock.

¿Qué es el bloqueo de objetos de S3?

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

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

Un cubo sin S3 Object Lock solo puede tener objetos sin ajustes de retención especificados. Ningún objeto ingerido tendrá valores de retención.

Un cubo con S3 Object Lock puede tener objetos con y sin ajustes de retención especificados por las aplicaciones cliente S3. Algunos objetos ingeridos tendrán valores de retención.

Un cubo con S3 Object Lock y la retención predeterminada configurada puede haber cargado objetos con ajustes de retención especificados y nuevos objetos sin ajustes de retención. Los nuevos objetos utilizan la configuración predeterminada, ya que la configuración de retención no se ha configurado a nivel de objeto.

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

Modos de retención

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

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

Configuración de retención para versiones de objetos

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

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

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

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

Valor de retención predeterminado para los depósitos

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

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

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

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

S3 Tareas de bloqueo de objetos

Las siguientes listas para administradores de grid y usuarios de tenant contienen las tareas de alto nivel para utilizar la función Bloqueo de objetos S3.

Administrador de grid

- Active la configuración de bloqueo de objetos S3 global para todo el sistema StorageGRID.
- Asegúrese de que las políticas de gestión del ciclo de vida de la información (ILM) son *obedientes*; es decir, cumplen con el "Requisitos de los depósitos con bloqueo de objetos S3 activado".
- Según sea necesario, permita que un inquilino utilice Compliance como modo de retención. De lo contrario, sólo se permite el modo Gobernanza.
- Según sea necesario, defina un período de retención máximo para un inquilino.

Usuario inquilino

- Revise las consideraciones sobre bloques y objetos con S3 Object Lock.
- Según sea necesario, póngase en contacto con el administrador de cuadrícula para habilitar la configuración global de bloqueo de objetos S3 y establecer permisos.
- Crear cubos con bloqueo de objetos S3 activado.
- Opcionalmente, configure los valores de retención predeterminados para un bloque:

    - Modo de retención predeterminado: Gobernanza o Cumplimiento, si lo permite el administrador de grid.
    - Período de retención predeterminado: Debe ser inferior o igual al período de retención máximo definido por el administrador de grid.
- Utilice la aplicación cliente S3 para agregar objetos y, opcionalmente, establecer una retención específica de objetos:
    - Modo de retención. Gobernanza o cumplimiento de normativas, si lo permite el administrador de grid.
    - Retener hasta fecha: Debe ser menor o igual que lo permitido por el período de retención máximo definido por el administrador de grid.

Requisitos para bloques con bloqueo de objetos de S3 habilitado

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

Requisitos para objetos en bloques con S3 Object Lock habilitado

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

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

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

1. **Procesamiento de objetos**

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

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

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

2. **Retención y eliminación de objetos**

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

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

¿Puedo seguir gestionando los depósitos compatibles heredados?

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

Actualizar S3 Retención predeterminada de bloqueo de objetos

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

Antes de empezar

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

Pasos

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

   Aparece la página de detalles bucket.

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

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

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

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

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

   El **período de retención predeterminado** indica cuánto tiempo deben conservarse los nuevos objetos agregados a este depósito, a partir del momento en que se ingieren. Especifique un valor inferior o igual al período de retención máximo del inquilino, según lo establece el administrador de grid.

   Un período de retención *maximum*, que puede ser un valor de 1 día a 100 años, se establece cuando el administrador de grid crea el inquilino. Cuando establece un período de retención *default*, no puede exceder el valor establecido para el período de retención máximo. Si es necesario, pida al administrador de grid que aumente o reduzca el período de retención máximo.

7. Seleccione **Guardar cambios**.

Configurar StorageGRID CORS para depósitos y objetos

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

Antes de empezar

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

- Para OBTENER solicitudes de configuración de CORS, pertenece a un grupo de usuarios que tiene el "Permite gestionar todos los bloques o ver todos los bloques". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.
- Para las solicitudes de configuración de PUT CORS, pertenece a un grupo de usuarios que tiene el "Permite gestionar todos los depósitos". Este permiso anula la configuración de permisos en las políticas de grupo o bloque.
- El "Permiso de acceso raíz" proporciona acceso a todas las solicitudes de configuración de CORS.

Acerca de esta tarea

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

Activar CORS para un cucharón

Pasos

1. Utilice un editor de texto para crear el XML necesario. Este ejemplo muestra el XML utilizado para habilitar CORS para un bloque de S3. Específicamente:
   - Permite que cualquier dominio envíe solicitudes GET al depósito
   - Solo permite que `http://www.example.com` el dominio envíe solicitudes GET, POST y DELETE
   - Se permiten todas las cabeceras 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 cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
3. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

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

Modificar el ajuste de CORS

Pasos

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

Desactive el ajuste CORS

Pasos

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

Información relacionada

"Configurar StorageGRID CORS para una interfaz de administración"

Suprimir objetos del depósito

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

Consideraciones y requisitos

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

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

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

- Mientras los objetos se eliminan, el estado del depósito es **Eliminando objetos: Solo lectura**. En este estado, no puede agregar nuevos objetos al depósito.
- Cuando todos los objetos se han eliminado, el bloque permanece en su estado de solo lectura. Puede realizar una de las siguientes acciones:
  - Vuelva a colocar el depósito en modo de escritura y reutilícelo para objetos nuevos
  - Elimine el cucharón

- Mantenga el bucket en modo de solo lectura para reservar su nombre para uso futuro

- Si un bloque tiene el control de versiones de objetos activado, los marcadores de eliminación que se crearon en StorageGRID 11,8 o posterior se pueden eliminar mediante la eliminación de objetos en las operaciones de bloque.
- Si un bloque tiene el control de versiones de objetos activado, la operación de supresión de objetos no eliminará los marcadores de supresión creados en StorageGRID 11,7 o anteriores. Consulte la información sobre la supresión de objetos en un depósito en "Cómo se eliminan los objetos con versiones de S3".
- Si utiliza "replicación entre grid", tenga en cuenta lo siguiente:
  - El uso de esta opción no elimina ningún objeto del depósito en la otra cuadrícula.
  - Si selecciona esta opción para el depósito de origen, se activará la alerta **Fallo de replicación entre redes** si agrega objetos al depósito de destino en la otra cuadrícula. Si no puede garantizar que nadie agregará objetos al depósito de la otra cuadrícula, "desactive la replicación entre grid" para ese depósito antes de eliminar todos los objetos del depósito.

Antes de empezar

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

Pasos

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

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

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

   Menú Actions

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

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

   Detalles

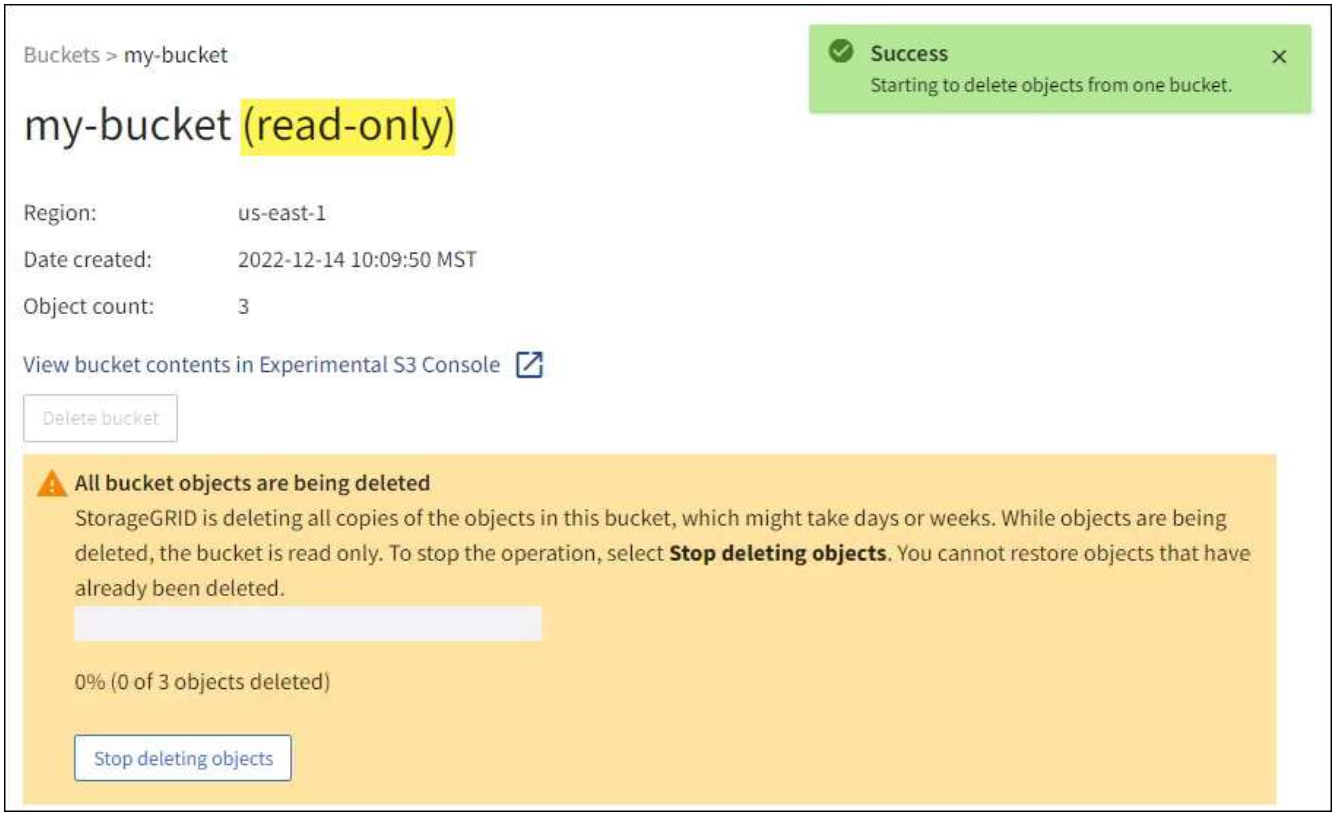
   a. Seleccione un nombre de cubo para mostrar sus detalles.

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

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

   Después de unos minutos:

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

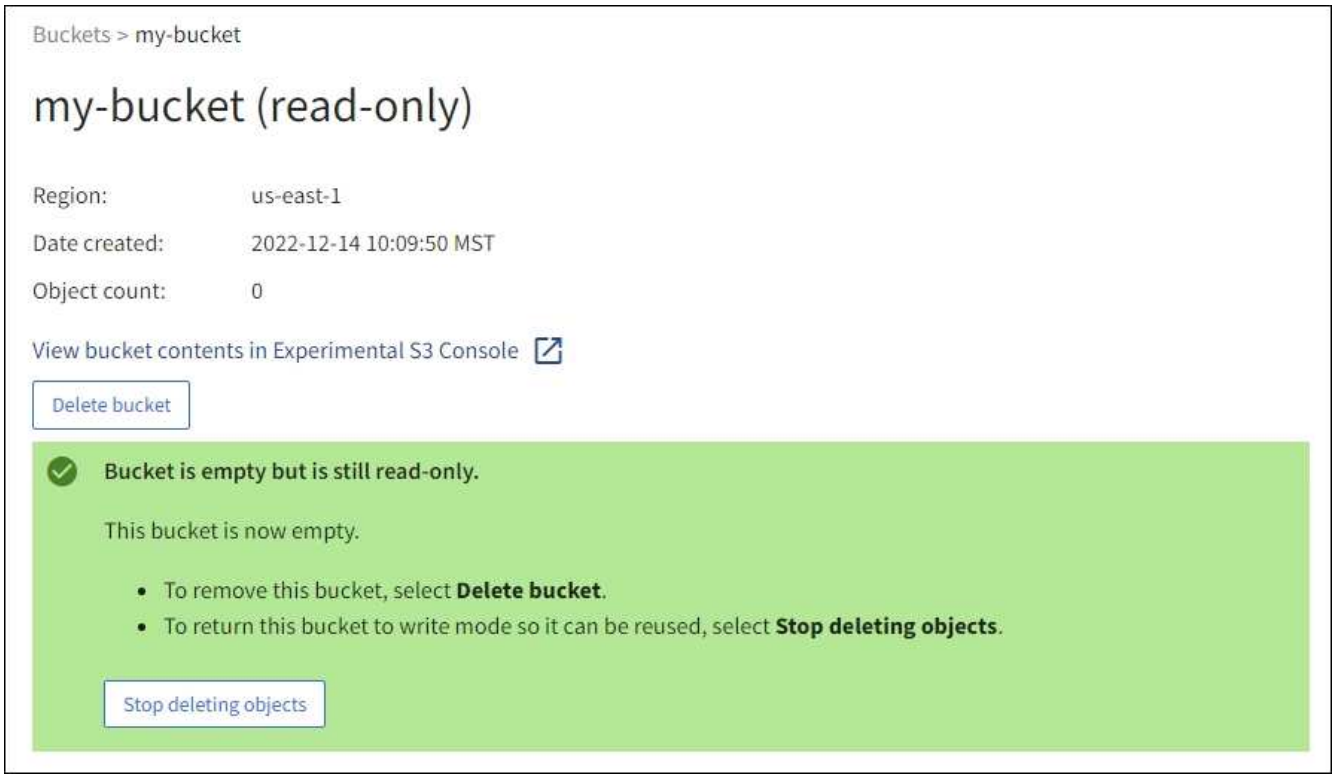


5. Según sea necesario mientras se ejecuta la operación, seleccione **Detener eliminación de objetos** para detener el proceso. Luego, opcionalmente, seleccione **Eliminar objetos en el cubo** para reanudar el proceso.

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

6. Espere a que se complete la operación.

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



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

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

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

Eliminar bloque de S3

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

Antes de empezar

- Ha iniciado sesión en el gestor de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.
- Los cucharones que desea eliminar están vacíos. Si los depósitos que desea suprimir están *NOT* vacíos, "suprimir objetos del depósito".

Acerca de esta tarea

Estas instrucciones describen cómo eliminar un bloque de S3 mediante el administrador de inquilinos.

También puede eliminar S3 cubos utilizando "API de gestión de inquilinos"o el "API REST DE S3".

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

Pasos

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

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

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

   Menú Actions

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

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

   Detalles

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

   b. Seleccione **Eliminar cubo**.

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

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

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

Utilice la consola S3

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

La consola S3 le permite:

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

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

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

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

Antes de empezar

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

Pasos

1. Seleccione **Almacenamiento** > **Cubos** > ***nombre del cubo***.
2. Seleccione la ficha Consola de S3.
3. Pegue el ID de clave de acceso y la clave de acceso secreta en los campos. De lo contrario, selecciona **Cargar claves de acceso** y selecciona tu `.csv` archivo.
4. Seleccione **Iniciar sesión**.
5. Aparece la tabla de objetos de cubo. Puede gestionar objetos según sea necesario.

Información adicional

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

Gestione servicios de plataformas S3

Servicios de plataforma S3

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

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

Descripción general de los servicios de la plataforma

Los servicios de plataforma de StorageGRID pueden ayudarte a implementar una estrategia de cloud híbrido permitiéndote enviar notificaciones de eventos y copias de objetos S3 y metadatos de objetos a destinos externos.

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

Se puede configurar cualquier combinación de servicios de plataforma para un único bloque de S3. Por ejemplo, puede configurar tanto el "Servicio CloudMirror" como "notificaciones" en un bucket de StorageGRID S3 para que pueda reflejar objetos específicos en Amazon Simple Storage Service (S3), mientras envía una notificación sobre cada objeto a una aplicación de supervisión de terceros para ayudarle a realizar un seguimiento de sus gastos de AWS.

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

Cómo se configuran los servicios de plataforma

Los servicios de plataforma se comunican con 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, un punto final de webhook o un clúster de Elasticsearch alojado localmente, en AWS o en otro lugar.

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

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

- Si desea que todos los objetos cuyas claves comiencen con `/images` se repliquen en un bucket de Amazon S3, debe agregar una configuración de replicación al bucket de origen.
- Si también desea enviar notificaciones cuando estos objetos están almacenados en el bloque, debe añadir 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 de la configuración XML está regido por las API DE REST de S3 que se usan para implementar los servicios de plataforma StorageGRID:

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

Consideraciones sobre el uso de servicios de plataforma

Consideración	Detalles
Supervisión del extremo de destino	Debe supervisar la disponibilidad de cada extremo de destino. Si se pierde la conectividad con el extremo de destino durante un periodo de tiempo prolongado y existe una gran acumulación de solicitudes, se producirá un error en las solicitudes de cliente adicionales (como solicitudes PUT) a StorageGRID. Debe volver a intentar estas solicitudes con errores cuando se pueda acceder al extremo.
Limitación de punto final de destino	El software StorageGRID puede reducir las solicitudes entrantes de S3 para un bloque si la velocidad a la que se envían las solicitudes supera la velocidad a la que el extremo de destino puede recibir las solicitudes. La limitación sólo se produce cuando hay una acumulación de solicitudes que están a la espera de ser enviadas al extremo de destino. El único efecto visible es que las solicitudes entrantes de S3 tardarán más en ejecutarse. Si empieza a detectar un rendimiento significativamente más lento, debe reducir la tasa de procesamiento o utilizar un extremo con mayor capacidad. Si la acumulación de solicitudes sigue creciendo, las operaciones de S3 del cliente (como SOLICITUDES PUT) fallarán en el futuro. Las solicitudes de CloudMirror tienen más probabilidades de que se vean afectadas por el rendimiento del extremo de destino, ya que estas solicitudes suelen requerir más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.

Consideración	Detalles
Solicitud de garantías	StorageGRID garantiza la realización de pedidos de operaciones en un objeto dentro de un sitio. Siempre que todas las operaciones contra un objeto se encuentren en el mismo sitio, el estado del objeto final (para replicación) será siempre igual al estado en StorageGRID. StorageGRID hace todo un esfuerzo por intentar solicitar solicitudes cuando se realizan operaciones en todos los sitios de StorageGRID. Por ejemplo, si escribe un objeto inicialmente en el sitio A y después sobrescribe el mismo objeto en el sitio B, no se garantiza que el objeto final replicado por CloudMirror en el bloque de destino sea el más nuevo.
Eliminaciones de objetos condicionados por ILM	Para coincidir con el comportamiento de eliminación de AWS CRR y Amazon Simple Notification Service, CloudMirror y las solicitudes de notificación de eventos no se envían cuando se elimina un objeto del bloque de origen debido a las reglas de gestión de la vida útil de la información de StorageGRID. Por ejemplo, no se envían solicitudes de notificaciones de eventos o CloudMirror si una regla de ILM elimina un objeto después de 14 días. Por el contrario, las solicitudes de integración de búsqueda se envían cuando los objetos se eliminan debido a ILM.
Utilizando puntos finales Kafka	Para puntos finales Kafka, TLS mutuo no es compatible. Como resultado, si se ha `ssl.client.auth` establecido en en `required` la configuración de su broker Kafka, puede causar problemas de configuración de punto final Kafka. La autenticación de los puntos finales de Kafka utiliza los siguientes tipos de autenticación. Estos tipos son diferentes de los utilizados para la autenticación de otros puntos finales, como Amazon SNS, y requieren credenciales de nombre de usuario y contraseña. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Nota:** Los ajustes de proxy de almacenamiento configurados no se aplican a los endpoints de servicios de la plataforma Kafka.

Consideraciones sobre el uso del servicio de replicación de CloudMirror

Consideración	Detalles
Estado de replicación	StorageGRID no admite `x-amz-replication-status` el encabezado.

Consideración	Detalles
Tamaño del objeto	El tamaño máximo de los objetos que se pueden replicar en un bloque de destino mediante el servicio de replicación de CloudMirror es de 5 TIB, que es el mismo que el tamaño máximo de objeto *admitido*. **Nota**: El tamaño máximo *Recommended* para una sola operación PutObject es de 5 GiB (5.368.709.120 bytes). Si tiene objetos que sean mayores de 5 GIB, utilice la carga de varias partes en su lugar.
Versiones de bloques e ID de versión	Si el bloque de S3 de origen de StorageGRID tiene habilitado el control de versiones, también debe habilitar el control de versiones para el bloque de destino. Al usar el control de versiones, tenga en cuenta que el orden de las versiones de objetos en el bloque de destino es el mejor esfuerzo y no está garantizado por el servicio CloudMirror, debido a las limitaciones del protocolo S3. **Nota**: Los ID de versión para el depósito de origen en StorageGRID no están relacionados con los ID de versión para el depósito de destino.
Etiquetado para versiones de objetos	El servicio CloudMirror no replica ninguna solicitud PutObjectTagging o DeleteObjectTagging que proporcione un ID de versión, debido a las limitaciones del protocolo S3. Debido a que los ID de versión para el origen y el destino no están relacionados, no hay forma de garantizar que se replique una actualización de etiqueta para un ID de versión específico. Por el contrario, el servicio CloudMirror replica las solicitudes PutObjectTagging o las solicitudes DeleteObjectTagging que no especifican un ID de versión. Estas solicitudes actualizan las etiquetas de la clave más reciente (o la versión más reciente si el bloque está versionado). También se replican búsquedas normales con etiquetas (no actualizaciones de etiquetado).
Cargas y valores de varias partes `ETag`	Cuando se crea un mirroring de objetos cargados con una carga de varias partes, el servicio CloudMirror no conserva las piezas. Como resultado, el `ETag` valor del objeto reflejado será diferente al `ETag` valor del objeto original.
Objetos cifrados con SSE-C (cifrado en el lado del servidor con claves proporcionadas por el cliente)	El servicio CloudMirror no admite objetos cifrados con SSE-C. Si intenta ingerir un objeto en el depósito de origen para la replicación de CloudMirror y la solicitud incluye los encabezados de solicitud SSE-C, la operación falla.
Bloque con S3 Object Lock habilitado	La replicación no es compatible con buckets de origen o destino con el bloqueo de objetos S3 habilitado.

Conozca el servicio de replicación de CloudMirror

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

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

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

CloudMirror y ILM

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

CloudMirror y replicación entre grid

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

CloudMirror y bloques de S3

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

Cucharones existentes

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

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

Varios cubos de destino

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 puede replicar un objeto en más de un bloque a la vez.

Bloques con versiones o sin versiones

Puede configurar la replicación de CloudMirror en bloques con versiones o sin versiones. Los cubos de destino se pueden versionar o no versionar. Puede utilizar cualquier combinación de cubos con versiones y sin versiones. Por ejemplo, puede especificar un bloque con versiones como destino para un bloque de origen sin versiones o viceversa. También puede replicar entre cubos sin versiones.

Eliminación, bucles de replicación y eventos

Comportamiento de eliminación

Es el mismo comportamiento que el comportamiento de eliminación del servicio Amazon S3, Replicación entre regiones (CRR). Al eliminar un objeto en un bloque de origen nunca se elimina un objeto replicado en el destino. Si se van a crear versiones de los cubos de origen y de destino, se replica el marcador de borrado. Si el depósito de destino no tiene versiones, al suprimir un objeto del depósito de origen no se replica el marcador de eliminación en el depósito de destino ni se elimina el objeto de destino.

Protección de bucles de replicación

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

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

Eventos en el bloque de destino

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

Comprender las notificaciones para bloques

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, un punto final de webhook o Amazon Simple Notification Service.

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

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

La singularidad y el orden de las notificaciones no están garantizados. Como resultado de las operaciones realizadas para garantizar el éxito en la entrega, se podría enviar más de una notificación de un evento al destino. Además, como la entrega es asíncrona, no se garantiza que la ordenación del tiempo de las notificaciones en el destino coincida con la ordenación de eventos del bloque de origen, especialmente en las operaciones que se originan en diferentes sitios de StorageGRID. Puede utilizar la `sequencer` clave en el mensaje de evento para determinar el orden de los eventos de 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 evento:
  - S3:ObjetoCreado:
  - S3:ObjectCreated:Put
  - S3:ObjectCreated:Post
  - S3:ObjectCreated:Copiar
  - S3:ObjectCreated:CompleteMultipartUpload
  - S3:ObjectRemoved:
  - S3:ObjectRemoved:Eliminar
  - S3:ObjectRemoved:DeleteMarkerCreated

    - S3:ObjectRestore:Post
- Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar, pero no incluyen algunas claves ni utilizan valores específicos para otros, como se muestra en la tabla:

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

Comprender el servicio de integración de búsquedas

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

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

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

Aunque la integración de Elasticsearch se puede configurar en un bucket con S3 Object Lock habilitado, los metadatos de S3 Object Lock (incluidos el estado Retain Until Date y Legal hold) de los objetos no se incluirán en los metadatos enviados a Elasticsearch.

> Debido a que el servicio de integración de búsqueda hace que los metadatos del objeto se envíen a un destino, su configuración XML se conoce como "*metadata* notification configuration XML". Este XML de configuración es diferente del XML de configuración de notificación utilizado para activar las notificaciones *event*.

Integración de búsqueda y bloques de S3

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

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

Buscar notificaciones

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 del funcionamiento de la política de ILM de la cuadrícula.
- Los metadatos o las etiquetas de los objetos son añadidos, actualizados o eliminados. El conjunto completo de metadatos y etiquetas se envía siempre al momento de la actualización, no sólo los valores modificados.

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

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

Servicio de integración de búsqueda y Elasticsearch

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

Gestione los extremos de los servicios de plataforma

Configure los extremos de servicios de la plataforma

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

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

¿Qué es un extremo de servicios de plataforma?

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

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

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

Extremos para la replicación de CloudMirror

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

Extremos para notificaciones

StorageGRID admite puntos finales de Amazon SNS, Kafka y webhook. Los puntos finales de Simple Queue Service (SQS) y AWS Lambda no son compatibles.

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.

Extremos del servicio de integración de búsqueda

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

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

Información relacionada

"Administre StorageGRID"

Especifique URN para el extremo de servicios de la plataforma

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

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

URN elementos

El URN para un punto final de servicios de plataforma debe empezar por `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 especifica el URN para un punto final de CloudMirror alojado en StorageGRID, el URN puede empezar por `urn:sgws`.

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

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

Por ejemplo, para seguir especificando el URN para un punto final de CloudMirror alojado en StorageGRID, debe agregar `s3` a Get `urn:sgws:s3`.

Para la mayoría de los puntos finales, el elemento final del URN identifica el recurso de destino específico en el URI de destino, por ejemplo, `sns-topic-name` .

Para los puntos finales de webhook, el recurso de destino es el propio URI de destino.

Servicio	Recurso específico
Replicación de CloudMirror	`bucket-name`
Notificaciones	`sns-topic-name` o. `kafka-topic-name` **Nota:** Para los puntos finales de webhook, el elemento final del URN puede ser cualquier cadena, siempre que el URN del punto final sea único.
Integración de búsqueda	`domain-name/index-name/type-name` **Nota:** Si el clúster Elasticsearch está **no** configurado para crear índices automáticamente, debe crear el índice manualmente antes de crear el punto final.

Urnas para servicios alojados en AWS y GCP

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

- Replicación de CloudMirror:

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

- Notificaciones:

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

- Integración de búsqueda:

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

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

Servicios alojados localmente

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

- Replicación de CloudMirror:

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

  Para un extremo de CloudMirror alojado en StorageGRID, se puede especificar un URN válido que comience por `urn:sgws`:

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

- Notificaciones:

  Especifique un punto final de Amazon Simple Notification Service:

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

  Especifique un punto final Kafka:

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

Especifique un punto final de webhook:

```
urn:mysite:webhook:optional:optional:webhook-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` elemento puede ser cualquier cadena siempre que el URN del punto final sea único.

Cree un extremo de servicios de plataforma

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

Antes de empezar

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

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

  - Nombre del recurso único (URN)

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

  - Credenciales de autenticación (si es necesario):

Buscar puntos finales de integración

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
- Basic HTTP: Nombre de usuario y contraseña

Extremos de replicación de CloudMirror

En el caso de los extremos de replicación de CloudMirror, se pueden usar las siguientes credenciales:

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

Extremos de Amazon SNS

Para los extremos de Amazon SNS, puede usar 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 requiere verificación del certificado)

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

Pasos

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

   El tipo de servicio de plataforma que 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 de recursos único (URI) del extremo.

   Utilice uno de los siguientes formatos:

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

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

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

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

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

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

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

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

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

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

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

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

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

> Si desea autenticación para los puntos finales del webhook, configure la Seguridad de la capa de transporte mutua (mTLS) enPaso 9 .

Buscar puntos finales de integración

Introduzca 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	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
Clave de acceso	Usa credenciales de estilo AWS para autenticar conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta
HTTP básico	Utiliza un nombre de usuario y una contraseña para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña

Extremos de replicación de CloudMirror

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

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

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

Extremos de Amazon SNS

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

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

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

Puntos finales de Kafka

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

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

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

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

8. Seleccione **continuar**.
9. Seleccione un botón de opción para **Verificar certificados** para elegir cómo se verifica la conexión TLS al punto final.

La mayoría de los puntos finales

Verifique la conexión TLS para la integración de búsqueda, la replicación de CloudMirror, Amazon SNS o los puntos finales de Kafka.

Tipo de verificación del certificado	Descripción
TLS	Valida el certificado del servidor para conexiones TLS al recurso del punto final.
Desactivado	La verificación del certificado está deshabilitada. Esta opción no es segura.
Utilizar certificado de CA personalizado	El certificado CA personalizado se utiliza para verificar la identidad del servidor cuando se conecta al punto final.
Utilizar certificado de CA del sistema operativo	Utilice el certificado de CA de cuadrícula predeterminado instalado en el sistema operativo para asegurar las conexiones.

Solo puntos finales de webhook

Verificar la conexión TLS para los puntos finales del webhook.

Tipo de verificación del certificado	Descripción
TLS	Valida el certificado del servidor para conexiones TLS al recurso del punto final.
mTLS	Valida los certificados de cliente y servidor para conexiones TLS mutuas al recurso del punto final.
Desactivado	La verificación del certificado está deshabilitada. Esta opción no es segura.
Utilizar certificado de CA personalizado	El certificado CA personalizado se utiliza para verificar la identidad del servidor cuando se conecta al punto final.

Cuando selecciona **mTLS**, estas opciones estarán disponibles.

Tipo de verificación del certificado	Descripción
No verificar el certificado del servidor	Deshabilita la verificación del certificado del servidor, lo que significa que no se verifica la identidad del servidor. Esta opción no es segura.
Certificado de cliente	El certificado de cliente se utiliza para verificar la identidad del cliente cuando se conecta al punto final.

Tipo de verificación del certificado	Descripción
Clave privada del cliente	La clave privada para el certificado del cliente. Si está encriptado, debe utilizar el formato tradicional PKCS #1 (el formato PKCS #8 no es compatible).
Frase de contraseña de la clave privada del cliente	La frase de contraseña para descifrar la clave privada del cliente. Si la clave privada no está cifrada, déjelo en blanco.

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

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

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

Información relacionada

- "Especifique URN para el extremo de servicios de la plataforma"
- "Configure la replicación de CloudMirror"
- "Configure las notificaciones de eventos"
- "Configure el servicio de integración de búsqueda"

Probar la conexión para el extremo de servicios de la plataforma

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

Antes de empezar

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

Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

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

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

2. Seleccione el extremo cuya conexión desea probar.

   Aparece la página de detalles del extremo.

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

Editar extremo de servicios de plataforma

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

Antes de empezar

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

Pasos

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

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

2. Seleccione el extremo que desea editar.

   Aparece la página de detalles del extremo.

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

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

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

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

d. Según sea necesario, cambie el método para verificar los certificados.

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

Eliminar extremo de servicios de plataforma

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

Antes de empezar

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

Pasos

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

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

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

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

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

   Aparecerá un mensaje de confirmación.

4. Seleccione **Eliminar punto final**.

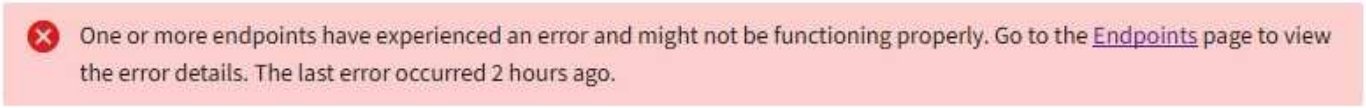
Solucionar errores de extremos de servicios de plataforma

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

Determine si se ha producido un error

Si se ha producido algún error de punto final de servicios de plataforma en los últimos 7 días, el panel de

control del gestor de inquilinos muestra un mensaje de alerta. Puede ir a la página de extremos de servicios de plataforma para ver más detalles sobre el error.



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

Pasos

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

Compruebe si el error sigue estando actualizado

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

Pasos

1. Seleccione el extremo.

   Aparece la página de detalles del extremo.

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

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

Resolver errores de punto final

Puede utilizar el mensaje **último error** de la página de detalles del punto final para ayudar a determinar qué está causando el error. Es posible que algunos errores requieran que edite el extremo para resolver el problema. Por ejemplo, se puede producir un error CloudMirroring si StorageGRID no puede acceder al bloque de S3 de destino porque no tiene los permisos de acceso correctos o si la clave de acceso ha caducado. El mensaje es «Las credenciales del punto final o el acceso al destino deben actualizarse» y los detalles son «ACCESSDENIED» o «InvalidAccessKeyId».

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

Pasos

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

Credenciales de extremo con permisos insuficientes

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

Información relacionada

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

Configure la replicación de CloudMirror

Para habilitar la replicación de CloudMirror para un bucket, cree y aplique un XML de configuración de replicación de bucket válido.

Antes de empezar

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

Acerca de esta tarea

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

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 bloques".

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

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

- Al crear y aplicar 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 buckets de origen o destino con el bloqueo de objetos S3 habilitado.
- Si habilita la replicación de CloudMirror en un bloque que contiene objetos, se replican los nuevos objetos agregados al bloque, pero los objetos existentes del bloque no se replican. Debe actualizar los objetos existentes para activar la replicación.

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

Pasos

1. Habilite la replicación para su bloque de origen:
   - Utilice un editor de texto para crear el XML de configuración de replicación necesario para habilitar la replicación, tal y como se especifica en la API de replicación de S3.
   - Al configurar XML:
     - Tenga en cuenta que StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso `Filter` del elemento para reglas y sigue las convenciones de V1 para eliminar versiones de objetos. Consulte la documentación de Amazon sobre la configuración de replicación para obtener más información.
     - Use el URN de un extremo de bloque de S3 como destino.
     - Si lo desea, agregue el `<StorageClass>` elemento y especifique una de las siguientes opciones:
       - `STANDARD`: La clase de almacenamiento predeterminada. Si no especifica una clase de almacenamiento al cargar un objeto, se `STANDARD` utilizará la clase de almacenamiento.
       - `STANDARD_IA`: (Estándar - Acceso poco frecuente.) Utilice esta clase de almacenamiento para los datos a los que se accede con menos frecuencia, pero que siguen requiriendo un acceso rápido cuando es 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 cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
3. Seleccione el nombre del bloque de origen.

   Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma** > **replicación**.
5. Seleccione la casilla de verificación **Habilitar replicación**.

6. Pegue el XML de configuración de replicación en el cuadro de texto y seleccione **Guardar cambios**.

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

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

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

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

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

Información relacionada

"Cree un extremo de servicios de plataforma"

Configure las notificaciones de eventos

Para habilitar las notificaciones de un depósito, cree XML de configuración de notificaciones y utilice el Gestor de inquilinos para aplicar el XML a un bloque.

Antes de empezar

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

Acerca de esta tarea

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 Amazon SNS de destino, el tema de Kafka o el punto final del webhook 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 notificación de buckets S3, consulte la "Instrucciones para implementar aplicaciones cliente de S3".

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

- Al crear y aplicar un XML de configuración de notificación válido, debe utilizar el URN de un punto final de notificaciones de eventos para cada destino.

- Aunque la notificación de eventos se puede configurar en un depósito con bloqueo de objetos S3 activado, los metadatos de bloqueo de objetos S3 (incluidos el estado de retención legal y la fecha de retención hasta) 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, al tema de Kafka o al punto final del webhook utilizado como destino.
- Si habilita las notificaciones de eventos para un bloque que contiene objetos, las notificaciones se envían solo para las acciones que se realizan una vez guardada la configuración de notificación.

Pasos

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

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

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

   Aparece la página de detalles bucket.

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

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

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

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

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

b. Confirme que se haya enviado una notificación al tema de Amazon SNS de destino, al tema de Kafka o al punto final del webhook.

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

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

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

Información relacionada

- "Comprender las notificaciones para bloques"
- "USE LA API DE REST DE S3"

- "Cree un extremo de servicios de plataforma"

Configure el servicio de integración de búsqueda

Para activar la integración de búsqueda de un depósito, cree XML de integración de búsqueda y utilice el gestor de inquilinos para aplicar el XML al bloque.

Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket S3 cuyo contenido desea indexar.
- El punto final que pretende utilizar como destino para el servicio de integración de búsqueda ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar el servicio de integración de búsqueda para un bloque de origen, al crear un objeto o actualizar los metadatos o las etiquetas de un objeto se activan los metadatos de objeto que se enviarán al extremo de destino.

Si habilita el servicio de integración de búsqueda para un depósito que ya contiene objetos, las notificaciones de metadatos no se envían automáticamente para los objetos existentes. Actualice estos objetos existentes para asegurarse de que sus metadatos se agregan al índice de búsqueda de destino.

Pasos

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

      Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, puede enviar metadatos para objetos con el prefijo `images` a un destino y metadatos para los objetos con el prefijo `videos` a otro. Las configuraciones que tienen prefijos superpuestos no son válidas y se rechazan cuando se envían. Por ejemplo, no se permite una configuración que incluya una regla para los objetos con el prefijo `test` y una segunda regla para los objetos con el prefijo `test2`.

      Si es necesario, consulte la Ejemplos del XML de configuración de metadatos.

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

Elementos del XML de configuración de notificación de metadatos:

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos Regla.	Sí
Regla	Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Regla.	No
Estado	El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas. Incluido en el elemento Regla.	Sí
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para hacer coincidir todos los objetos, especifique un prefijo vacío. Incluido en el elemento Regla.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Regla.	Sí

Nombre	Descripción	Obligatorio
No	URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades: • `es` debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en la forma `domain-name/myindex/mytype`. Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404. EL VALOR DE URN se incluye en el elemento Destination.	Sí

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

   Aparece la página de detalles bucket.

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

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

7. Compruebe que el servicio de integración de búsqueda está configurado correctamente:
   a. Añada un objeto al bloque de origen que cumpla los requisitos para activar una notificación de metadatos tal y como se especifica en el XML de configuración.

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

   b. Confirme que se ha agregado un documento JSON que contiene los metadatos y las etiquetas del objeto al índice de búsqueda especificado en el extremo.

Después de terminar

Según sea necesario, se puede deshabilitar la integración de búsqueda para un bloque con cualquiera de los siguientes métodos:

- Seleccione **STORAGE (S3)** > **Buckets** y desactive la casilla de verificación **Enable search integration**.
- Si utiliza la API de S3 directamente, utilice una solicitud de notificación DELETE Bucket. Consulte las instrucciones para implementar aplicaciones cliente de S3.

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

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

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Ejemplo: Configuración de notificación de metadatos con dos reglas

En este ejemplo, los metadatos del objeto para los objetos que coinciden con el prefijo `/images` se envían a un destino, mientras que los metadatos del objeto para los objetos que coinciden con el prefijo `/videos` se envían 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

Al habilitar el servicio de integración de búsqueda para un bloque, se genera un documento JSON y se envía al extremo de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas del objeto.

Este ejemplo muestra un ejemplo del JSON que podría generarse cuando se crea un objeto con la clave `SGWS/Tagging.txt` en un cubo llamado `test`. El `test` depósito no está versionado, por lo que la `versionId` 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 bloque, el nombre del objeto y el ID de versión, si existe.

Información sobre bloques y objetos

`bucket`: Nombre del cubo

`key`: Nombre de clave de objeto

`versionID`: Versión de objeto, para objetos en cubos versionados

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

Metadatos del sistema

`size`: Tamaño del objeto (en bytes) como visible para un cliente HTTP

`md5`: HASH de objeto

Metadatos del usuario

`metadata`: Todos los metadatos de 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 los resultados en Elasticsearch

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

USE LA API DE REST DE S3

Versiones y actualizaciones compatibles con la API de REST DE S3

StorageGRID admite la API de simple Storage Service (S3), que se implementa como un conjunto de servicios web de transferencia de estado de representación (REST).

La compatibilidad con la API REST DE S3 permite conectar las aplicaciones orientadas a servicios desarrolladas para servicios web S3 con el almacenamiento de objetos en las instalaciones que utiliza el sistema StorageGRID. Se requieren cambios mínimos en el uso actual de llamadas API DE REST DE S3 en una aplicación cliente.

Versiones compatibles

StorageGRID admite las siguientes versiones específicas de STS, S3 y HTTP:

Elemento	Versión
Especificación de la API de STS AssumeRole	"Documentación de Amazon Web Services (AWS): Referencia de la API de Amazon Assumerole" Para obtener más información sobre AssumeRole, consulte"Configurar AssumeRole" .
Especificación de la API S3	"Documentación de AWS: Referencia de la API de Amazon Simple Storage Service"
HTTP	1,1 Para obtener más información acerca de HTTP, vea HTTP/1.1 (RFC 7230-35). "RFC de IETF 2616: Protocolo de transferencia de hipertexto (HTTP/1.1)" **Nota**: StorageGRID no admite canalización HTTP/1.1.

Actualizaciones del soporte de la API de REST DE S3

Liberar	Comentarios
12,0	• Se agregó soporte para compartir recursos de origen cruzado (CORS) para una interfaz de administración, lo que permite que otro dominio acceda a datos en StorageGRID mediante API de administración. "Leer más" . • Se agregó soporte para STS AssumeRole y la política de sesión. Ver "un ejemplo de una política de sesión" . Puede configurar AssumeRole en grupos de inquilinos.
11,9	• Se ha agregado soporte para valores de suma de comprobación SHA-256 calculados previamente para las siguientes solicitudes y cabeceras soportadas. Puede utilizar esta función para verificar la integridad de los objetos cargados: ◦ Completa multipartCarga: `x-amz-checksum-sha256` ◦ CreateMultipartUpload: `x-amz-checksum-algorithm` ◦ GetObject: `x-amz-checksum-mode` ◦ Objeto de cabecera: `x-amz-checksum-mode` ◦ ListParts ◦ Objeto PutObject: `x-amz-checksum-sha256` ◦ Parte de carga: `x-amz-checksum-sha256` • Se ha añadido la capacidad del administrador de grid de controlar la retención a nivel de inquilino y la configuración de cumplimiento de normativas. Esta configuración afecta a la configuración de bloqueo de objetos S3. ◦ Modo de retención predeterminado de buckets y modo de retención de objetos: Gobernanza o cumplimiento de normativas, si lo permite el administrador de grid. ◦ Período de retención por defecto del depósito y fecha de retención del objeto: Debe ser menor o igual que lo permitido por el período de retención máximo definido por el administrador de grid. • Soporte mejorado para `aws-chunked` codificación de contenido y valores de streaming `x-amz-content-sha256`. Limitaciones: ◦ Si está presente, `chunk-signature` es opcional y no está validado ◦ Si está presente, `x-amz-trailer` el contenido se ignora
11,8	Se han actualizado los nombres de las operaciones S3 para que coincidan con los nombres utilizados en el "Documentación de Amazon Web Services (AWS): Referencia de API de Amazon simple Storage Service".

Liberar	Comentarios
11,7	• Agregado "Referencia rápida: Solicitudes de API de S3 admitidas". • Se ha añadido soporte para el uso del modo de GOBIERNO con S3 Object Lock. • Se ha añadido soporte para la cabecera de respuesta específica de StorageGRID `x-ntap-sg-cgr-replication-status` para las solicitudes de objetos GET Object y HEAD Object. Este encabezado proporciona el estado de replicación de un objeto para la replicación entre grid. • Las solicitudes SelectObjectContent ahora admiten objetos de Parquet.
11,6	• Se ha agregado soporte para el uso `partNumber` del parámetro request en las solicitudes GET Object y HEAD Object. • Se añadió compatibilidad con un modo de retención predeterminado y un período de retención predeterminado en el nivel de bloque para S3 Object Lock. • Se ha añadido compatibilidad con `s3:object-lock-remaining-retention-days` la clave de condición de política para establecer el rango de períodos de retención permitidos para los objetos. • Se ha cambiado el tamaño máximo de *recommended* para una única operación PUT Object a 5 GiB (5.368.709.120 bytes). Si tiene objetos que sean mayores de 5 GIB, utilice la carga de varias partes en su lugar.
11,5	• Se ha agregado compatibilidad para gestionar el cifrado de bloques. • Se añadió compatibilidad con el bloqueo de objetos S3 y las solicitudes de cumplimiento heredadas obsoletas. • Se ha agregado soporte para el uso DE DELETE Multiple Objects en cubos con versiones. • El `Content-MD5` encabezado de solicitud ahora está correctamente soportado.
11,4	• Se añadió compatibilidad con el etiquetado DE bloques DE DELETE, GET Bucket y PUT Bucket. No se admiten etiquetas de asignación de costes. • En el caso de bloques creados en StorageGRID 11.4, ya no es necesario restringir los nombres de claves de objetos para cumplir con las prácticas recomendadas de rendimiento. • Se ha añadido soporte para las notificaciones de bloques en el `s3:ObjectRestore:Post` tipo de evento. • Ahora se aplican los límites de tamaño de AWS para piezas multiparte. Cada parte de una carga de varias partes debe tener entre 5 MIB y 5 GIB. La última parte puede ser menor que 5 MIB. • Añadido soporte para TLS 1,3

Liberar	Comentarios
11,3	• Se ha añadido compatibilidad con el cifrado en el servidor de los datos de objetos con las claves proporcionadas por el cliente (SSE-C). • Se ha añadido soporte para operaciones de ciclo de vida de SUPRESIÓN, OBTENCIÓN y COLOCACIÓN DE bloques (sólo acción de caducidad) y para `x-amz-expiration` la cabecera de respuesta. • Se han actualizado PUT Object, PUT Object - Copy y Multipart Upload para describir el impacto de las reglas de ILM que utilizan la colocación síncrona en el procesamiento. • Ya no se admiten los cifrados TLS 1.1.
11,2	Compatibilidad añadida para la restauración DE objetos POSTERIOR para uso con pools de almacenamiento en cloud. Se añadió compatibilidad con el uso de la sintaxis AWS para ARN, claves de condición de política y variables de política en políticas de grupos y bloques. Se seguirán soportando las políticas de grupo y bloque existentes que utilicen la sintaxis StorageGRID. **Nota:** los usos de ARN/URN en otra configuración JSON/XML, incluidos los utilizados en las características personalizadas de StorageGRID, no han cambiado.
11,1	Se ha añadido soporte para el uso compartido de recursos de origen cruzado (CORS), HTTP para conexiones de clientes S3 a nodos de grid y configuraciones de cumplimiento en bloques.
11,0	Se añadió compatibilidad para configurar servicios de plataforma (replicación de CloudMirror, notificaciones e integración de búsqueda de Elasticsearch) para los bloques. También se ha agregado soporte para las restricciones de ubicación de etiquetado de objetos para bloques y la coherencia disponible.
10,4	Se ha agregado compatibilidad con los cambios de análisis de ILM en las versiones, las actualizaciones de página de nombres de dominio de extremo, las condiciones y variables en las directivas, los ejemplos de directivas y el permiso PutOverwriteObject.
10,3	Se ha añadido compatibilidad con las versiones.
10,2	Se ha añadido compatibilidad con las políticas de acceso a grupos y bloques y para la copia de varias partes (cargar artículo - copia).
10,1	Se añadió compatibilidad con la carga de varias partes, las solicitudes de estilo hospedado virtual y la autenticación v4.
10,0	Soporte inicial de la API REST S3 por parte del sistema StorageGRID . La versión actualmente compatible de la *Referencia de API del servicio de almacenamiento simple* es 2006-03-01.

Referencia rápida: Solicitudes de API de S3 admitidas

En esta página se resume cómo StorageGRID admite las API de Amazon Simple Storage Service (S3).

Esta página incluye solo las operaciones S3 compatibles con StorageGRID.

> Para ver la documentación de AWS para cada operación, seleccione el enlace en el encabezado.

Parámetros de consulta URI comunes y cabeceras de solicitud

A menos que se indique lo contrario, se soportan los siguientes parámetros de consulta de URI comunes:

- `versionId` (según sea necesario para las operaciones de objeto)

A menos que se indique lo contrario, se admiten las siguientes cabeceras de solicitud comunes:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Información relacionada

- "S3 Detalles de implementación de la API de REST"
- "Referencia de API de Amazon Simple Storage Service: Encabezados de solicitud comunes"

"AbortMultipartUpload"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID soporta todos parámetros y cabeceras comunes para esta solicitud, además de este parámetro de consulta URI adicional:

- `uploadId`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones para cargas de varias partes"

"CompleteMultipartUpload"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID soporta todos parámetros y cabeceras comunes para esta solicitud, además de este parámetro de consulta URI adicional:

- `uploadId`
- `x-amz-checksum-sha256`

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

Documentación de StorageGRID

"CompleteMultipartUpload"

"CopyObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo parámetros y cabeceras comunes para esta solicitud, además de estos encabezados adicionales:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`

- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"CopyObject"

"CreateBucket"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo parámetros y cabeceras comunes para esta solicitud, además de estos encabezados adicionales:

- `x-amz-bucket-object-lock-enabled`

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en bloques"

"CreateMultipartUpload"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo parámetros y cabeceras comunes para esta solicitud, además de estos encabezados adicionales:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"CreateMultipartUpload"

"DeleteBucket"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteBucketCors"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteBucketEncryption"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteBucketLifecycle"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

- "Operaciones en bloques"
- "Cree una configuración del ciclo de vida de S3"

"DeleteBucketPolicy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteBucketReplication"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteBucketTagging"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo parámetros y cabeceras comunespara esta solicitud, además de este encabezado de solicitud adicional:

- `x-amz-bypass-governance-retention`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en objetos"

"DeleteObjects"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo parámetros y cabeceras comunespara esta solicitud, además de este encabezado de solicitud adicional:

- `x-amz-bypass-governance-retention`

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en objetos"

"DeleteObjectTagging"

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en objetos"

"GetBucketAcl"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketCors"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketEncryption"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketLifecycleConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

- "Operaciones en bloques"
- "Cree una configuración del ciclo de vida de S3"

"GetBucketLocation"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketNotificationConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketPolicy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketReplication"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"Etiquetado de GetBucketTagging"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketVersioning"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID soporta todos parámetros y cabeceras comunes para esta solicitud, además de estos parámetros de consulta URI adicionales:

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

Y estos encabezados de solicitud adicionales:

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"GetObject"

"GetObjectAcl"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en objetos"

"GetObjectLegalHold"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"GetObjectLockConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"GetObjectRetention"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"GetObjectEtiquetado"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en objetos"

"Segmento de cabeza"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"Objeto principal"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo parámetros y cabeceras comunes para esta solicitud, además de estos encabezados adicionales:

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`

- `If-Unmodified-Since`
- `Range`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Objeto principal"

"ListCuchers"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

Operaciones en el servicio › ListBuckets

"ListCargas multipartitas"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos los parámetros y cabeceras comunescasos de esta solicitud, además de estos parámetros adicionales:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"ListCargas multipartitas"

"ListObjects"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos los parámetros y cabeceras comunescasos de esta solicitud, además de estos parámetros adicionales:

- `delimiter`
- `encoding-type`
- `marker`

- `max-keys`
- `prefix`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"ListObjectsV2"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos los parámetros y cabeceras comunescasos de esta solicitud, además de estos parámetros adicionales:

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"ListObjectVersions"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos los parámetros y cabeceras comunescasos de esta solicitud, además de estos parámetros adicionales:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"ListParts"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos los parámetros y cabeceras comunescasos de esta solicitud, además de estos parámetros adicionales:

- `max-parts`
- `part-number-marker`
- `uploadId`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"ListCargas multipartitas"

"A cargo de PutBucketCors"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en bloques"

"PutBucketEncryption"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

Documentación de StorageGRID

"Operaciones en bloques"

"PutBucketLifecycleConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- `And`
- `Days`
- `Expiration`
- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

Documentación de StorageGRID

- "Operaciones en bloques"
- "Cree una configuración del ciclo de vida de S3"

"PutBucketNotificationConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- `Event`
- `Filter`
- `FilterRule`
- `Id`

- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

Documentación de StorageGRID

"Operaciones en bloques"

"Política de PutBucketPolicy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Para obtener detalles sobre los campos de cuerpo JSON admitidos, consulte"Utilice las políticas de acceso de bloques y grupos" .

"PutBucketReplication"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Etiquetas XML de cuerpo de solicitud

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

Documentación de StorageGRID

"Operaciones en bloques"

"PutBucketTagging"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en bloques"

"PutBucketVersioning"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Parámetros de cuerpo de solicitud

StorageGRID admite los siguientes parámetros de cuerpo de solicitud:

- `VersioningConfiguration`
- `Status`

Documentación de StorageGRID

"Operaciones en bloques"

"Objeto de puta"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo parámetros y cabeceras comunes para esta solicitud, además de estos encabezados adicionales:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Solicitar el cuerpo

- Datos binarios del objeto

Documentación de StorageGRID

"Objeto de puta"

"PutObjectLegalHold"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"PutObjectLockConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"PutObjectRetention"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo parámetros y cabeceras comunespara esta solicitud, además de este encabezado adicional:

- `x-amz-bypass-governance-retention`

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"PutObjectEtiquetado"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon

S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en objetos"

"RestoreObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Para obtener más información sobre los campos de cuerpo admitidos, consulte "RestoreObject".

"SelectObjectContent"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Para obtener más información sobre los campos de cuerpo admitidos, consulte lo siguiente:

- "Utilice S3 Select"
- "SelectObjectContent"

"UploadPart"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID soporta todos parámetros y cabeceras comunes para esta solicitud, además de estos parámetros de consulta URI adicionales:

- `partNumber`
- `uploadId`

Y estos encabezados de solicitud adicionales:

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Solicitar el cuerpo

- Datos binarios de la pieza

Documentación de StorageGRID

"UploadPart"

"UploadPartCopy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID soporta todos parámetros y cabeceras comunes para esta solicitud, además de estos parámetros de consulta URI adicionales:

- `partNumber`
- `uploadId`

Y estos encabezados de solicitud adicionales:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"UploadPartCopy"

Probar la configuración de la API de REST S3

Puede usar la interfaz de línea de comandos (CLI de AWS) de Amazon Web Services para probar la conexión con el sistema y verificar que puede leer y escribir objetos.

Antes de empezar

- Ha descargado e instalado la CLI de AWS desde "aws.amazon.com/cli".
- Opcionalmente, usted tiene "se ha creado un punto final de equilibrio de carga". De lo contrario, conoce la dirección IP del nodo de almacenamiento al que desea conectarse y el número de puerto que se va a utilizar. Consulte "Puertos y direcciones IP para las conexiones de cliente".
- Tienes "Se ha creado una cuenta de inquilino de S3".
- Ha iniciado sesión en el inquilino y "se creó una clave de acceso".

Para obtener más información sobre estos pasos, consulte "Configurar conexiones de cliente".

Pasos

1. Configure los ajustes de la CLI de AWS para usar la cuenta que creó en el sistema StorageGRID:
   a. Acceda al modo de configuración: `aws configure`
   b. Introduzca el ID de clave de acceso de la cuenta que creó.
   c. Introduzca la clave de acceso secreta de la cuenta que creó.
   d. Introduzca la región por defecto que se va a utilizar. Por ejemplo, `us-east-1`.
   e. Introduzca el formato de salida predeterminado que se va a utilizar o pulse **Intro** para seleccionar JSON.
2. Crear un bucket.

   En este ejemplo se supone que ha configurado un punto final de equilibrio de carga para utilizar la dirección IP 10.96.101.17 y el puerto 10443.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   Si el bloque se crea correctamente, se devuelve la ubicación del bloque, como se puede ver en el ejemplo siguiente:

   ```
   "Location": "/testbucket"
   ```

3. Cargue un objeto.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   put-object --bucket testbucket --key s3.pdf --body C:\s3-
   test\upload\s3.pdf
   ```

   Si el objeto se carga correctamente, se devuelve un ETag que es un hash de los datos del objeto.

4. Enumere el contenido del cucharón para verificar que el objeto se ha cargado.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   list-objects --bucket testbucket
   ```

5. Elimine el objeto.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   delete-object --bucket testbucket --key s3.pdf
   ```

6. Eliminar el bloque.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Cómo StorageGRID implementa la API DE REST de S3

Solicitudes de clientes en conflicto

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias".

El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Coherencia

La consistencia proporciona un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios. Puede cambiar la consistencia según lo requiera la aplicación.

De forma predeterminada, StorageGRID garantiza la consistencia de lectura tras escritura para los objetos recién creados. Cualquier operación GET posterior a una operación PUT completada con éxito podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, las actualizaciones de metadatos y las eliminaciones son eventualmente consistentes.

Si desea realizar operaciones de objeto en otra coherencia, puede:

- Especificar una consistencia paracada cucharón .
- Especifique una consistencia para Cada operación de API.
- Cambie la consistencia predeterminada en toda la cuadrícula realizando una de las siguientes tareas:
  - En el Administrador de cuadrícula, vaya a **Configuración** > **Sistema** > **Configuración de almacenamiento** > **Consistencia del depósito predeterminado**.
  - .

> Un cambio en la consistencia de toda la cuadrícula se aplica solo a los depósitos creados después de que se haya cambiado el valor. Para determinar los detalles de un cambio, consulte el registro de auditoría ubicado en `/var/local/log` (busque **consistencyLevel**).

Valores de coherencia

La consistencia afecta cómo se distribuyen los metadatos que StorageGRID utiliza para rastrear objetos entre los nodos. La consistencia afecta la disponibilidad de los objetos para las solicitudes del cliente.

Puede establecer la coherencia de un bloque o una operación de API en uno de los valores siguientes:

- **Todos**: Todos los nodos reciben metadatos de objeto 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. Cuando se configura la semántica de quórum, se aplican los siguientes comportamientos:

- Permite la tolerancia a fallas del sitio para las solicitudes de los clientes cuando las redes tienen tres o más sitios. Las redes de dos sitios no tendrán tolerancia a fallas del sitio.
- Las siguientes operaciones S3 no tendrán éxito si un sitio está inactivo:
  - DeleteBucketEncryption
  - PonerBucketBranch
  - PutBucketEncryption
  - PutBucketVersioning
  - PutObjectLegalHold
  - PutObjectLockConfiguration
  - PutObjectRetention

Si es necesario, puedes "Configurar la semántica de quórum de StorageGRID para lograr una consistencia global sólida" .

- **Strong-site**: Los metadatos de objetos se distribuyen inmediatamente a otros nodos en el sitio. Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
- **Read-after-new-write**: Proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
- **Disponible**: Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Utilice los elementos de consistencia «Read-after-new-write» y «available»

Cuando una operación de CABEZAL u OBTENCIÓN utiliza la consistencia de lectura después de nueva escritura, StorageGRID realiza la búsqueda en varios pasos de la siguiente manera:

- Primero busca el objeto con una baja consistencia.
- Si esa búsqueda falla, repite la búsqueda en el siguiente valor de consistencia hasta que alcanza una consistencia equivalente al comportamiento para strong-global.

Si una operación HEAD u GET utiliza la coherencia «Read-after-new-write» pero el objeto no existe, la búsqueda de objetos siempre alcanzará una coherencia equivalente al comportamiento de un nivel global sólido. Debido a que esta consistencia requiere que haya disponibles varias copias de los metadatos del objeto en cada sitio, puede recibir un número elevado de errores de servidor interno 500 si hay dos o más nodos de almacenamiento en el mismo sitio disponibles.

A menos que necesite garantías de consistencia similares a Amazon S3, puede evitar estos errores para las operaciones HEAD y GET estableciendo la consistencia en “Disponible”. Cuando una operación de CABEZAL u OBTENCIÓN utiliza la consistencia «disponible», StorageGRID solo proporciona consistencia eventual. No vuelve a intentar una operación fallida en el aumento de la coherencia, por lo que no es necesario que haya varias copias de los metadatos del objeto disponibles.

Especifique la consistencia para el funcionamiento de la API

Para configurar la coherencia de una operación de API individual, los valores de coherencia deben ser compatibles con la operación y debe especificar la coherencia en el encabezado de solicitud. Este ejemplo establece la coherencia en «sitio fuerte» para una operación GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

Debe utilizar la misma consistencia para las operaciones PutObject y GetObject.

Especificar la consistencia para el depósito

Para configurar la coherencia del bloque, puede usar la solicitud StorageGRID"PONGA la consistencia del cucharón". O puede "cambiar la consistencia de un cucharón" hacerlo desde el Administrador de inquilinos.

Al establecer la coherencia de un cucharón, tenga en cuenta lo siguiente:

- La configuración de la coherencia de un bloque determina la coherencia que se usa para las operaciones S3 realizadas en los objetos del bloque o en la configuración de bloque. No afecta a las operaciones del propio cucharón.
- La coherencia de una operación API individual anula la coherencia del bloque.
- En general, los bloques deben utilizar la consistencia predeterminada «Read-after-new-write». Si las solicitudes no funcionan correctamente, cambie el comportamiento del cliente de aplicación si es posible. O bien, configure el cliente para especificar la consistencia de cada solicitud API. Defina la consistencia en el nivel del cucharón sólo como último recurso.

Cómo interactúan la consistencia y las reglas ILM para afectar la protección de datos

Tanto la elección de coherencia como la regla de ILM afectan al modo de protección de los objetos. Estos ajustes pueden interactuar.

Por ejemplo, la consistencia utilizada cuando se almacena un objeto afecta la ubicación inicial de los metadatos del objeto, mientras que el comportamiento de procesamiento seleccionado para la regla de ILM afecta la ubicación inicial de las copias de objetos. Dado que StorageGRID requiere acceso a los metadatos de un objeto y a sus datos para satisfacer las solicitudes de los clientes, seleccionar niveles de protección correspondientes para la coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas del sistema más predecibles.

Los siguientes "opciones de procesamiento" se encuentran disponibles para las reglas de ILM:

Registro doble
: StorageGRID realiza de inmediato copias provisionales del objeto y devuelve la operación correcta al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Estricto
: Todas las copias especificadas en la regla de ILM deben realizarse antes de devolver correctamente al cliente.

Equilibrado

StorageGRID intenta realizar todas las copias especificadas en la regla de gestión del ciclo de vida de la información durante el procesamiento; si no es posible, se realizarán copias provisionales y se devolverán correctamente al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Ejemplo de cómo pueden interactuar la regla de consistencia e ILM

Supongamos que tiene una cuadrícula de tres sitios con la siguiente regla ILM y la siguiente consistencia:

- **Regla ILM**: Crear tres copias de objetos, una en el sitio local y una en cada sitio remoto. Utilice el comportamiento de ingesta estricto.
- **Consistencia**: Fuerte-global (los metadatos del objeto se distribuyen inmediatamente a múltiples sitios).

Cuando un cliente almacena un objeto en la red, StorageGRID realiza tres copias del objeto y distribuye metadatos a varios sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra pérdida en el momento del mensaje de ingesta exitosa. Por ejemplo, si el sitio local se pierde poco después de la ingesta, aún existen copias de los datos y metadatos del objeto en los sitios remotos. El objeto es totalmente recuperable desde los otros sitios.

Si, en cambio, utilizara la misma regla ILM y la consistencia del sitio fuerte, el cliente podría recibir un mensaje de éxito después de que los datos del objeto se repliquen en los sitios remotos pero antes de que los metadatos del objeto se distribuyan allí. En este caso, el nivel de protección de los metadatos del objeto no coincide con el nivel de protección de los datos del objeto. Si el sitio local se pierde poco después de la ingesta, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre las reglas de coherencia y de ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Control de versiones de objetos

Puede establecer el estado de control de versiones de un bloque si desea conservar varias versiones de cada objeto. Habilitar el control de versiones de un bloque puede ayudar a protegerse contra la eliminación accidental de objetos y permite recuperar y restaurar versiones anteriores de un objeto.

El sistema StorageGRID implementa versiones con compatibilidad para la mayoría de las funciones y con algunas limitaciones. StorageGRID admite hasta 10,000 versiones de cada objeto.

El control de versiones de objetos puede combinarse con la gestión del ciclo de vida de la información (ILM) de StorageGRID o con la configuración del ciclo de vida de bloques de S3. Debe activar el control de versiones de forma explícita para cada bloque. Cuando se habilita el control de versiones para un bloque, a cada objeto agregado al bloque se le asigna un ID de versión, que genera el sistema StorageGRID.

No se admite el uso de la autenticación multifactor (MFA).

> El control de versiones solo se puede habilitar en bloques creados con StorageGRID versión 10.3 o posterior.

ILM y versiones

Las políticas de ILM se aplican a cada versión de un objeto. Un proceso de análisis de ILM analiza continuamente todos los objetos y los vuelve a evaluar en relación con la política actual de ILM. Todos los

cambios realizados en las políticas de ILM se aplican a todos los objetos procesados anteriormente. Esto incluye versiones que se han ingerido previamente si la versión está activada. El análisis de ILM aplica nuevos cambios de ILM a los objetos procesados previamente.

Para los objetos S3 en bloques con control de versiones, el soporte de control de versiones le permite crear reglas de ILM que utilicen 'Tiempo no corriente' como Tiempo de referencia (seleccione **Sí** para la pregunta, '¿Aplicar esta regla solo a versiones de objetos anteriores?' en "Paso 1 del asistente Crear una regla de ILM"). Cuando se actualiza un objeto, sus versiones anteriores se vuelven no actuales. El uso de un filtro de tiempo no corriente permite crear políticas que reduzcan el impacto en el almacenamiento de las versiones anteriores de objetos.

> Cuando se carga una nueva versión de un objeto mediante una operación de carga de varias partes, la hora no actual de la versión original del objeto se refleja cuando se creó la carga de varias partes para la nueva versión, no cuando se completó la carga de varias partes. En casos limitados, la hora no actual de la versión original puede ser horas o días antes de la hora de la versión actual.

Información relacionada

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

Use la API REST DE S3 para configurar el bloqueo de objetos de S3

Si la configuración global Bloqueo de objetos S3 está habilitada para el sistema StorageGRID, puede crear depósitos con Bloqueo de objetos S3 habilitado. Puede especificar la retención predeterminada para cada bloque o la configuración de retención para cada versión de objeto.

Cómo habilitar S3 Object Lock para un bucket

Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, también puede habilitar el bloqueo de objetos S3 al crear cada bloque.

S3 Bloqueo de objetos es un ajuste permanente que solo se puede activar cuando se crea un depósito. No puede agregar o deshabilitar S3 Object Lock después de crear un bucket.

Para activar el bloqueo de objetos S3 para un depósito, utilice uno de estos métodos:

- Cree el bloque con el Administrador de arrendatarios. Consulte "Crear bloque de S3".
- Cree el depósito mediante una solicitud CreateBucket con la `x-amz-bucket-object-lock-enabled` cabecera de solicitud. Consulte "Operaciones en bloques".

S3 Object Lock requiere el control de versiones de bloque, que se habilita automáticamente cuando se crea el bloque. No puede suspender el control de versiones del depósito. Consulte "Control de versiones de objetos".

Configuración de retención predeterminada para un bloque

Cuando S3 Object Lock está habilitado para un depósito, puede habilitar opcionalmente la retención predeterminada para el bloque y especificar un modo de retención predeterminado y un período de retención predeterminado.

Modo de retención predeterminado

- En modo de CUMPLIMIENTO:
  - El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta.
  - La fecha de retención del objeto se puede aumentar, pero no se puede reducir.
  - No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.
- En modo de GOBIERNO:
  - Los usuarios con `s3:BypassGovernanceRetention` permiso pueden utilizar `x-amz-bypass-governance-retention: true` la cabecera de solicitud para omitir la configuración de retención.
  - Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha.
  - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Período de retención predeterminado

Cada depósito puede tener un período de retención predeterminado especificado en años o días.

Cómo establecer la retención predeterminada para un depósito

Para definir la retención predeterminada de un depósito, utilice uno de estos métodos:

- Gestione la configuración de bloques desde el Gestor de inquilinos. Consulte "Cree un bloque de S3" y "Actualizar S3 Retención predeterminada de bloqueo de objetos".
- Emita una solicitud PutObjectLockConfiguration para el depósito para especificar el modo por defecto y el número por defecto de días o años.

PutObjectLockConfiguration

La solicitud PutObjectLockConfiguration le permite establecer y modificar el modo de retención predeterminado y el período de retención predeterminado para un depósito que tiene S3 Object Lock activado. También es posible eliminar los ajustes de retención predeterminados previamente configurados.

Cuando se ingieren nuevas versiones de objetos en el depósito, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` no se especifican y `x-amz-object-lock-retain-until-date`. El período de retención por defecto se utiliza para calcular la fecha de retención hasta si `x-amz-object-lock-retain-until-date` no se especifica.

Si el período de retención predeterminado se modifica tras recibir una versión de objeto, la fecha de retención hasta la de la versión del objeto sigue siendo la misma y no se vuelve a calcular con el nuevo período de retención predeterminado.

Debe tener `s3:PutBucketObjectLockConfiguration` el permiso, o ser account root, para completar esta operación.

```
`Content-MD5`La cabecera de solicitud se debe especificar en la solicitud de VENTA.
```

Ejemplo de solicitud

Este ejemplo habilita el bloqueo de objetos S3 para un depósito y establece el modo de retención predeterminado en CUMPLIMIENTO DE NORMATIVAS y el período de retención predeterminado en 6 años.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Cómo determinar la retención predeterminada de un depósito

Para determinar si S3 Object Lock está activado para un depósito y para ver el modo de retención y el período de retención predeterminados, utilice uno de estos métodos:

- Ver el depósito en el Gestor de inquilinos. Consulte "Ver S3 cubos".
- Emitir una solicitud GetObjectLockConfiguration.

GetObjectLockConfiguration

La solicitud GetObjectLockConfiguration le permite determinar si el bloqueo de objetos S3 está habilitado para un depósito y, si está activado, consulte si hay un modo de retención predeterminado y un período de retención configurado para el depósito.

Cuando se ingieren nuevas versiones de objetos en el depósito, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` no se especifica. El período de retención por defecto se utiliza para calcular la fecha de retención hasta si `x-amz-object-lock-retain-until-date` no se especifica.

Debe tener `s3:GetBucketObjectLockConfiguration` el permiso, o ser account root, para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Ejemplo de respuesta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Cómo especificar la configuración de retención para un objeto

Un bucket con S3 Object Lock habilitado puede contener una combinación de objetos con y sin la configuración de retención de S3 Object Lock.

La configuración de retención en el nivel de objeto se especifica mediante la API DE REST S3. La configuración de retención de un objeto anula cualquier configuración de retención predeterminada del bloque.

Puede especificar los siguientes ajustes para cada objeto:

- **Modo de retención**: Ya sea CUMPLIMIENTO o GOBIERNO.
- **Retain-until-date**: Una fecha que especifica cuánto tiempo la versión del objeto debe ser retenida por StorageGRID.

- En el modo de CUMPLIMIENTO DE NORMATIVAS, si la fecha de retención hasta la fecha es posterior, el objeto se puede recuperar, pero no se puede modificar ni eliminar. Se puede aumentar la fecha de retención hasta la fecha, pero esta fecha no se puede reducir ni eliminar.
- En el modo de GOBIERNO, los usuarios con permiso especial pueden omitir la configuración Retener hasta la fecha. Pueden eliminar una versión de objeto antes de que haya transcurrido su período de retención. También pueden aumentar, disminuir o incluso eliminar la fecha de retención hasta la fecha.

- **Retención legal**: La aplicación de una retención legal a una versión de objeto bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesite poner una retención legal en un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, pero permanece en su lugar hasta que se elimina explícitamente.

  La configuración de conservación legal de un objeto es independiente del modo de retención y la retención hasta la fecha. Si una versión de objeto está bajo una conservación legal, nadie puede eliminar esa versión.

Para especificar la configuración de bloqueo de objetos S3 al agregar una versión de objeto a un depósito, emita una "Objeto de puta" "CopyObject", o "CreateMultipartUpload" una solicitud.

Puede utilizar lo siguiente:

- `x-amz-object-lock-mode`, Que puede ser CUMPLIMIENTO o GOBERNANZA (distingue entre mayúsculas y minúsculas).

  > Si especifica `x-amz-object-lock-mode`, también debe especificar `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - El valor Retain-until-date debe tener el formato `2020-08-10T21:46:00Z`. Se permiten segundos fraccionarios, pero sólo se conservan 3 dígitos decimales (precisión de milisegundos). No se permiten otros formatos ISO 8601.
  - La fecha de retención debe ser futura.
- `x-amz-object-lock-legal-hold`

  Si la conservación legal está ACTIVADA (distingue entre mayúsculas y minúsculas), el objeto se colocará bajo una retención legal. Si se HA DESACTIVADO la retención legal, no se ha colocado ningún tipo de retención legal. Cualquier otro valor produce un error 400 Bad Request (InvalidArgument).

Si utiliza alguno de estos encabezados de solicitud, tenga en cuenta estas restricciones:

- `Content-MD5`La cabecera de solicitud es necesaria si hay alguna `x-amz-object-lock-*` cabecera de solicitud presente en la solicitud PutObject. `Content-MD5` No es necesario para CopyObject o CreateMultipartUpload.
- Si el depósito no tiene S3 Object Lock activado y hay un `x-amz-object-lock-*` encabezado de solicitud, se devuelve un error de 400 Bad Request (InvalidRequest).
- La solicitud PutObject admite el uso de `x-amz-storage-class: REDUCED_REDUNDANCY` para que coincida con el comportamiento de AWS. Sin embargo, cuando un objeto se procesa en un bucket con el bloqueo de objetos S3 habilitado, StorageGRID siempre ejecuta un procesamiento de compromiso doble.
- Una respuesta posterior a la versión GET o HeadObject incluirá las cabeceras `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date` y `x-amz-object-lock-legal-hold`, si está

configurada y si el remitente de la solicitud tiene los permisos correctos `s3:Get*`.

Puede utilizar `s3:object-lock-remaining-retention-days` la clave de condición de política para limitar los períodos de retención mínimos y máximos permitidos para los objetos.

Cómo actualizar la configuración de retención de un objeto

Si necesita actualizar la configuración de retención legal o retención para una versión de objeto existente, puede realizar las siguientes operaciones de subrecursos de objeto:

- `PutObjectLegalHold`

  Si el nuevo valor de retención legal está ACTIVADO, el objeto se colocará bajo una retención legal. Si el valor de la retención legal está DESACTIVADO, se levanta la retención legal.

- `PutObjectRetention`
  - El valor de modo puede ser CUMPLIMIENTO o GOBIERNO (distingue entre mayúsculas y minúsculas).
  - El valor Retain-until-date debe tener el formato `2020-08-10T21:46:00Z`. Se permiten segundos fraccionarios, pero sólo se conservan 3 dígitos decimales (precisión de milisegundos). No se permiten otros formatos ISO 8601.
  - Si una versión de objeto tiene una fecha de retención existente, sólo puede aumentarla. El nuevo valor debe ser el futuro.

Cómo utilizar el modo de GOBIERNO

Los usuarios que tienen el `s3:BypassGovernanceRetention` permiso pueden omitir la configuración de retención activa de un objeto que utiliza el modo de GOBIERNO. Cualquier operación DELETE u PutObjectRetention debe incluir la `x-amz-bypass-governance-retention:true` cabecera de solicitud. Estos usuarios pueden realizar las siguientes operaciones adicionales:

- Realice las operaciones DeleteObject o DeleteObjects para eliminar una versión de objeto antes de que haya transcurrido su período de retención.

  Los objetos que están bajo una retención legal no se pueden eliminar. La conservación legal debe estar DESACTIVADA.

- Realice operaciones PutObjectRetention que cambian el modo de una versión de objeto de GOBIERNO a CUMPLIMIENTO antes de que haya transcurrido el período de retención del objeto.

  Cambiar el modo de CUMPLIMIENTO a GOBIERNO nunca está permitido.

- Realice operaciones PutObjectRetention para aumentar, disminuir o eliminar el período de retención de una versión de objeto.

Información relacionada

- "Gestione objetos con S3 Object Lock"
- "Utilice Bloqueo de objetos S3 para retener objetos"
- "Guía del usuario de Amazon Simple Storage Service: Bloqueo de objetos"

Cree una configuración del ciclo de vida de S3

Puede crear una configuración del ciclo de vida de S3 para controlar cuándo se eliminan objetos específicos del sistema StorageGRID.

El ejemplo sencillo de esta sección muestra cómo puede controlar una configuración del ciclo de vida de S3 cuando se eliminan ciertos objetos (caducados) de bloques S3 específicos. El ejemplo de esta sección es solo con fines ilustrativos. Para obtener información detallada sobre la creación de configuraciones del ciclo de vida S3, consulte "Guía del usuario de Amazon Simple Storage Service: Gestión del ciclo de vida de los objetos". Tenga en cuenta que StorageGRID solo admite acciones de caducidad, no admite acciones de transición.

Qué es la configuración del ciclo de vida

Una configuración de ciclo de vida es un conjunto de reglas que se aplican a los objetos en bloques de S3 específicos. Cada regla especifica qué objetos se ven afectados y cuándo caducarán dichos objetos (en una fecha específica o después de un número determinado de días).

StorageGRID admite hasta 1,000 reglas de ciclo de vida en una configuración del ciclo de vida. Cada regla puede incluir los siguientes elementos XML:

- Caducidad: Elimine un objeto cuando se alcance una fecha especificada o cuando se alcance un número especificado de días, empezando desde el momento en que se ingirió el objeto.
- NoncurrentVersionExpiration: Elimine un objeto cuando se alcance un número especificado de días, empezando desde el momento en que el objeto se volvió no actual.
- Filtro (prefijo, etiqueta)
- Estado
- ID

Cada objeto sigue la configuración de retención de un ciclo de vida de bloques de S3 o una política de ILM. Cuando se configura el ciclo de vida de un bloque de S3, las acciones de caducidad del ciclo de vida anulan la política de ILM de los objetos que coinciden con el filtro de ciclo de vida del bloque. Los objetos que no coinciden con el filtro de ciclo de vida del bloque utilizan la configuración de retención de la política de ILM. Si un objeto coincide con un filtro de ciclo de vida del bloque y no se especifica ninguna acción de caducidad explícitamente, no se utiliza la configuración de retención de la política de ILM y se implica que las versiones de los objetos se retienen permanentemente. Consulte "Ejemplo de prioridades del ciclo de vida del bloque de S3 y de una política de ILM".

Como resultado, es posible que se elimine un objeto de la cuadrícula aunque las instrucciones de colocación de una regla de ILM aún se apliquen al objeto. O bien, es posible que un objeto se conserve en la cuadrícula incluso después de que hayan transcurrido las instrucciones de colocación de ILM para el objeto. Para obtener más información, consulte "Cómo funciona ILM durante la vida de un objeto".

> La configuración del ciclo de vida de bloques se puede usar con bloques que tienen habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida de bloques no se admite para bloques compatibles con versiones anteriores.

StorageGRID admite el uso de las siguientes operaciones de bloques para gestionar las configuraciones del ciclo de vida:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration

- PutBucketLifecycleConfiguration

Cree la configuración del ciclo de vida

Como primer paso en la creación de una configuración de ciclo de vida, se crea un archivo JSON que incluye una o varias reglas. Por ejemplo, este archivo JSON incluye tres reglas, de la siguiente manera:

1. La regla 1 se aplica solo a los objetos que coinciden con el prefijo `category1/` y que tienen `key2` un valor de `tag2`. El `Expiration` parámetro especifica que los objetos que coincidan con el filtro caducarán a la medianoche del 22 de agosto de 2020.
2. La regla 2 se aplica sólo a los objetos que coinciden con el prefijo `category2/`. El `Expiration` parámetro especifica que los objetos que coincidan con el filtro caducarán 100 días después de que se hayan ingerido.

   > Las reglas que especifican un número de días son relativas al momento en que se ingirió el objeto. Si la fecha actual supera la fecha de ingesta más el número de días, es posible que algunos objetos se eliminen del bloque en cuanto se aplique la configuración del ciclo de vida.

3. La regla 3 se aplica sólo a los objetos que coinciden con el prefijo `category3/`. `Expiration`El parámetro especifica que todas las versiones no corrientes de los objetos coincidentes caducarán 50 días después de que dejen de ser actuales.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Aplicar la configuración del ciclo de vida al bloque

Después de crear el archivo de configuración de ciclo de vida, se aplica a un depósito emitiendo una solicitud PutBucketLifecycleConfiguration.

Esta solicitud aplica la configuración del ciclo de vida en el archivo de ejemplo a los objetos de un depósito denominado `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que una configuración del ciclo de vida se ha aplicado correctamente al bloque, emita una solicitud GetBucketLifecycleConfiguration. Por ejemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Una respuesta correcta muestra la configuración del ciclo de vida que acaba de aplicar.

Validar que la caducidad del ciclo de vida del bloque se aplica al objeto

Puede determinar si una regla de caducidad en la configuración del ciclo de vida se aplica a un objeto específico al emitir una solicitud PutObject, HeadObject o GetObject. Si se aplica una regla, la respuesta incluye un `Expiration` parámetro que indica cuándo caduca el objeto y qué regla de caducidad se ha coincidido.

> Como el ciclo de vida del bloque anula el ciclo de vida de la información, la `expiry-date` que se muestra es la fecha real que se eliminará el objeto. Para obtener más información, consulte "Cómo se determina la retención de objetos".

Por ejemplo, esta solicitud PutObject se emitió el 22 de junio de 2020 y coloca un objeto en el `testbucket` depósito.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La respuesta correcta indica que el objeto caducará en 100 días (01 de octubre de 2020) y que coincide con la regla 2 de la configuración del ciclo de vida.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Por ejemplo, esta solicitud HeadObject se ha utilizado para obtener metadatos para el mismo objeto en el cubo de testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La respuesta correcta incluye los metadatos del objeto e indica que el objeto caducará en 100 días y que coincide con la regla 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Para los bloques con control de versiones activado, `x-amz-expiration` la cabecera de respuesta sólo se aplica a las versiones actuales de los objetos.

Recomendaciones para implementar la API REST de S3

Debe seguir estas recomendaciones al implementar la API DE REST de S3 para usar con StorageGRID.

Recomendaciones para las cabezas a los objetos no existentes

Si su aplicación verifica rutinariamente si existe un objeto en una ruta en la que no espera que el objeto exista realmente, debe usar la opción "Disponible"."coherencia" . Por ejemplo, debe utilizar la consistencia "Disponible" si su aplicación encabeza una ubicación antes de PUT en ella.

De lo contrario, si la OPERACIÓN de CABEZAL no encuentra el objeto, es posible que reciba una cantidad alta de errores de servidor interno 500 si dos o más nodos de almacenamiento del mismo sitio no están disponibles o no se puede acceder a un sitio remoto.

Puede establecer la consistencia «disponible» para cada depósito mediante "PONGA la consistencia del cucharón"la solicitud o puede especificar la coherencia en el encabezado de solicitud para una operación de

API individual.

Recomendaciones para las claves de objeto

Siga estas recomendaciones para los nombres de clave del objeto, según cuándo se creó el bloque por primera vez.

Bloques creados en StorageGRID 11,4 o versiones anteriores

- No utilice valores aleatorios como los primeros cuatro caracteres de las claves de objeto. Esto contrasta con la anterior recomendación de AWS para prefijos clave. En su lugar, utilice prefijos no aleatorios y no únicos, como `image` .
- Si sigue la recomendación anterior de AWS para utilizar caracteres aleatorios y únicos en los prefijos de clave, coloque un prefijo en las claves de objeto con un nombre de directorio. Es decir, utilice este formato:

  `mybucket/mydir/f8e3-image3132.jpg`

  En lugar de este formato:

  `mybucket/f8e3-image3132.jpg`

Bloques creados en StorageGRID 11,4 o versiones posteriores

No es necesario restringir los nombres clave de objetos para cumplir con las prácticas recomendadas de rendimiento. En la mayoría de los casos, puede utilizar valores aleatorios para los primeros cuatro caracteres de nombres de clave de objeto.

> Una excepción a esto es una carga de trabajo S3 que elimina continuamente todos los objetos después de un breve periodo de tiempo. Para minimizar el impacto en el rendimiento de este caso de uso, varíe una parte inicial del nombre de la clave cada varios miles de objetos con algo similar a la fecha. Por ejemplo, suponga que un cliente S3 normalmente escribe 2.000 objetos por segundo y la política de ciclo de vida de la gestión de la vida útil de la información o del bloque elimina los objetos al cabo de tres días. Para minimizar el impacto en el rendimiento, puede asignar un nombre a las claves utilizando un patrón como el siguiente: `/mybucket/mydir/`*`yyyymmddhhmmss-random_UUID`*`.jpg`

Recomendaciones para lecturas de rango

Si "opción global para comprimir objetos almacenados"está activado, las aplicaciones cliente S3 deben evitar realizar operaciones GetObject que especifiquen un rango de bytes. Estas operaciones de «lectura de rango» son ineficientes, puesto que StorageGRID debe descomprimir los objetos de forma efectiva para acceder a los bytes solicitados. Las operaciones GetObject que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, no es eficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden tener un tiempo de espera.

> Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

Soporte para la API de REST DE Amazon S3

S3 Detalles de implementación de la API de REST

El sistema StorageGRID implementa la API de servicio de almacenamiento simple (API 2006-03-01) con compatibilidad para la mayoría de las operaciones y con algunas limitaciones. Debe comprender los detalles de la implementación al integrar las aplicaciones cliente de la API DE REST de S3.

El sistema StorageGRID admite tanto solicitudes virtuales de tipo hospedado como solicitudes de tipo path.

Gestión de fechas

La implementación de StorageGRID de la API REST de S3 solo admite formatos de fecha HTTP válidos.

El sistema StorageGRID sólo admite formatos de fecha HTTP válidos para cualquier encabezado que acepte valores de fecha. La parte horaria de la fecha puede especificarse en formato de hora media de Greenwich (GMT) o en formato de hora universal coordinada (UTC) sin desplazamiento de zona horaria (se debe especificar +0000). Si incluye `x-amz-date` la cabecera en la solicitud, sustituye cualquier valor especificado en la cabecera de solicitud Fecha. Cuando se utiliza la versión 4 de firma de AWS, el `x-amz-date` encabezado debe estar presente en la solicitud firmada porque no se admite el encabezado de fecha.

Encabezados de solicitud comunes

El sistema StorageGRID soporta las cabeceras de solicitud comunes definidas por "Referencia de API de Amazon Simple Storage Service: Encabezados de solicitud comunes", con una excepción.

Solicite el encabezado	Implementación
Autorización	Compatibilidad completa con la firma AWS Versión 2 Compatibilidad con la versión 4 de la firma de AWS, con las siguientes excepciones: • Al proporcionar el valor de suma de comprobación de carga útil real en `x-amz-content-sha256`, el valor se acepta sin validación, como si se hubiera proporcionado el valor `UNSIGNED-PAYLOAD` para la cabecera. Cuando se proporciona un `x-amz-content-sha256` valor de encabezado que implica `aws-chunked` la transmisión (por ejemplo, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), las firmas de fragmento no se verifican contra los datos del fragmento.

Encabezados de respuesta comunes

El sistema StorageGRID admite todos los encabezados de respuesta comunes definidos por *simple Storage Service API Reference*, con una excepción.

Encabezado de respuesta	Implementación
x-amz-id-2	No se utiliza

Autenticar solicitudes

El sistema StorageGRID admite el acceso autenticado y anónimo a objetos mediante la API de S3.

La API S3 admite la versión 2 de Signature y la versión 4 de Signature para autenticar solicitudes de API S3.

Las solicitudes autenticadas deben firmarse mediante su ID de clave de acceso y su clave de acceso secreta.

El sistema StorageGRID soporta dos métodos de autenticación: El encabezado HTTP `Authorization` y el uso de parámetros de consulta.

Utilice el encabezado autorización HTTP

El encabezado HTTP `Authorization` es utilizado por todas las operaciones de la API S3 excepto las solicitudes anónimas cuando lo permite la política de bloque. `Authorization`El encabezado contiene toda la información de firma necesaria para autenticar una solicitud.

Utilice los parámetros de consulta

Puede utilizar parámetros de consulta para agregar información de autenticación a una URL. Esto se conoce como firma previa de la dirección URL, que se puede utilizar para otorgar acceso temporal a recursos específicos. Los usuarios con la URL prefirmada no necesitan conocer la clave de acceso secreta para acceder al recurso, lo que permite proporcionar acceso restringido de terceros a un recurso.

Operaciones en el servicio

El sistema StorageGRID admite las siguientes operaciones en el servicio.

Funcionamiento	Implementación
ListCuchers (Anteriormente llamado GET Service)	Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones.
Obtenga el uso del almacenamiento	La solicitud StorageGRID "Obtenga el uso del almacenamiento"le indica la cantidad total de almacenamiento que utiliza una cuenta y de cada bloque asociado a la cuenta. Se trata de una operación en el servicio con una ruta de acceso de / y un parámetro de consulta personalizado (`?x-ntap-sg-usage`) agregada.
OPCIONES /	Las aplicaciones cliente pueden emitir `OPTIONS /` solicitudes al puerto S3 de un nodo de almacenamiento, sin proporcionar credenciales de autenticación S3, para determinar si el nodo de almacenamiento está disponible. Puede usar esta solicitud para supervisar o para permitir que los equilibradores de carga externos identifiquen cuando un nodo de almacenamiento esté inactivo.

Operaciones en bloques

El sistema StorageGRID admite un máximo de 5,000 bloques para cada cuenta de

inquilino de S3.

Cada rejilla puede tener un máximo de 100.000 cubos.

Para admitir 5.000 buckets, cada nodo de almacenamiento del grid debe tener un mínimo de 64 GB de RAM.

Las restricciones de nombre de bloque siguen las restricciones de región estándar de AWS EE.UU., pero debe restringirlas a las convenciones de nomenclatura DNS para admitir solicitudes virtuales de estilo hospedado de S3.

En la siguiente sección, se ofrece más información:

- "Guía del usuario de Amazon Simple Storage Service: Cuotas de buckets, restricciones y limitaciones"
- "Configure los nombres de dominio de punto final S3"

Las operaciones ListObjects (GET Bucket) y ListObjectVersions (GET Bucket object versions) admiten StorageGRID"valores de coherencia" .

Puede comprobar si las actualizaciones a la hora del último acceso están habilitadas o deshabilitadas para grupos individuales. Consulte "GET Bucket última hora de acceso".

En la siguiente tabla se describe cómo StorageGRID implementa operaciones de bloque de API DE REST de S3. Para realizar alguna de estas operaciones, se deben proporcionar las credenciales de acceso necesarias para la cuenta.

Funcionamiento	Implementación
CreateBucket	Crea un nuevo cucharón. Al crear la cuchara, se convierte en el propietario de la cuchara. • Los nombres de los bloques deben cumplir con las siguientes reglas: ◦ Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino). ◦ Debe ser compatible con DNS. ◦ Debe contener al menos 3 y no más de 63 caracteres. ◦ Puede ser una serie de una o más etiquetas, con etiquetas adyacentes separadas por un punto. Cada etiqueta debe comenzar y terminar con una letra minúscula o un número y solo puede utilizar letras minúsculas, números y guiones. ◦ No debe ser una dirección IP con formato de texto. ◦ No debe utilizar periodos en solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor. • Por defecto, los cubos se crean en la `us-east-1` región; sin embargo, puede utilizar el `LocationConstraint` elemento de solicitud en el cuerpo de la solicitud para especificar una región diferente. Al utilizar el `LocationConstraint` elemento, debe especificar el nombre exacto de una región que se ha definido mediante Grid Manager o la API de gestión de grid. Póngase en contacto con el administrador del sistema si no conoce el nombre de región que debe utilizar. **Nota**: Se producirá un error si su solicitud de CreateBucket utiliza una región que no se ha definido en StorageGRID. • Puede incluir `x-amz-bucket-object-lock-enabled` el encabezado de solicitud para crear un depósito con S3 Object Lock activado. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3". Debe habilitar S3 Object Lock cuando crea el bloque. No puede agregar o deshabilitar S3 Object Lock después de crear un bucket. S3 Object Lock requiere el control de versiones de bloques, que se habilita automáticamente al crear el bloque.
DeleteBucket	Elimina el cucharón.
DeleteBucketCors	Elimina la configuración de CORS para el cucharón.
DeleteBucketEncryption	Elimina el cifrado predeterminado del depósito. Los objetos cifrados existentes permanecen cifrados, pero todos los objetos nuevos agregados al depósito no están cifrados.
DeleteBucketLifecycle	Elimina la configuración del ciclo de vida del depósito. Consulte "Cree una configuración del ciclo de vida de S3".

Funcionamiento	Implementación
DeleteBucketPolicy	Suprime la política asociada al depósito.
DeleteBucketReplication	Suprime la configuración de replicación asociada al depósito.
DeleteBucketTagging	Utiliza el `tagging` subrecurso para eliminar todas las etiquetas de un depósito. **Precaución**: Si se establece una etiqueta de política de ILM no predeterminada para este cubo, habrá una `NTAP-SG-ILM-BUCKET-TAG` etiqueta de cubo con un valor asignado. No emita una solicitud DeleteBucketTagging si hay una `NTAP-SG-ILM-BUCKET-TAG` etiqueta de depósito. En su lugar, emita una solicitud PutBucketTagging con solo la `NTAP-SG-ILM-BUCKET-TAG` etiqueta y su valor asignado para eliminar todas las demás etiquetas del depósito. No modifique ni elimine la `NTAP-SG-ILM-BUCKET-TAG` etiqueta del depósito.
GetBucketAcl	Devuelve una respuesta positiva y el ID, DisplayName y el permiso del propietario del depósito, lo que indica que el propietario tiene acceso completo al depósito.
GetBucketCors	Devuelve la `cors` configuración del cucharón.
GetBucketEncryption	Devuelve la configuración de cifrado predeterminada para el depósito.
GetBucketLifecycleConfiguration (Anteriormente llamado GET Bucket Lifecycle)	Devuelve la configuración del ciclo de vida del cucharón. Consulte "Cree una configuración del ciclo de vida de S3".
GetBucketLocation	Devuelve la región que se estableció utilizando el `LocationConstraint` elemento en la solicitud CreateBucket. Si la región del bloque es `us-east-1`, se devuelve una cadena vacía para la región.
GetBucketNotificationConfiguration (Anteriormente denominado notificación GET Bucket)	Devuelve la configuración de notificación adjunta al depósito.
GetBucketPolicy	Devuelve la política adjunta al depósito.
GetBucketReplication	Devuelve la configuración de replicación asociada al bloque.

Funcionamiento	Implementación
Etiquetado de GetBucketTagging	Utiliza `tagging` el subrecurso para devolver todas las etiquetas de un depósito. **Precaución**: Si se establece una etiqueta de política de ILM no predeterminada para este cubo, habrá una `NTAP-SG-ILM-BUCKET-TAG` etiqueta de cubo con un valor asignado. No modifique ni elimine esta etiqueta.
GetBucketVersioning	Esta implantación utiliza el `versioning` subrecurso para devolver el estado de control de versiones de un depósito. • *BLANK*: El control de versiones nunca se ha activado (el bloque no está versionado) • Activado: El control de versiones está activado • Suspendido: El control de versiones se ha habilitado anteriormente y se ha suspendido
GetObjectLockConfiguration	Devuelve el modo de retención predeterminado del depósito y el período de retención predeterminado, si está configurado. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".
Segmento de cabeza	Determina si existe un bloque y tiene permiso para acceder a él. Esta operación devuelve: • `x-ntap-sg-bucket-id`: El UUID del bucket en formato UUID. • `x-ntap-sg-trace-id`: El identificador de rastreo único de la solicitud asociada.

Funcionamiento	Implementación
ListObjects y ListObjectsV2 (Anteriormente denominado GET Bucket)	Devuelve algunos o todos (hasta 1.000) de los objetos de un cubo. La clase de almacenamiento para los objetos puede tener cualquiera de dos valores, incluso si el objeto se ingirió con `REDUCED_REDUNDANCY` la opción de clase storage: • `STANDARD`, Que indica que el objeto se almacena en un pool de almacenamiento que consta de nodos de almacenamiento. • `GLACIER`, Que indica que el objeto se ha movido al depósito externo especificado por Cloud Storage Pool. Si el depósito contiene un gran número de claves eliminadas que tienen el mismo prefijo, la respuesta puede incluir algunas `CommonPrefixes` que no contienen claves. Para las solicitudes HeadObject y ListObject, StorageGRID devuelve las marcas de tiempo de LastModified con diferente precisión, mientras que AWS devuelve las marcas de tiempo con la misma precisión, como se muestra en los siguientes ejemplos: • Objeto principal de StorageGRID : "Última modificación": "2024-09-26T16:43:24+00:00" • Objeto de lista StorageGRID : "Última modificación": "2024-09-26T16:43:24.931000+00:00" • Objeto principal de AWS: "Última modificación": "2023-10-17T00:19:54+00:00" • AWS ListObject: "Última modificación": "2023-10-17T00:19:54+00:00"
ListObjectVersions (Versiones de objeto GET Bucket con nombre anterior)	Con acceso DE LECTURA en un bloque, mediante esta operación con `versions` el subrecurso, se enumeran los metadatos de todas las versiones de objetos del bloque.
A cargo de PutBucketCors	Establece la configuración de CORS para un depósito para que éste pueda atender solicitudes de origen cruzado. El uso compartido de recursos de origen cruzado (CORS) es un mecanismo de seguridad que permite a las aplicaciones web de cliente de un dominio acceder a los recursos de un dominio diferente. Por ejemplo, supongamos que utiliza un depósito S3 denominado `images` para almacenar gráficos. Al establecer la configuración de CORS para el `images` depósito, puede permitir que las imágenes de ese depósito se muestren en el sitio web `http://www.example.com`.

Funcionamiento	Implementación
PutBucketEncryption	Establece el estado de cifrado predeterminado de un depósito existente. Cuando se habilita el cifrado a nivel de bloque, se cifran todos los objetos nuevos que se añadan al bloque.StorageGRID admite el cifrado en el lado del servidor con claves gestionadas por StorageGRID. Al especificar la regla de configuración de cifrado del servidor, establezca el `SSEAlgorithm` parámetro en `AES256` y no utilice el `KMSMasterKeyID` parámetro. La configuración de cifrado por defecto de bucket se ignora si la solicitud de carga de objeto ya especifica el cifrado (es decir, si la solicitud incluye el `x-amz-server-side-encryption-*` encabezado de solicitud).
PutBucketLifecycleConfiguration (Anteriormente llamado PUT Bucket Lifecycle)	Crea una nueva configuración de ciclo de vida para el bloque o sustituye a una configuración de ciclo de vida existente. StorageGRID admite hasta 1,000 reglas de ciclo de vida en una configuración del ciclo de vida. Cada regla puede incluir los siguientes elementos XML: • Caducidad (días, fecha, ExpiredObjectDeleteMarker) • Caducidad de versiones sin corriente (NewerNoncurrentVersions, NoncurrentDays) • Filtro (prefijo, etiqueta) • Estado • ID StorageGRID no admite estas acciones: • AbortEncompleteMultipartUpload • Transición Consulte "Cree una configuración del ciclo de vida de S3". Para comprender cómo la acción de caducidad en un ciclo de vida de un depósito interactúa con las instrucciones de ubicación de ILM, consulte "Cómo funciona ILM a lo largo de la vida de un objeto". **Nota**: La configuración del ciclo de vida de la cuchara se puede utilizar con cucharones que tengan habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida de la cuchara no es compatible con cucharones legados compatibles.

Funcionamiento	Implementación

PutBucketNotificationConfiguration
 	
(Anteriormente denominado notificación PUT Bucket)
	Configura las notificaciones para el depósito mediante el XML de configuración de notificación incluido en el cuerpo de la solicitud. Debe tener en cuenta los siguientes detalles de implementación:
	
	• StorageGRID admite temas de Amazon Simple Notification Service (Amazon SNS), temas de Kafka o puntos finales de webhook como destinos. No se admiten los puntos finales de Simple Queue Service (SQS) ni de AWS Lambda.
	• El destino de las notificaciones debe especificarse como URN de un extremo de StorageGRID. Se pueden crear extremos con el administrador de inquilinos o la API de gestión de inquilinos.
	
	El extremo debe existir para que la configuración de la notificación se realice correctamente. Si el punto final no existe, se devuelve un `400 Bad Request` error con el código `InvalidArgument`.
	
	• No puede configurar una notificación para los siguientes tipos de evento. Estos tipos de evento **no** son compatibles.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar, excepto que no incluyen algunas claves y utilizan valores específicos para otros, como se muestra en la lista siguiente:
	◦ **EventSource**
	
	`sgws:s3`
	
	◦ * AwsRegion*
	
	no incluido
	
	◦ **x-amz-id-2**
	
	no incluido
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

Política de PutBucketPolicy	Establece la política asociada al depósito. Ver "Utilice las políticas de acceso de bloques y grupos" .

Funcionamiento	Implementación
PutBucketReplication	Configura "Replicación de CloudMirror de StorageGRID" el depósito mediante el XML de configuración de replicación proporcionado en el cuerpo de la solicitud. Para la replicación de CloudMirror, debe tener en cuenta los siguientes detalles de la implementación: • StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso `Filter` del elemento para reglas y sigue las convenciones de V1 para eliminar versiones de objetos. Para obtener más información, consulte "Guía del usuario de Amazon Simple Storage Service: Configuración de replicación". • La replicación de bloques se puede configurar en bloques con versiones o sin versiones. • Puede especificar un segmento de destino diferente en cada regla del XML de configuración de replicación. Un bloque de origen puede replicar en más de un bloque de destino. • Los bloques de destino se deben especificar como URN de extremos StorageGRID tal y como se especifica en el administrador de inquilinos o la API de gestión de inquilinos. Consulte "Configure la replicación de CloudMirror". El extremo debe existir para que la configuración de replicación se complete correctamente. Si el punto final no existe, la solicitud falla como `400 Bad Request` . El mensaje de error indica: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • No es necesario especificar un `Role` en el XML de configuración. StorageGRID no utiliza este valor y se ignorará si se envía. • Si omite la clase storage del XML de configuración, StorageGRID utiliza la `STANDARD` clase storage de forma predeterminada. • Si elimina un objeto del bloque de origen o elimina el propio bloque de origen, el comportamiento de replicación entre regiones es el siguiente: ◦ Si elimina el objeto o bloque antes de que se haya replicado, el objeto o bloque no se replicará y no se le notificará. ◦ Si elimina el objeto o bloque después de haber sido replicado, StorageGRID sigue el comportamiento estándar de eliminación de Amazon S3 para V1 de replicación entre regiones.

Funcionamiento	Implementación
PutBucketTagging	Utiliza el `tagging` subrecurso para agregar o actualizar un juego de etiquetas para un depósito. Al añadir etiquetas de bloque, tenga en cuenta las siguientes limitaciones: • Tanto StorageGRID como Amazon S3 admiten hasta 50 etiquetas por cada bloque. • Las etiquetas asociadas con un bloque deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode de longitud. • Los valores de etiqueta pueden tener una longitud máxima de 256 caracteres Unicode. • La clave y los valores distinguen entre mayúsculas y minúsculas. **Precaución**: Si se establece una etiqueta de política de ILM no predeterminada para este cubo, habrá una `NTAP-SG-ILM-BUCKET-TAG` etiqueta de cubo con un valor asignado. Asegúrese de que la `NTAP-SG-ILM-BUCKET-TAG` etiqueta de cubo está incluida con el valor asignado en todas las solicitudes de PutBucketTagging. No modifique ni elimine esta etiqueta. **Nota**: Esta operación sobrescribirá cualquier etiqueta actual que el cubo ya tenga. Si se omite alguna etiqueta existente del conjunto, esas etiquetas se eliminarán para el cucharón.
PutBucketVersioning	Utiliza `versioning` el subrecurso para definir el estado de control de versiones de un bloque existente. Puede establecer el estado de control de versiones con uno de los siguientes valores: • Enabled: Activa el control de versiones de los objetos del bloque. Todos los objetos que se agregan al bloque reciben un ID de versión único. • Suspendido: Desactiva el control de versiones de los objetos del bloque. Todos los objetos agregados al depósito reciben el ID de versión `null` .
PutObjectLockConfiguration	Configura o elimina el modo de retención predeterminado y el período de retención predeterminado. Si se modifica el período de retención predeterminado, la fecha de retención hasta la de las versiones de objeto existentes seguirá siendo la misma y no se volverá a calcular utilizando el nuevo período de retención predeterminado. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" para obtener información detallada.

Operaciones en objetos

Operaciones en objetos

En esta sección se describe cómo el sistema StorageGRID implementa operaciones de la API DE REST de S3 para objetos.

Las siguientes condiciones se aplican a todas las operaciones de objeto:

- StorageGRID"valores de coherencia" son compatibles con todas las operaciones sobre objetos, con excepción de las siguientes:
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObjectRetention
  - SelectObjectContent
- Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.
- Todos los objetos de un bloque StorageGRID son propiedad del propietario del bloque, incluidos los objetos creados por un usuario anónimo o por otra cuenta.

En la siguiente tabla se describe cómo StorageGRID implementa operaciones de objetos API DE REST de S3.

Funcionamiento	Implementación
DeleteObject	La autenticación multifactor (MFA) y el encabezado de respuesta `x-amz-mfa` no son compatibles. Al procesar una solicitud DeleteObject, StorageGRID intenta eliminar inmediatamente todas las copias del objeto de todas las ubicaciones almacenadas. Si se realiza correctamente, StorageGRID devuelve una respuesta al cliente inmediatamente. Si no se pueden eliminar todas las copias en 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y, a continuación, indica que se ha realizado correctamente al cliente. **Creación de versiones** Para eliminar una versión específica, el solicitante debe ser el propietario del depósito y utilizar el `versionId` subrecurso. El uso de este subrecurso elimina permanentemente la versión. Si el `versionId` corresponde a un marcador de borrado, la cabecera de respuesta `x-amz-delete-marker` se devuelve establecida en `true`. • Si se suprime un objeto sin el `versionId` subrecurso de un depósito con el control de versiones activado, se genera un marcador de supresión. El `versionId` para el marcador de supresión se devuelve mediante `x-amz-version-id` la cabecera de respuesta y la `x-amz-delete-marker` cabecera de respuesta se devuelve establecida en `true`. • Si se suprime un objeto sin el `versionId` subrecurso de un depósito con control de versiones suspendido, se suprime permanentemente una versión 'nula' ya existente o un marcador de supresión 'nulo' y se genera un nuevo marcador de supresión 'nulo'. `x-amz-delete-marker`La cabecera de respuesta se devuelve definida en `true`. **Nota**: En algunos casos, pueden existir varios marcadores de borrado para un objeto. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"para obtener más información sobre cómo eliminar versiones de objetos en el modo de GOBIERNO.
DeleteObjects (Anteriormente denominado DELETE Múltiples Objetos)	La autenticación multifactor (MFA) y el encabezado de respuesta `x-amz-mfa` no son compatibles. Se pueden eliminar varios objetos en el mismo mensaje de solicitud. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"para obtener más información sobre cómo eliminar versiones de objetos en el modo de GOBIERNO.

Funcionamiento	Implementación
DeleteObjectTagging	Utiliza el `tagging` subrecurso para eliminar todas las etiquetas de un objeto. **Creación de versiones** Si el `versionId` parámetro de consulta no se especifica en la solicitud, la operación suprime todas las etiquetas de la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado MethodNotAllowed con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.
GetObject	"GetObject"
GetObjectAcl	Si se proporcionan las credenciales de acceso necesarias para la cuenta, la operación devuelve una respuesta positiva y el ID, DisplayName y permiso del propietario del objeto, lo que indica que el propietario tiene acceso completo al objeto.
GetObjectLegalHold	"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
GetObjectRetention	"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
GetObjectEtiquetado	Utiliza el `tagging` subrecurso para devolver todas las etiquetas de un objeto. **Creación de versiones** Si el `versionId` parámetro de consulta no se especifica en la solicitud, la operación devuelve todas las etiquetas de la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado MethodNotAllowed con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.
Objeto principal	"Objeto principal"
RestoreObject	"RestoreObject"
Objeto de puta	"Objeto de puta"
CopyObject (Anteriormente denominado Objeto PUT - Copiar)	"CopyObject"
PutObjectLegalHold	"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

Funcionamiento	Implementación
PutObjectRetention	"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
PutObjectEtiquetado	Utiliza el `tagging` subrecurso para agregar un juego de etiquetas a un objeto existente. **Límites de etiqueta de objeto** Puede agregar etiquetas a nuevos objetos cuando los cargue o puede agregarlos a objetos existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas por cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode de longitud y los valores de etiqueta pueden tener hasta 256 caracteres Unicode de longitud. La clave y los valores distinguen entre mayúsculas y minúsculas. **Comportamiento de ingesta y actualizaciones de etiquetas** Cuando utiliza PutObjectTagging para actualizar las etiquetas de un objeto, StorageGRID no vuelve a ingerir el objeto. Esto significa que no se utiliza la opción de comportamiento de ingesta especificada en la regla de ILM que coincide. Cualquier cambio en la ubicación del objeto que se active por la actualización se realice cuando los procesos de ILM normales se reevalúan el ILM en segundo plano. Esto significa que si la regla ILM utiliza la opción estricta para el comportamiento de ingesta, no se realiza ninguna acción si no se pueden realizar las ubicaciones de objetos necesarias (por ejemplo, porque una nueva ubicación requerida no está disponible). El objeto actualizado conserva su ubicación actual hasta que sea posible la colocación requerida. **Resolución de conflictos** Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación. **Creación de versiones** Si el `versionId` parámetro de consulta no se especifica en la solicitud, la operación agrega etiquetas a la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado MethodNotAllowed con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.
SelectObjectContent	"SelectObjectContent"

StorageGRID admite las siguientes cláusulas, tipos de datos y operadores de selección de Amazon S3 para el "SelectObjectContent".

> No se admiten los elementos que no aparecen en la lista.

Para obtener la sintaxis, consulte "SelectObjectContent". Para obtener más información acerca de S3 Select, consulte la "Documentación de AWS para S3 Select".

Solo las cuentas de inquilino con S3 Select habilitado pueden emitir consultas de SelectObjectContent. Consulte la "Consideraciones y requisitos para usar S3 Select".

Cláusulas

- SELECCIONAR lista
- CLÁUSULA FROM
- Cláusula WHERE
- Cláusula LIMIT

Tipos de datos

- bool
- entero
- cadena
- flotante
- decimal, numérico
- fecha/hora

Operadores

Operadores lógicos

- Y..
- NO
- O.

Operadores de comparación

- <
- >
- ⇐
- >=
- =
- =
- <>

- !=
- ENTRE
- PULG

Operadores de comparación de patrones

- COMO
- _
- %

Operadores unitarios

- ES NULL
- NO ES NULL

Operadores de matemáticas

- +
- -
- *
- /
- %

StorageGRID sigue la prioridad del operador de Amazon S3 Select.

Funciones de agregados

- MEDIA()
- RECUENTO (*)
- MÁX.()
- MIN()
- SUMA()

Funciones condicionales

- CASO
- COALCE
- NULLIF

Funciones de conversión

- CAST (para tipo de datos compatible)

Funciones de fecha

- FECHA_AÑADIR
- DIF_FECHA

- EXTRAER
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

Funciones de cadena

- CHAR_LENGTH, CHARACTER_LENGTH
- INFERIOR
- SUBCADENA
- RECORTE
- SUPERIOR

Usar cifrado del servidor

El cifrado del lado del servidor le permite proteger los datos de objetos en reposo. StorageGRID cifra los datos mientras escribe el objeto y descifra los datos cuando accede al objeto.

Si desea utilizar el cifrado en el servidor, puede elegir una de las dos opciones mutuamente excluyentes, basándose en cómo se administran las claves de cifrado:

- **SSE (cifrado del lado del servidor con claves administradas por StorageGRID)**: Cuando se emite una solicitud de S3 para almacenar un objeto, StorageGRID cifra el objeto con una clave única. Cuando emite una solicitud S3 para recuperar el objeto, StorageGRID utiliza la clave almacenada para descifrar el objeto.
- **SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente)**: Cuando se emite una solicitud S3 para almacenar un objeto, se proporciona su propia clave de cifrado. Cuando recupera un objeto, proporciona la misma clave de cifrado que parte de la solicitud. Si las dos claves de cifrado coinciden, el objeto se descifra y se devuelven los datos del objeto.

  Mientras que StorageGRID gestiona todas las operaciones de cifrado y descifrado de objetos, debe gestionar las claves de cifrado que proporcione.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente.

> Si un objeto está cifrado con SSE o SSE-C, se ignorará cualquier configuración de cifrado a nivel de bloque o de cuadrícula.

Utilice SSE

Para cifrar un objeto con una clave única administrada por StorageGRID, se utiliza el siguiente encabezado de solicitud:

```
x-amz-server-side-encryption
```

El encabezado de solicitud SSE es compatible con las siguientes operaciones de objeto:

- "Objeto de puta"
- "CopyObject"
- "CreateMultipartUpload"

Utilice SSE-C

Para cifrar un objeto con una clave única que administra, se utilizan tres encabezados de solicitud:

Solicite el encabezado	Descripción
`x-amz-server-side-encryption-customer-algorithm`	Especifique el algoritmo de cifrado. El valor de la cabecera debe ser `AES256`.
`x-amz-server-side-encryption-customer-key`	Especifique la clave de cifrado que se utilizará para cifrar o descifrar el objeto. El valor de la clave debe estar codificado en base64 de 256 bits.
`x-amz-server-side-encryption-customer-key-MD5`	Especifique el resumen MD5 de la clave de cifrado según RFC 1321, que se utiliza para garantizar que la clave de cifrado se haya transmitido sin errores. El valor del resumen MD5 debe estar codificado en base64 de 128 bits.

Las siguientes operaciones de objeto admiten los encabezados de solicitud de SSE-C:

- "GetObject"
- "Objeto principal"
- "Objeto de puta"
- "CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Consideraciones para utilizar el cifrado del servidor con claves proporcionadas por el cliente (SSE-C)

Antes de utilizar SSE-C, tenga en cuenta las siguientes consideraciones:

- Debe usar https.

> StorageGRID rechaza cualquier solicitud hecha a través de http Cuando se utiliza SSE-C. Para consideraciones de seguridad, debe considerar cualquier clave que envíe accidentalmente usando http para ser comprometida. Deseche la llave y gírela según corresponda.

- La ETag en la respuesta no es la MD5 de los datos del objeto.
- Debe gestionar la asignación de claves de cifrado a objetos. StorageGRID no almacena claves de cifrado. Usted es responsable del seguimiento de la clave de cifrado que usted proporciona para cada objeto.
- Si su bloque está habilitado para versionado, cada versión de objeto debe tener su propia clave de cifrado.

Usted es responsable del seguimiento de la clave de cifrado utilizada para cada versión del objeto.

- Dado que gestiona las claves de cifrado en el cliente, también debe administrar cualquier protección adicional, como la rotación de claves, en el cliente.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente.

- Si la replicación entre grid o la replicación de CloudMirror están configuradas para el bucket, no se pueden ingerir objetos SSE-C. La operación de ingesta fallará.

Información relacionada

"Guía del usuario de Amazon S3: Uso del cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C)"

CopyObject

Puede utilizar la solicitud S3 CopyObject para crear una copia de un objeto que ya está almacenado en S3. Una operación CopyObject es la misma que realizar GetObject seguido de PutObject.

Resolver conflictos

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Tamaño del objeto

El tamaño máximo de *recommended* para una sola operación PutObject es de 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice su "carga de varias partes" lugar.

El tamaño máximo de *supported* para una sola operación PutObject es de 5 TiB (5.497.558.138.880 bytes).

> Si actualizó desde StorageGRID 11,6 o una versión anterior, se activará la alerta S3 PUT Object size too large si intenta cargar un objeto que supere los 5 GiB. Si tiene una instalación nueva de StorageGRID 11,7 o 11,8, la alerta no se activará en este caso. Sin embargo, para alinearse con el estándar AWS S3, las versiones futuras de StorageGRID no admitirán cargas de objetos de más de 5 GiB.

Caracteres UTF-8 en los metadatos de usuario

Si una solicitud incluye (no escapadas) valores UTF-8 en el nombre de clave o el valor de los metadatos definidos por el usuario, el comportamiento de StorageGRID no está definido.

StorageGRID no analiza ni interpreta los caracteres UTF-8 escapados incluidos en el nombre de clave o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 que se han escapado se tratan como caracteres ASCII:

- Las solicitudes se realizan correctamente si los metadatos definidos por el usuario incluyen caracteres UTF-8 que se han escapado.
- StorageGRID no devuelve `x-amz-missing-meta` el encabezado si el valor interpretado del nombre o

valor de la clave incluye caracteres no imprimibles.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario
- `x-amz-metadata-directive`: El valor por defecto es `COPY`, que permite copiar el objeto y los metadatos asociados.

  Puede `REPLACE` especificar que sobrescriba los metadatos existentes al copiar el objeto o que actualice los metadatos de los objetos.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: El valor por defecto es `COPY`, que permite copiar el objeto y todas las etiquetas.

  Puede especificar `REPLACE` que sobrescriba las etiquetas existentes al copiar el objeto o que actualice las etiquetas.

- Encabezados de solicitud de bloqueo de objetos S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si se realiza una solicitud sin estas cabeceras, se utiliza la configuración de retención por defecto del depósito para calcular el modo de versión del objeto y retener hasta la fecha. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".

- Encabezados de solicitud SSE:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

Consulte Solicitar encabezados para el cifrado del servidor

Encabezados de solicitud no compatibles

No se admiten las siguientes cabeceras de solicitud:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

  Cuando copia un objeto, si el objeto de origen tiene una suma de comprobación, StorageGRID no copia ese valor de suma de comprobación en el nuevo objeto. Este comportamiento se aplica tanto si intenta utilizar en la solicitud de objeto como si no `x-amz-checksum-algorithm`.

- `x-amz-website-redirect-location`

Opciones para clase de almacenamiento

El `x-amz-storage-class` encabezado de solicitud está soportado y afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente utiliza la confirmación doble o equilibrada "opción de ingesta".

- `STANDARD`

  (Predeterminado) especifica una operación de procesamiento de confirmación doble cuando la regla ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.

- `REDUCED_REDUNDANCY`

  Especifica una operación de procesamiento de confirmación única cuando la regla de ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.

> Si está ingiriendo un objeto en un depósito con S3 Object Lock activado, la `REDUCED_REDUNDANCY` opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, la `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Uso de x-amz-copy-source en CopyObject

Si el bloque de origen y la clave, especificados en `x-amz-copy-source` el encabezado, son diferentes del bloque y la clave de destino, se escribe una copia de los datos del objeto de origen en el destino.

Si el origen y el destino coinciden y la `x-amz-metadata-directive` cabecera se especifica como `REPLACE`, los metadatos del objeto se actualizan con los valores de metadatos proporcionados en la solicitud. En este caso, StorageGRID no vuelve a procesar el objeto. Esto tiene dos consecuencias importantes:

- No puede utilizar CopyObject para cifrar un objeto existente en su lugar, o para cambiar el cifrado de un objeto existente en su lugar. Si proporciona el `x-amz-server-side-encryption` encabezado o `x-amz-server-side-encryption-customer-algorithm` el encabezado, StorageGRID rechaza la solicitud y devuelve `XNotImplemented`.
- No se utiliza la opción de comportamiento de procesamiento especificado en la regla de ILM que coincida. Cualquier cambio en la ubicación del objeto que se active por la actualización se realice cuando los procesos de ILM normales se reevalúan el ILM en segundo plano.

  Esto significa que si la regla ILM utiliza la opción estricta para el comportamiento de ingesta, no se realiza ninguna acción si no se pueden realizar las ubicaciones de objetos necesarias (por ejemplo, porque una nueva ubicación requerida no está disponible). El objeto actualizado conserva su ubicación actual hasta que sea posible la colocación requerida.

Solicitar encabezados para el cifrado del servidor

Si "usar cifrado del lado del servidor", las cabeceras de solicitud que proporcione dependen de si el objeto de origen está cifrado y de si planea cifrar el objeto de destino.

- Si el objeto de origen se cifra mediante una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud CopyObject, para que el objeto se pueda descifrar y copiar:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key`: Especifique la clave de cifrado que proporcionó al crear el objeto de origen.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 que proporcionó cuando creó el objeto de origen.
- Si desea cifrar el objeto de destino (la copia) con una clave única que proporciona y administra, incluya los tres encabezados siguientes:
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Especifique una nueva clave de cifrado para el objeto de destino.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la nueva clave de cifrado.

  > Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones para "utilizando cifrado del lado del servidor".
- Si desea cifrar el objeto de destino (la copia) con una clave única administrada por StorageGRID (SSE), incluya este encabezado en la solicitud CopyObject:
  - `x-amz-server-side-encryption`

  > `server-side-encryption`El valor del objeto no se puede actualizar. En su lugar, realice una copia con un nuevo `server-side-encryption` valor mediante `x-amz-metadata-directive`: `REPLACE`.

Creación de versiones

Si el depósito de origen está versionado, puede utilizar `x-amz-copy-source` la cabecera para copiar la versión más reciente de un objeto. Para copiar una versión específica de un objeto, debe especificar explícitamente la versión que se va a copiar mediante el `versionId` subrecurso. Si el bloque de destino está versionado, la versión generada se devuelve en `x-amz-version-id` la cabecera de respuesta. Si se suspende el control de versiones para el depósito de destino, `x-amz-version-id` devuelve un valor nulo.

GetObject

Puede usar la solicitud GetObject S3 para recuperar un objeto de un bucket S3.

Objetos GetObject y multipart

Puede utilizar el `partNumber` parámetro request para recuperar una parte específica de un objeto segmentado o multiparte. El `x-amz-mp-parts-count` elemento de respuesta indica cuántas partes tiene el objeto.

Se puede establecer `partNumber` en 1 para objetos segmentados/multiparte y objetos no segmentados/no multiparte; sin embargo, el `x-amz-mp-parts-count` elemento de respuesta sólo se devuelve para objetos segmentados o multiparte.

Caracteres UTF-8 en los metadatos de usuario

StorageGRID no analiza ni interpreta caracteres UTF-8 escapados en los metadatos definidos por el usuario. Las solicitudes GET para un objeto con caracteres UTF-8 que se han escapado en los metadatos definidos por el usuario no devuelven `x-amz-missing-meta` el encabezado si el nombre o el valor de la clave incluyen caracteres no imprimibles.

Cabecera de solicitud admitida

Se admite el siguiente encabezado de solicitud:

- `x-amz-checksum-mode`: Especificar `ENABLED`

```
`Range`La cabecera no está soportada con `x-amz-checksum-mode` para
GetObject. Si se incluye `Range` en la solicitud con `x-amz-checksum-
mode` Enabled, StorageGRID no devuelve un valor de suma de comprobación
en la respuesta.
```

Encabezado de solicitud no compatible

La siguiente cabecera de solicitud no está soportada y devuelve `XNotImplemented`:

- `x-amz-website-redirect-location`

Creación de versiones

Si no se especifica un `versionId` subrecurso, la operación recupera la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de supresión, se devuelve un estado de no encontrado con la `x-amz-delete-marker` cabecera de respuesta establecida en `true`.

Solicitar encabezados para el cifrado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utilice los tres encabezados si el objeto está cifrado con una clave única que ha proporcionado.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique su clave de cifrado para el objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del objeto.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en "Usar cifrado del servidor".

Comportamiento de los objetos GetObject para Cloud Storage Pool

Si se ha almacenado un objeto en un "Pool de almacenamiento en cloud", el comportamiento de una solicitud GetObject depende del estado del objeto. Consulte "Objeto principal" para obtener más información.

> Si un objeto está almacenado en un Pool de almacenamiento en la nube y una o más copias del objeto también existen en la cuadrícula, las solicitudes de GetObject intentarán recuperar los datos de la cuadrícula, antes de recuperarlo del Pool de almacenamiento en la nube.

Estado del objeto	Comportamiento de GetObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un pool de almacenamiento tradicional o utilizando código de borrado	`200 OK` Se recupera una copia del objeto.
Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	`200 OK` Se recupera una copia del objeto.
Objeto que ha pasado a un estado no recuperable	`403 Forbidden`, `InvalidObjectState` Utilice una "RestoreObject" solicitud para restaurar el objeto a un estado recuperable.
Objeto en proceso de restauración a partir de un estado no recuperable	`403 Forbidden`, `InvalidObjectState` Espere a que finalice la solicitud RestoreObject.
Objeto completamente restaurado en el pool de almacenamiento en cloud	`200 OK` Se recupera una copia del objeto.

Objetos de varias partes o segmentados en un pool de almacenamiento en nube

Si cargó un objeto con varias partes o StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el pool de almacenamiento en cloud al muestrear un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud GetObject podría regresar incorrectamente `200 OK` cuando algunas partes del objeto ya se han trasladado a un estado no recuperable o cuando algunas partes del objeto aún no se han restaurado.

En estos casos:

- Es posible que la solicitud GetObject devuelva algunos datos, pero se detenga a mitad de la transferencia.
- Es posible que se devuelva una solicitud GetObject posterior `403 Forbidden` .

GetObject y replicación entre grid

Si está utilizando "federación de grid" y "replicación entre grid" está habilitado para un depósito, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud GetObject. La respuesta incluye el encabezado de respuesta específico de StorageGRID `x-ntap-sg-cgr-replication-status`, que tendrá uno de los siguientes valores:

Cuadrícula	Estado de replicación
Origen	• **COMPLETADO**: La replicación fue exitosa. • **PENDIENTE**: El objeto aún no ha sido replicado. • **FALLO**: La replicación falló con un fallo permanente. Un usuario debe resolver el error.
Destino	**REPLICA**: El objeto fue replicado desde la cuadrícula de origen.

> StorageGRID no admite `x-amz-replication-status` el encabezado.

Objeto principal

Puede utilizar la solicitud S3 HeadObject para recuperar metadatos de un objeto sin devolver el objeto en sí. Si el objeto está almacenado en un Cloud Storage Pool, puede usar HeadObject para determinar el estado de transición del objeto.

HeadObject y objetos multiparte

Puede utilizar el `partNumber` parámetro request para recuperar metadatos de una parte específica de un objeto multiparte o segmentado. El `x-amz-mp-parts-count` elemento de respuesta indica cuántas partes tiene el objeto.

Se puede establecer `partNumber` en 1 para objetos segmentados/multiparte y objetos no segmentados/no multiparte; sin embargo, el `x-amz-mp-parts-count` elemento de respuesta sólo se devuelve para objetos segmentados o multiparte.

Caracteres UTF-8 en los metadatos de usuario

StorageGRID no analiza ni interpreta caracteres UTF-8 escapados en los metadatos definidos por el usuario.

Las solicitudes de CABECERA para un objeto con caracteres UTF-8 que se han escapado en los metadatos definidos por el usuario no devuelven `x-amz-missing-meta` la cabecera si el nombre o el valor de la clave incluyen caracteres no imprimibles.

Cabecera de solicitud admitida

Se admite el siguiente encabezado de solicitud:

- `x-amz-checksum-mode`

  El `partNumber` parámetro y `Range` el encabezado no son compatibles con `x-amz-checksum-mode` para HeadObject. Cuando se incluyen en la solicitud con `x-amz-checksum-mode` Enabled, StorageGRID no devuelve un valor de suma de comprobación en la respuesta.

Encabezado de solicitud no compatible

La siguiente cabecera de solicitud no está soportada y devuelve `XNotImplemented`:

- `x-amz-website-redirect-location`

Creación de versiones

Si no se especifica un `versionId` subrecurso, la operación recupera la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de supresión, se devuelve un estado de no encontrado con la `x-amz-delete-marker` cabecera de respuesta establecida en `true`.

Solicitar encabezados para el cifrado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utilice los tres encabezados si el objeto está cifrado con una clave única que ha proporcionado.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique su clave de cifrado para el objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del objeto.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en "Usar cifrado del servidor".

Respuestas HeadObject para objetos de Cloud Storage Pool

Si el objeto se almacena en un "Pool de almacenamiento en cloud", se devuelven las siguientes cabeceras de respuesta:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Los encabezados de respuesta proporcionan información sobre el estado de un objeto a medida que se mueve a un pool de almacenamiento en cloud, y que, opcionalmente, se realiza la transición a un estado no recuperable y se restaura.

Estado del objeto	Respuesta a HeadObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un pool de almacenamiento tradicional o utilizando código de borrado	`200 OK` (No se devuelve ninguna cabecera de respuesta especial).

Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Hasta que el objeto se convierte en un estado no recuperable, el valor para `expiry-date` se establece en un tiempo lejano en el futuro. El sistema StorageGRID no controla la hora exacta de la transición.

El objeto ha pasado a estar en estado no recuperable, pero también existe al menos una copia en la cuadrícula	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	El valor para `expiry-date` se establece en algún tiempo lejano en el futuro.
	
	Nota: Si la copia en la cuadrícula no está disponible (por ejemplo, un nodo de almacenamiento está caído), debe emitir una "RestoreObject" solicitud para restaurar la copia del grupo de almacenamiento en la nube antes de poder recuperar el objeto con éxito.

El objeto ha pasado a un estado que no se puede recuperar y no existe ninguna copia en la cuadrícula	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objeto en proceso de restauración a partir de un estado no recuperable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Estado del objeto	Respuesta a HeadObject

Objeto completamente restaurado en el pool de almacenamiento en cloud	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	`expiry-date` Indica cuándo el objeto del pool de almacenamiento en la nube volverá a un estado no recuperable.

Objetos de varias partes o segmentos en el pool de almacenamiento en cloud

Si cargó un objeto con varias partes o StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el pool de almacenamiento en cloud al muestrear un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud HeadObject podría regresar incorrectamente `x-amz-restore: ongoing-request="false"` cuando algunas partes del objeto ya se han trasladado a un estado no recuperable o cuando algunas partes del objeto aún no se han restaurado.

HeadObject y replicación entre grid

Si está utilizando "federación de grid" y "replicación entre grid" está habilitado para un depósito, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud HeadObject. La respuesta incluye el encabezado de respuesta específico de StorageGRID `x-ntap-sg-cgr-replication-status`, que tendrá uno de los siguientes valores:

Cuadrícula	Estado de replicación
Origen	• **COMPLETADO**: La replicación fue exitosa. • **PENDIENTE**: El objeto aún no ha sido replicado. • **FALLO**: La replicación falló con un fallo permanente. Un usuario debe resolver el error.
Destino	**REPLICA**: El objeto fue replicado desde la cuadrícula de origen.

> StorageGRID no admite `x-amz-replication-status` el encabezado.

Objeto de puta

Puede utilizar la solicitud PutObject S3 para agregar un objeto a un depósito.

Resolver conflictos

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Tamaño del objeto

El tamaño máximo de *recommended* para una sola operación PutObject es de 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice su "carga de varias partes" lugar.

El tamaño máximo de *supported* para una sola operación PutObject es de 5 TiB (5.497.558.138.880 bytes).

> Si actualizó desde StorageGRID 11,6 o una versión anterior, se activará la alerta S3 PUT Object size too large si intenta cargar un objeto que supere los 5 GiB. Si tiene una instalación nueva de StorageGRID 11,7 o 11,8, la alerta no se activará en este caso. Sin embargo, para alinearse con el estándar AWS S3, las versiones futuras de StorageGRID no admitirán cargas de objetos de más de 5 GiB.

Tamaño de los metadatos del usuario

Amazon S3 limita el tamaño de los metadatos definidos por el usuario dentro de cada encabezado de solicitud PUT a 2 KB. StorageGRID limita los metadatos de usuario a 24 KiB. El tamaño de los metadatos definidos por el usuario se mide tomando la suma del número de bytes de la codificación UTF-8 de cada clave y valor.

Caracteres UTF-8 en los metadatos de usuario

Si una solicitud incluye (no escapadas) valores UTF-8 en el nombre de clave o el valor de los metadatos definidos por el usuario, el comportamiento de StorageGRID no está definido.

StorageGRID no analiza ni interpreta los caracteres UTF-8 escapados incluidos en el nombre de clave o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 que se han escapado se tratan como caracteres ASCII:

- Las solicitudes PutObject, CopyObject, GetObject y HeadObject se realizan correctamente si los metadatos definidos por el usuario incluyen caracteres UTF-8 que se han escapado.
- StorageGRID no devuelve `x-amz-missing-meta` el encabezado si el valor interpretado del nombre o valor de la clave incluye caracteres no imprimibles.

Límites de etiqueta de objeto

Puede agregar etiquetas a nuevos objetos cuando los cargue o puede agregarlos a objetos existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas por cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode de longitud y los valores de etiqueta pueden tener hasta 256 caracteres Unicode de longitud. La clave y los valores distinguen entre mayúsculas y minúsculas.

Propiedad del objeto

En StorageGRID, todos los objetos son propiedad de la cuenta de propietario del bloque, incluidos los objetos creados por una cuenta que no sea propietaria o un usuario anónimo.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  Cuando se especifica `aws-chunked` para `Content-Encoding`StorageGRID no se verifican los siguientes elementos:

  - StorageGRID no verifica el `chunk-signature` con respecto a los datos del fragmento.
  - StorageGRID no verifica el valor proporcionado para `x-amz-decoded-content-length` respecto al objeto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  La codificación de transferencia fragmentada se admite si `aws-chunked` también se utiliza la firma de carga útil.
- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario.

  Cuando especifique la pareja nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

  ```
  x-amz-meta-name: value
  ```

  Si desea utilizar la opción **Tiempo de creación definido por el usuario** como Tiempo de referencia para una regla de ILM, debe utilizar `creation-time` como nombre de los metadatos que registran cuando se creó el objeto. Por ejemplo:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  El valor para `creation-time` se evalúa como segundos desde el 1 de enero de 1970.

  > Una regla de ILM no puede usar un **Tiempo de creación definido por el usuario** para el Tiempo de referencia y la opción de ingesta equilibrada o estricta. Se devuelve un error cuando se crea la regla de ILM.

- `x-amz-tagging`
- Encabezados de solicitud de bloqueo de objetos de S3
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si se realiza una solicitud sin estas cabeceras, se utiliza la configuración de retención por defecto del depósito para calcular el modo de versión del objeto y retener hasta la fecha. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".
- Encabezados de solicitud SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Consulte Solicitar encabezados para el cifrado del servidor

Encabezados de solicitud no compatibles

No se admiten las siguientes cabeceras de solicitud:

- `If-Match`
- `If-None-Match`
- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

  El `x-amz-website-redirect-location` cabezal devuelve `XNotImplemented`.

Opciones para clase de almacenamiento

```
`x-amz-storage-class`Se admite el encabezado de solicitud. El valor
enviado para `x-amz-storage-class` afecta a la forma en que StorageGRID
protege los datos de los objetos durante la ingesta y no al número de
copias persistentes del objeto que se almacenan en el sistema StorageGRID
(que viene determinado por ILM).
```

Si la regla de ILM que coincide con un objeto ingerido utiliza la opción strict ingest, el `x-amz-storage-class` encabezado no tiene efecto.

Se pueden utilizar los siguientes valores para `x-amz-storage-class`:

- `STANDARD` (Predeterminado)
  - **Commit** doble: Si la regla ILM especifica la opción COMMIT doble para el comportamiento de procesamiento, tan pronto como un objeto se ingiere una segunda copia de ese objeto se crea y se distribuye a un nodo de almacenamiento diferente (COMMIT doble). Cuando se evalúa el ciclo de vida de la información, StorageGRID determina si estas copias provisionales iniciales cumplen las instrucciones de colocación que se indican en la regla. Si no es así, es posible que deban realizarse copias de objetos nuevas en ubicaciones diferentes y es posible que las copias provisionales iniciales deban eliminarse.
  - **Equilibrado**: Si la regla de ILM especifica la opción Equilibrada y StorageGRID no puede hacer inmediatamente todas las copias especificadas en la regla, StorageGRID hace dos copias provisionales en diferentes nodos de almacenamiento.

    Si StorageGRID puede crear inmediatamente todas las copias de objetos especificadas en la regla de ILM (ubicación síncrona), el `x-amz-storage-class` encabezado no tiene efecto.

- `REDUCED_REDUNDANCY`
  - **Commit doble**: Si la regla ILM especifica la opción COMMIT doble para el comportamiento de la ingesta, StorageGRID crea una única copia provisional mientras se ingiere el objeto (COMMIT único).
  - **Equilibrado**: Si la regla de ILM especifica la opción Equilibrada, StorageGRID hace una sola copia provisional solo si el sistema no puede hacer inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación síncrona, este encabezado no tiene ningún efecto. `REDUCED_REDUNDANCY`La opción se usa mejor cuando la regla de ILM que coincide con el objeto crea una copia replicada única. En este caso, utilizar `REDUCED_REDUNDANCY` elimina la creación y la eliminación innecesarias de una copia de objeto adicional para cada operación de ingesta.

  En otras circunstancias, no se recomienda utilizar `REDUCED_REDUNDANCY` la opción. `REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante la ingesta. Por ejemplo, puede perder datos si la única copia se almacena inicialmente en un nodo de almacenamiento que falla antes de que se pueda realizar la evaluación de ILM.

> Tener solo una copia replicada durante un periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

La especificación `REDUCED_REDUNDANCY` solo afecta al número de copias que se crean cuando se procesa un objeto por primera vez. No afecta a cuántas copias del objeto se realizan cuando el objeto se evalúa mediante las políticas de ILM activas y no da lugar a que los datos se almacenen en niveles más bajos de redundancia del sistema StorageGRID.

> Si está ingiriendo un objeto en un depósito con S3 Object Lock activado, la `REDUCED_REDUNDANCY` opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, la `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Solicitar encabezados para el cifrado del servidor

Puede utilizar los siguientes encabezados de solicitud para cifrar un objeto con cifrado del servidor. Las

opciones SSE y SSE-C son mutuamente excluyentes.

- **SSE**: Utilice el siguiente encabezado si desea cifrar el objeto con una clave única gestionada por StorageGRID.
  - `x-amz-server-side-encryption`

    Cuando el `x-amz-server-side-encryption` encabezado no está incluido en la solicitud PutObject, la cuadrícula "configuración de cifrado de objetos almacenados"se omite de la respuesta PutObject.
- **SSE-C**: Utilice los tres encabezados si desea cifrar el objeto con una clave única que proporciona y administra.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Especifique su clave de cifrado para el nuevo objeto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones para "utilizando cifrado del lado del servidor".

> Si un objeto está cifrado con SSE o SSE-C, se ignorará cualquier configuración de cifrado a nivel de bloque o de cuadrícula.

Creación de versiones

Si se activa el control de versiones para un depósito, se genera automáticamente una única `versionId` para la versión del objeto que se está almacenando. Esto `versionId` también se devuelve en la respuesta utilizando `x-amz-version-id` la cabecera de respuesta.

Si se suspende el control de versiones, la versión del objeto se almacena con un valor nulo `versionId` y, si ya existe una versión nula, se sobrescribirá.

Cálculos de firma para la cabecera de autorización

Al utilizar `Authorization` el encabezado para autenticar solicitudes, StorageGRID difiere de AWS de las siguientes maneras:

- StorageGRID no requiere que `host` se incluyan encabezados en `CanonicalHeaders`.
- StorageGRID no requiere `Content-Type` ser incluido dentro de `CanonicalHeaders`.
- StorageGRID no requiere que `x-amz-*` se incluyan encabezados en `CanonicalHeaders`.

> Como práctica recomendada general, incluya siempre estos encabezados en `CanonicalHeaders` para asegurarse de que están verificados; sin embargo, si excluye estos encabezados, StorageGRID no devuelve un error.

Para obtener más información, consulte "Cálculos de firma para la cabecera de autorización: Transferencia de

carga útil en un solo fragmento (AWS Signature versión 4)" .

Información relacionada

- "Gestión de objetos con ILM"
- "Referencia de API de Amazon Simple Storage Service: PutObject"

RestoreObject

Puede utilizar la solicitud S3 RestoreObject para restaurar un objeto almacenado en un Cloud Storage Pool.

Tipo de solicitud admitido

StorageGRID solo admite solicitudes RestoreObject para restaurar un objeto. No apoya el `SELECT` tipo de restauración. Seleccione Solicitudes devueltas `XNotImplemented`.

Creación de versiones

De forma opcional, especifique si desea `versionId` restaurar una versión específica de un objeto en un bloque con versiones. Si no especifica `versionId`, se restaurará la versión más reciente del objeto

Comportamiento de RestoreObject en objetos de Cloud Storage Pool

Si se ha almacenado un objeto en un "Pool de almacenamiento en cloud", una solicitud RestoreObject tiene el siguiente comportamiento, según el estado del objeto. Consulte "Objeto principal" para obtener más información.

> Si un objeto se almacena en un pool de almacenamiento en la nube y una o más copias del objeto también existen en la cuadrícula, no es necesario restaurar el objeto emitiendo una solicitud RestoreObject. En su lugar, la copia local se puede recuperar directamente mediante una solicitud GetObject.

Estado del objeto	Comportamiento de RestoreObject
El objeto se ingiere en StorageGRID pero aún no se ha evaluado por ILM, o el objeto no está en un pool de almacenamiento cloud	`403 Forbidden`, `InvalidObjectState`
Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	`200 OK` No se realizan cambios. **Nota**: Antes de que un objeto haya sido trasladado a un estado no recuperable, no puede cambiar su estado `expiry-date`.

Estado del objeto	Comportamiento de RestoreObject
Objeto que ha pasado a un estado no recuperable	`202 Accepted` Restaura una copia recuperable del objeto en Cloud Storage Pool durante el Núm. De días especificado en el cuerpo de la solicitud. Al final de este período, el objeto se devuelve a un estado no recuperable. De forma opcional, utilice el `Tier` elemento request para determinar cuánto tiempo tardará el trabajo de restauración en finalizar (`Expedited`, `Standard` o `Bulk`). Si no especifica `Tier`, se utilizará el `Standard` nivel. **Importante**: Si un objeto ha sido trasladado a S3 Glacier Deep Archive o el Cloud Storage Pool usa almacenamiento de Azure Blob, no puede restaurarlo usando el `Expedited` nivel. Se devuelve el siguiente error `403 Forbidden` , `InvalidTier`: `Retrieval option is not supported by this storage class`.
Objeto en proceso de restauración a partir de un estado no recuperable	`409 Conflict`, `RestoreAlreadyInProgress`
Objeto completamente restaurado en el pool de almacenamiento en cloud	`200 OK` **Nota:** Si un objeto ha sido restaurado a un estado recuperable, puede cambiarlo `expiry-date` volviendo a emitir la solicitud RestoreObject con un nuevo valor para `Days`. La fecha de restauración se actualiza en relación con la hora de la solicitud.

SelectObjectContent

Puede utilizar la solicitud S3 SelectObjectContent para filtrar el contenido de un objeto S3 en función de una simple instrucción SQL.

Para obtener más información, consulte "Referencia de API de Amazon Simple Storage Service: SelectObjectContent".

Antes de empezar

- La cuenta de inquilino tiene el permiso de S3 Select.
- Tiene `s3:GetObject` permiso para el objeto que desea consultar.
- El objeto que desea consultar debe tener uno de los siguientes formatos:
  - **CSV**. Se puede utilizar tal cual o comprimir en archivos GZIP o bzip2.
  - **Parquet**. Requisitos adicionales para objetos de parquet:
    - S3 Select solo admite la compresión en columnas usando GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos de parquet.
    - S3 La selección no es compatible con la salida de parquet. Debe especificar el formato de salida como CSV o JSON.
    - El tamaño máximo del grupo de filas sin comprimir es de 512 MB.

        - Debe utilizar los tipos de dato especificados en el esquema del objeto.
        - No puede utilizar los tipos lógicos INTERVAL, JSON, LIST, TIME o UUID.
- La expresión SQL tiene una longitud máxima de 256 KB.
- Cualquier registro de la entrada o de los resultados tiene una longitud máxima de 1 MIB.

Ejemplo de sintaxis de solicitud CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Ejemplo de sintaxis de solicitud de parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Ejemplo de consulta SQL

Esta consulta obtiene el nombre del estado, 2010 poblaciones, 2015 poblaciones estimadas y el porcentaje de cambio con respecto a los datos del censo estadounidense. Los registros del archivo que no son estados se ignoran.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Las primeras líneas del archivo que se va a consultar, `SUB-EST2020_ALL.csv`, se ven así:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Ejemplo de uso de AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Las primeras líneas del archivo de salida, `changes.csv`, tienen el siguiente aspecto:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Ejemplo de uso AWS-CLI (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

Las primeras líneas del archivo de salida, changes.csv, se ven así:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operaciones para cargas de varias partes

Operaciones para cargas de varias partes

En esta sección se describe cómo StorageGRID admite las operaciones para cargas de varias partes.

Las siguientes condiciones y notas se aplican a todas las operaciones de carga de varias partes:

- No debe superar las 1.000 cargas simultáneas de varias partes en un solo bloque porque los resultados de las consultas ListMultipartUploads de ese bloque podrían devolver resultados incompletos.
- StorageGRID aplica los límites de tamaño de AWS para piezas multiparte. Los clientes de S3 deben seguir estas directrices:
  - Cada parte de una carga de varias partes debe estar entre 5 MIB (5,242,880 bytes) y 5 GIB (5,368,709,120 bytes).
  - La última parte puede ser más pequeña que 5 MIB (5,242,880 bytes).
  - En general, los tamaños de las piezas deben ser lo más grandes posible. Por ejemplo, utilice tamaños de parte de 5 GIB para un objeto de 100 GIB. Debido a que cada parte se considera un objeto único, el uso de piezas de gran tamaño reduce la sobrecarga de metadatos de StorageGRID.
  - En el caso de objetos de menor tamaño de 5 GIB, considere usar la carga sin varias partes.
- ILM se evalúa para cada parte de un objeto de varias partes a medida que se ingiere y para el objeto como un todo cuando se completa la carga de varias partes, si la regla de ILM utiliza el equilibrado o estricto "opción de ingesta". Debe saber cómo afecta esto a la ubicación de objetos y piezas:
  - Si el ILM cambia mientras se realiza una carga de varias partes de S3 GB, es posible que algunas partes del objeto no cumplan los requisitos del ILM actuales cuando se complete la carga de varias partes. Cualquier pieza que no se coloque correctamente se pondrá en cola para volver a evaluarla y

posteriormente se moverá a la ubicación correcta.

  - Al evaluar ILM para una pieza, StorageGRID filtra el tamaño de la pieza, no el tamaño del objeto. Esto significa que las partes de un objeto se pueden almacenar en ubicaciones que no cumplan con los requisitos de ILM para el objeto como un todo. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan a DC1 mientras que todos los objetos más pequeños se almacenan a DC2, cada parte de 1 GB de una carga de varias partes de 10 partes se almacena a DC2 en el momento de la ingesta. Sin embargo, cuando se evalúa ILM para el objeto como un todo, todas las partes del objeto se mueven a DC1.

- Todas las operaciones de carga multiparte son compatibles con StorageGRID"valores de coherencia" .
- Cuando se ingiere un objeto mediante la carga de varias partes, no se aplica el"Umbral de segmentación de objetos (1 GiB)".
- Según sea necesario, puede utilizar "cifrado del lado del servidor" con cargas de varias partes. Para utilizar SSE (cifrado del lado del servidor con claves administradas por StorageGRID), debe incluir `x-amz-server-side-encryption` el encabezado de solicitud solo en la solicitud CreateMultipartUpload. Para utilizar SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente), debe especificar los mismos tres encabezados de solicitud de clave de cifrado en la solicitud CreateMultipartUpload y en cada solicitud subsiguiente UploadPart.
- Un objeto cargado de varias partes se incluye en un"cubo de rama" si la ingesta se inició antes de la marca de tiempo Antes del depósito base, independientemente de cuándo se complete la carga.

Funcionamiento	Implementación
AbortMultipartUpload	Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones.
CompleteMultipartUpload	Consulte "CompleteMultipartUpload"
CreateMultipartUpload (Anteriormente denominado Iniciar carga de varias partes)	Consulte "CreateMultipartUpload"
ListCargas multipartitas	Consulte "ListCargas multipartitas"
ListParts	Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones.
UploadPart	Consulte "UploadPart"
UploadPartCopy	Consulte "UploadPartCopy"

CompleteMultipartUpload

La operación CompleteMultipartUpload completa una carga de varias partes de un objeto mediante el ensamblaje de las piezas cargadas anteriormente.

StorageGRID soporta valores no consecutivos en orden ascendente para el `partNumber` parámetro request con CompleteMultipartUpload. El parámetro puede comenzar con cualquier valor.

Resolver conflictos

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  `x-amz-storage-class`El encabezado afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente especifica el xref:{relative_path}../ilm/data-protection-options-for-ingest.html["Opción de registro doble o ingesta equilibrada"].

- `STANDARD`

  (Predeterminado) especifica una operación de procesamiento de confirmación doble cuando la regla ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.

- `REDUCED_REDUNDANCY`

  Especifica una operación de procesamiento de confirmación única cuando la regla de ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.

  Si está ingiriendo un objeto en un depósito con S3 Object Lock activado, la `REDUCED_REDUNDANCY` opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, la `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Si no se completa una carga de varias partes en un plazo de 15 días, la operación se Marca como inactiva y todos los datos asociados se eliminan del sistema.

El `ETag` valor devuelto no es una suma de MD5 de los datos, sino que sigue la implementación de Amazon S3 API del `ETag` valor para objetos de varias partes.

Encabezados de solicitud no compatibles

No se admiten las siguientes cabeceras de solicitud:

- `If-Match`
- `If-None-Match`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Creación de versiones

Esta operación completa una carga de varias partes. Si el control de versiones está activado para un depósito, la versión del objeto se crea después de completar la carga de varias partes.

Si se activa el control de versiones para un depósito, se genera automáticamente una única `versionId` para la versión del objeto que se está almacenando. Esto `versionId` también se devuelve en la respuesta utilizando `x-amz-version-id` la cabecera de respuesta.

Si se suspende el control de versiones, la versión del objeto se almacena con un valor nulo `versionId` y, si ya existe una versión nula, se sobrescribirá.

> Cuando se habilita el control de versiones para un bloque, al completar una carga de varias partes siempre se crea una versión nueva, incluso si hay cargas simultáneas de varias partes completadas en la misma clave de objeto. Cuando el control de versiones no está habilitado para un bloque, es posible iniciar una carga de varias partes y, a continuación, hacer que se inicie y finalice otra carga de varias partes primero en la misma clave de objeto. En cubos sin versiones, la carga de varias partes que finaliza por última vez tiene prioridad.

Error en la replicación, notificación o notificación de metadatos

Si el bloque donde se produce la carga de varias partes está configurado para un servicio de plataforma, la carga de varias partes se realiza correctamente incluso si la acción de replicación o notificación asociada falla.

Un inquilino puede activar la replicación o notificación con errores actualizando los metadatos o las etiquetas del objeto. Un arrendatario puede volver a enviar los valores existentes para evitar realizar cambios no deseados.

Consulte "Solucione problemas de servicios de plataforma".

CreateMultipartUpload

La operación CreateMultipartUpload (anteriormente denominada Iniciar carga de varias partes) inicia una carga de varias partes para un objeto y devuelve un ID de carga.

```
`x-amz-storage-class`Se admite el encabezado de solicitud. El valor
enviado para `x-amz-storage-class` afecta a la forma en que StorageGRID
protege los datos de los objetos durante la ingesta y no al número de
copias persistentes del objeto que se almacenan en el sistema StorageGRID
(que viene determinado por ILM).
```

Si la regla de ILM que coincide con un objeto ingerido utiliza el estricto "opción de ingesta", `x-amz-storage-class` la cabecera no tiene ningún efecto.

Se pueden utilizar los siguientes valores para `x-amz-storage-class`:

- `STANDARD` (Predeterminado)
  - **Confirmación doble**: Si la regla ILM especifica la opción de ingesta de confirmación doble, tan pronto como se ingiere un objeto, se crea una segunda copia de ese objeto y se distribuye a un nodo de almacenamiento diferente (confirmación doble). Cuando se evalúa el ciclo de vida de la información, StorageGRID determina si estas copias provisionales iniciales cumplen las instrucciones de colocación que se indican en la regla. Si no es así, es posible que deban realizarse copias de objetos nuevas en ubicaciones diferentes y es posible que las copias provisionales iniciales deban eliminarse.
  - **Equilibrado**: Si la regla de ILM especifica la opción Equilibrada y StorageGRID no puede hacer inmediatamente todas las copias especificadas en la regla, StorageGRID hace dos copias provisionales en diferentes nodos de almacenamiento.

    Si StorageGRID puede crear inmediatamente todas las copias de objetos especificadas en la regla de ILM (ubicación síncrona), el `x-amz-storage-class` encabezado no tiene efecto.
- `REDUCED_REDUNDANCY`
  - **Confirmación doble**: Si la regla de ILM especifica la opción Confirmación doble, StorageGRID crea una sola copia provisional a medida que se ingiere el objeto (confirmación única).
  - **Equilibrado**: Si la regla de ILM especifica la opción Equilibrada, StorageGRID hace una sola copia provisional solo si el sistema no puede hacer inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación síncrona, este encabezado no tiene ningún efecto. `REDUCED_REDUNDANCY`La opción se usa mejor cuando la regla de ILM que coincide con el objeto crea una copia replicada única. En este caso, utilizar `REDUCED_REDUNDANCY` elimina la creación y la eliminación innecesarias de una copia de objeto adicional para cada operación de ingesta.

  En otras circunstancias, no se recomienda utilizar `REDUCED_REDUNDANCY` la opción. `REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante la ingesta. Por ejemplo, puede perder datos si la única copia se almacena inicialmente en un nodo de almacenamiento que falla antes de que se pueda realizar la evaluación de ILM.

> Tener solo una copia replicada durante un periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

La especificación `REDUCED_REDUNDANCY` solo afecta al número de copias que se crean cuando se procesa un objeto por primera vez. No afecta a cuántas copias del objeto se realizan cuando el objeto se evalúa mediante las políticas de ILM activas y no da lugar a que los datos se almacenen en niveles más bajos de redundancia del sistema StorageGRID.

> Si está ingiriendo un objeto en un depósito con S3 Object Lock activado, la `REDUCED_REDUNDANCY` opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, la `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `Content-Type`
- `x-amz-checksum-algorithm`

  Actualmente, solo se admite el valor de SHA256 para `x-amz-checksum-algorithm`.

- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario

  Cuando especifique la pareja nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

  ```
  x-amz-meta-_name_: `value`
  ```

  Si desea utilizar la opción **Tiempo de creación definido por el usuario** como Tiempo de referencia para una regla de ILM, debe utilizar `creation-time` como nombre de los metadatos que registran cuando se creó el objeto. Por ejemplo:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  El valor para `creation-time` se evalúa como segundos desde el 1 de enero de 1970.

  > No se permite agregar `creation-time` como metadatos definidos por el usuario si está agregando un objeto a un depósito que tiene activada la conformidad heredada. Se devolverá un error.

- Encabezados de solicitud de bloqueo de objetos S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si se realiza una solicitud sin estos encabezados, la configuración de retención predeterminada del bloque se utiliza para calcular la versión del objeto mantener hasta la fecha.

  "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

- Encabezados de solicitud SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Solicitar encabezados para el cifrado del servidor

Para obtener más información sobre cómo StorageGRID trata los caracteres UTF-8, consulte "Objeto de puta".

Solicitar encabezados para el cifrado del servidor

Puede utilizar los siguientes encabezados de solicitud para cifrar un objeto de varias partes con cifrado del servidor. Las opciones SSE y SSE-C son mutuamente excluyentes.

- **SSE**: Utilice el siguiente encabezado en la solicitud CreateMultipartUpload si desea cifrar el objeto con una clave única gestionada por StorageGRID. No especifique esta cabecera en ninguna de las solicitudes de artículo de carga.
  - `x-amz-server-side-encryption`
- **SSE-C**: Utilice los tres encabezados en la solicitud CreateMultipartUpload (y en cada solicitud subsiguiente UploadPart) si desea cifrar el objeto con una clave única que proporcione y administre.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Especifique su clave de cifrado para el nuevo objeto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.

Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones para "utilizando cifrado del lado del servidor".

Encabezados de solicitud no compatibles

No se admite el siguiente encabezado de solicitud:

- `x-amz-website-redirect-location`

  El `x-amz-website-redirect-location` cabezal devuelve `XNotImplemented`.

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

ListCargas multipartitas

La operación ListMultipartUploads muestra las cargas de varias partes en curso para un bloque.

Se admiten los siguientes parámetros de solicitud:

- `encoding-type`
- `key-marker`

- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

UploadPart

La operación UploadPart carga una pieza en una carga de varias partes para un objeto.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Solicitar encabezados para el cifrado del servidor

Si especificó el cifrado SSE-C para la solicitud CreateMultipartUpload, también debe incluir los siguientes encabezados de solicitud en cada solicitud UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique la misma clave de cifrado que proporcionó en la solicitud CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el mismo resumen de MD5 que proporcionó en la solicitud CreateMultipartUpload.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en "Usar cifrado del servidor".

Si especificó una suma de comprobación SHA-256 durante la solicitud CreateMultipartUpload, también debe incluir la siguiente cabecera de solicitud en cada solicitud UploadPart:

- `x-amz-checksum-sha256`: Especifique la suma de comprobación SHA-256 para esta parte.

Encabezados de solicitud no compatibles

No se admiten las siguientes cabeceras de solicitud:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

UploadPartCopy

La operación UploadPartCopy carga una parte de un objeto copiando datos de un objeto existente como origen de datos.

La operación UploadPartCopy se implementa con todo el comportamiento de la API DE REST DE Amazon S3. Reservado el derecho a realizar modificaciones.

Esta solicitud lee y escribe los datos de objetos especificados en `x-amz-copy-source-range` el sistema StorageGRID.

Se admiten los siguientes encabezados de solicitud:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Solicitar encabezados para el cifrado del servidor

Si especificó el cifrado SSE-C para la solicitud CreateMultipartUpload, también debe incluir los siguientes encabezados de solicitud en cada solicitud UploadPartCopy:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique la misma clave de cifrado que proporcionó en la solicitud CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el mismo resumen de MD5 que proporcionó en la solicitud CreateMultipartUpload.

Si el objeto de origen se cifra utilizando una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud UploadPartCopy, para que el objeto se pueda descifrar y copiar:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Especifique la clave de cifrado que proporcionó al crear el objeto de origen.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique el resumen

MD5 que proporcionó cuando creó el objeto de origen.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en "Usar cifrado del servidor".

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

Respuestas de error

El sistema StorageGRID es compatible con todas las respuestas de error estándar de la API DE REST de S3 que se aplican. Además, la implementación de StorageGRID añade varias respuestas personalizadas.

códigos de error API de S3 admitidos

Nombre	Estado de HTTP
ACCESSDENIED	403 Prohibido
BadDigest	400 solicitud incorrecta
BucketAlreadyExists	409 conflicto
BucketNotEmpty	409 conflicto
IncompleteBody	400 solicitud incorrecta
Internalerror	500 error de servidor interno
InvalidAccessKeyId	403 Prohibido
InvalidArgument	400 solicitud incorrecta
InvalidBucketName	400 solicitud incorrecta
InvalidBucketState	409 conflicto
InvalidDigest	400 solicitud incorrecta
InvalidEncryptionAlgorithmError	400 solicitud incorrecta
InvalidPart	400 solicitud incorrecta

Nombre	Estado de HTTP
InvalidPartOrder	400 solicitud incorrecta
InvalidRange	416 rango solicitado no utilizable
InvalidRequest	400 solicitud incorrecta
InvalidStorageClass	400 solicitud incorrecta
InvalidTag	400 solicitud incorrecta
InvalidURI	400 solicitud incorrecta
KeyTooLong	400 solicitud incorrecta
MalformedXML	400 solicitud incorrecta
MetadataTooLarge	400 solicitud incorrecta
MethodNotAllowed	405 método no permitido
MissingContentLength	411 longitud requerida
MissingRequestBodyError	400 solicitud incorrecta
MissingSecurityHeader	400 solicitud incorrecta
NoSuchBucket	404 no encontrado
NoSuchKey	404 no encontrado
NoSuchUpload	404 no encontrado
NotImplimed	501 no implementada
NoSuchBucketPolicy	404 no encontrado
ObjectLockConfigurationNotFoundError	404 no encontrado
Error de precondiciónError	Error de condición 412
RequestTimeTooSowed	403 Prohibido
ServiceUnavailable	503 Servicio no disponible

Nombre	Estado de HTTP
SignatureDoesNotMatch	403 Prohibido
Cucharones TooMany	400 solicitud incorrecta
UserKeyMustBeSpecified	400 solicitud incorrecta

códigos de error personalizados de StorageGRID

Nombre	Descripción	Estado de HTTP
XBucketLifecycleNotAllowed	No se permite la configuración del ciclo de vida de los bloques en un bloque compatible heredado	400 solicitud incorrecta
XBucketPolicyParseException	Error al analizar la política JSON de bloques recibidos.	400 solicitud incorrecta
XCondit. Cumplimiento	Operación denegada debido a la configuración de cumplimiento anterior.	403 Prohibido
XDSLA ReducedRedundancyForbidden	No se permite una redundancia reducida en el bloque compatible con la tecnología heredada	400 solicitud incorrecta
XMaxBucketPolicyLengthExceeded	Su política supera la longitud máxima permitida de la política de bloques.	400 solicitud incorrecta
XMissingInternalRequestHeader	Falta un encabezado de una solicitud interna.	400 solicitud incorrecta
Cumplimiento de XNoSuchBucketCompliance	El bloque especificado no tiene la conformidad heredada activada.	404 no encontrado
XNotAcceptable	La solicitud contiene uno o más encabezados de aceptación que no se han podido satisfacer.	406 no aceptable
XNotImplemed	La solicitud que ha proporcionado implica una funcionalidad que no se ha implementado.	501 no implementada

Operaciones personalizadas de StorageGRID

Operaciones personalizadas de StorageGRID

El sistema StorageGRID admite operaciones personalizadas que se añaden a la API DE

REST DE la versión S3.

La siguiente tabla enumera las operaciones personalizadas que admite StorageGRID.

Funcionamiento	Descripción
"OBTENGA coherencia de bloques"	Devuelve la coherencia aplicada a un bloque determinado.
"PONGA la consistencia del cucharón"	Establece la coherencia aplicada a un bloque determinado.
"GET Bucket última hora de acceso"	Devuelve si las actualizaciones del último tiempo de acceso están habilitadas o deshabilitadas para un bloque en particular.
"PUT Bucket última hora de acceso"	Permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para un bloque en particular.
"Configuración de notificaciones de metadatos de DELETE Bucket"	Elimina el XML de configuración de notificación de metadatos asociado a un bloque en particular.
"OBTENGA la configuración de notificación de metadatos del bloque de datos"	Devuelve el XML de configuración de notificación de metadatos asociado a un bloque determinado.
"Configuración de notificaciones de metadatos de PUT Bucket"	Configura el servicio de notificación de metadatos para un bloque.
"Obtenga el uso del almacenamiento"	Indica la cantidad total de almacenamiento que utiliza una cuenta y para cada depósito asociado a la cuenta.
"Obsoleto: CreateBucket con configuración de cumplimiento"	Obsoleto y no compatible: Ya no puede crear nuevos bloques con el cumplimiento de normativas habilitado.
"En desuso: OBTENGA el cumplimiento de normativas de bloques"	Obsoleto pero compatible: Devuelve la configuración de cumplimiento vigente para un bloque compatible existente.
"Obsoleto: PUT Bucket Compliance"	Obsoleto pero compatible: Permite modificar la configuración de cumplimiento de un bloque compatible heredado.

OBTENGA coherencia de bloques

La solicitud OBTENER coherencia de bloques permite determinar la coherencia que se aplica a un bloque en particular.

La consistencia predeterminada se establece en garantía de lectura tras escritura para los objetos recién creados.

Debe tener el permiso s3:GetBucketConsistency, o bien ser la raíz de la cuenta, para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Respuesta

En el XML de respuesta, `<Consistency>` devolverá uno de los siguientes valores:

Coherencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.
fuerte en todo el mundo	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
sitio seguro	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
lectura-después-nueva-escritura	(Predeterminado) proporciona coherencia de lectura tras escritura para los nuevos objetos y coherencia final para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
disponible	Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Ejemplo de respuesta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Información relacionada

"Coherencia"

PONGA la consistencia del cucharón

La solicitud COLOCAR coherencia de bloques permite especificar la coherencia que se debe aplicar a las operaciones realizadas en un bloque.

La consistencia predeterminada se establece en garantía de lectura tras escritura para los objetos recién creados.

Antes de empezar

Debe tener el permiso s3:PutBucketConsistency, o bien ser la raíz de la cuenta, para completar esta operación.

Solicitud

El `x-ntap-sg-consistency` parámetro debe contener uno de los valores siguientes:

Coherencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.
fuerte en todo el mundo	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
sitio seguro	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
lectura-después-nueva-escritura	(Predeterminado) proporciona coherencia de lectura tras escritura para los nuevos objetos y coherencia final para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.

Coherencia	Descripción
disponible	Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Nota: En general, debes usar la consistencia de “Leer después de la nueva escritura”. Si las solicitudes no funcionan correctamente, cambie el comportamiento del cliente de aplicación si es posible. O bien, configure el cliente para especificar la consistencia de cada solicitud API. Defina la consistencia en el nivel del cucharón sólo como último recurso.

Ejemplo de solicitud

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Información relacionada

"Coherencia"

GET Bucket última hora de acceso

La solicitud DE tiempo DE acceso del último bloque DE GET Bucket permite determinar si las actualizaciones de la última hora de acceso están habilitadas o deshabilitadas para bloques individuales.

Para completar esta operación, debe tener el permiso s3:GetBucketLastAccessTime, o ser la raíz de la cuenta.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

Este ejemplo muestra que las actualizaciones de la última hora de acceso están habilitadas para el bloque.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

PUT Bucket última hora de acceso

La solicitud DE la última hora de acceso al bloque DE PUT permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para bloques individuales. Al deshabilitar las actualizaciones de la última hora de acceso, se mejora el rendimiento, y es la configuración predeterminada para todos los bloques creados con la versión 10.3.0 o posterior.

Para completar esta operación, debe tener el permiso s3:PutBucketLastAccessTime para un bloque o ser raíz de cuenta.

> A partir de la versión 10.3 de StorageGRID, las actualizaciones de la última hora de acceso se deshabilitan de forma predeterminada para todos los bloques nuevos. Si tiene bloques que se crearon con una versión anterior de StorageGRID y desea coincidir con el nuevo comportamiento predeterminado, debe deshabilitar explícitamente las actualizaciones de la última hora de acceso para cada uno de esos bloques anteriores. Puede activar o desactivar las actualizaciones en la hora del último acceso mediante la solicitud de hora de último acceso de PUT Bucket o desde la página de detalles de un bucket en el gestor de inquilinos. Consulte "Activar o desactivar las actualizaciones de la hora del último acceso".

Si se desactivan las actualizaciones de la última hora de acceso para un bloque, se aplicará el siguiente comportamiento a las operaciones del bloque:

- Las solicitudes GetObject, GetObjectAcl, GetObjectTagging y HeadObject no actualizan la hora del último acceso. El objeto no se agrega a las colas para la evaluación de la gestión del ciclo de vida de la información (ILM).
- Las solicitudes CopyObject y PutObjectTagging que actualizan solo los metadatos también actualizan la hora de último acceso. El objeto se agrega a las colas para la evaluación de ILM.
- Si las actualizaciones de la hora del último acceso están deshabilitadas para el bloque de origen, las solicitudes de CopyObject no actualizan la hora del último acceso para el bloque de origen. El objeto que se copió no se agrega a colas para la evaluación de ILM para el bloque de origen. Sin embargo, para el destino, las solicitudes de CopyObject siempre actualizan la hora del último acceso. La copia del objeto se agrega a las colas para la evaluación de ILM.
- Las solicitudes de CompleteMultipartUpload actualizan la hora del último acceso. El objeto completado se agrega a las colas para la evaluación de ILM.

Solicitar ejemplos

En este ejemplo se habilita la hora de último acceso para un bloque.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

En este ejemplo se deshabilita la hora de último acceso para un bloque.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configuración de notificaciones de metadatos de DELETE Bucket

La solicitud de configuración DE notificación DE metadatos DELETE Bucket permite deshabilitar el servicio de integración de búsqueda para bloques individuales al eliminar el XML de configuración.

Para completar esta operación, debe tener el permiso s3:DeleteBucketMetadataNotification para un bloque o ser raíz de cuenta.

Ejemplo de solicitud

Este ejemplo muestra cómo deshabilitar el servicio de integración de búsqueda para un bloque.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

OBTENGA la configuración de notificación de metadatos del bloque de datos

La solicitud de configuración DE notificación DE metadatos GET Bucket permite recuperar el XML de configuración que se utiliza para configurar la integración de búsqueda de bloques individuales.

Para completar esta operación, debe tener el permiso s3:GetBucketMetadataNotification, o ser raíz de la cuenta.

Ejemplo de solicitud

Esta solicitud recupera la configuración de notificación de metadatos para el depósito denominado `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Respuesta

El cuerpo de la respuesta incluye la configuración de notificación de metadatos para el bloque. La configuración de notificaciones de metadatos permite determinar cómo se configura el bloque para la integración de búsquedas. Es decir, permite determinar a qué objetos se indexan y a qué extremos se envían los metadatos de sus objetos.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Cada configuración de notificación de metadatos incluye una o varias reglas. Cada regla especifica los objetos a los que se aplica y el destino al que StorageGRID debe enviar metadatos de objetos. Los destinos se deben especificar con el URN de un extremo de StorageGRID.

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos Regla.	Sí

Nombre	Descripción	Obligatorio
Regla	Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Regla.	No
Estado	El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas. Incluido en el elemento Regla.	Sí
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para hacer coincidir todos los objetos, especifique un prefijo vacío. Incluido en el elemento Regla.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Regla.	Sí

Nombre	Descripción	Obligatorio
No	URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades: • `es` debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en la forma `domain-name/myindex/mytype`. Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404. El valor de urn se incluye en el elemento Destination.	Sí

Ejemplo de respuesta

El XML incluido entre las `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` etiquetas muestra cómo se configura la integración con un punto final de integración de búsqueda para el bloque. En este ejemplo, los metadatos del objeto se envían a un índice de Elasticsearch denominado `current` y tipo denominado `2017` que se aloja en un dominio de AWS denominado `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Información relacionada

"Usar una cuenta de inquilino"

Configuración de notificaciones de metadatos de PUT Bucket

La solicitud de configuración de notificación DE metadatos DE PUT Bucket permite habilitar el servicio de integración de búsqueda para bloques individuales. El XML de configuración de notificación de metadatos que se proporciona en el cuerpo de la solicitud especifica los objetos cuyos metadatos se envían al índice de búsqueda de destino.

Para completar esta operación, debe tener el permiso s3:PutBucketMetadataNotification para un bloque o ser raíz de la cuenta.

Solicitud

La solicitud debe incluir la configuración de notificación de metadatos en el cuerpo de la solicitud. Cada configuración de notificación de metadatos incluye una o varias reglas. Cada regla especifica los objetos a los que se aplica y el destino al que StorageGRID debe enviar metadatos de objetos.

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

Las configuraciones que tienen prefijos superpuestos no son válidas y se rechazan cuando se envían. Por ejemplo, no se permitiría una configuración que incluyera una regla para objetos con el prefijo `test` y una segunda regla para objetos con el prefijo `test2`.

Los destinos se deben especificar con el URN de un extremo de StorageGRID. El punto final debe existir

cuando se ejecuta la configuración de notificación de metadatos o la solicitud falla como A. `400 Bad Request` El mensaje de error indica: `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN`.

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

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

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

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

Solicitar ejemplos

Este ejemplo muestra habilitar la integración de búsqueda de un bloque. En este ejemplo, los metadatos de objeto de todos los objetos se envían al mismo destino.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

En este ejemplo, los metadatos del objeto para los objetos que coinciden con el prefijo `/images` se envían a un destino, mientras que los metadatos del objeto para los objetos que coinciden con el prefijo `/videos` se envían a un segundo destino.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<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>
```

JSON generado por el servicio de integración de búsqueda

Al habilitar el servicio de integración de búsqueda para un bloque, se genera un documento JSON y se envía al extremo de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas del objeto.

Este ejemplo muestra un ejemplo del JSON que podría generarse cuando se crea un objeto con la clave `SGWS/Tagging.txt` en un cubo llamado `test`. El `test` depósito no está versionado, por lo que la `versionId` etiqueta está vacía.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadatos de objetos incluidos en las notificaciones de metadatos

En la tabla se enumeran todos los campos que se incluyen en el documento JSON que se envían al extremo de destino cuando la integración de búsqueda está habilitada.

El nombre del documento incluye el nombre del bloque, el nombre del objeto y el ID de versión, si existe.

Tipo	Nombre del elemento	Descripción
Información sobre bloques y objetos	cucharón	Nombre del bloque
Información sobre bloques y objetos	clave	Nombre de clave de objeto
Información sobre bloques y objetos	ID de versión	Versión de objeto, para objetos en bloques con versiones
Información sobre bloques y objetos	región	Región de bloque, por ejemplo `us-east-1`
Metadatos del sistema	tamaño	Tamaño del objeto (en bytes) visible para un cliente HTTP
Metadatos del sistema	md5	Hash de objeto
Metadatos del usuario	metadatos *`key:value`*	Todos los metadatos de usuario del objeto, como pares clave-valor

Tipo	Nombre del elemento	Descripción
Etiquetas	etiquetas *key:value*	Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor

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

Información relacionada

"Usar una cuenta de inquilino"

OBTENGA la solicitud de uso del almacenamiento

La solicitud GET Storage Usage le indica la cantidad total de almacenamiento que está usando una cuenta y por cada bloque asociado con la cuenta.

La cantidad de almacenamiento utilizada por una cuenta y sus depósitos se puede obtener mediante una solicitud de ListBuckets modificada con el `x-ntap-sg-usage` parámetro de consulta. Se realiza un seguimiento del uso del almacenamiento en bloques de forma independiente de las solicitudes DE PUT y DELETE procesadas por el sistema. Es posible que haya algún retraso antes de que los valores de uso coincidan con los valores esperados en función del procesamiento de las solicitudes, especialmente si el sistema está sometido a cargas pesadas.

De forma predeterminada, StorageGRID intenta recuperar la información de uso con una coherencia global fuerte. Si no se puede lograr una coherencia global fuerte, StorageGRID intenta recuperar la información de uso en una coherencia de sitio fuerte.

Debe tener el permiso s3:ListAllMyBuckets o ser la raíz de la cuenta para completar esta operación.

Ejemplo de solicitud

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

Este ejemplo muestra una cuenta que tiene cuatro objetos y 12 bytes de datos en dos bloques. Cada bloque contiene dos objetos y seis bytes de datos.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Creación de versiones

Cada versión de objeto almacenada contribuirá a los `ObjectCount` valores y `DataBytes` en la respuesta. Los marcadores de borrado no se agregan al `ObjectCount` total.

Información relacionada

"Coherencia"

Solicitudes de bloque obsoletas para cumplimiento de normativas heredadas

Solicitudes de bloque obsoletas para cumplimiento de normativas heredadas

Es posible que deba utilizar la API DE REST de StorageGRID S3 para gestionar los bloques creados con la función de cumplimiento heredada.

Función de cumplimiento de normativas obsoleta

La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3.

Si anteriormente habilitó la configuración de cumplimiento global, la opción de bloqueo de objetos S3 global se habilita en StorageGRID 11.6. Ya no se pueden crear nuevos bloques con la función de cumplimiento habilitada; sin embargo, según sea necesario, se puede utilizar la API DE REST de StorageGRID S3 para gestionar bloques existentes que cumplen las normativas.

- "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
- "Gestión de objetos con ILM"
- "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

Solicitudes de cumplimiento de normativas obsoletas:

- "Obsoleto: PONGA modificaciones de solicitud de cucharón para el cumplimiento"

  El elemento XML de SGCompliance está obsoleto. Anteriormente, podría incluir este elemento personalizado de StorageGRID en el cuerpo de solicitud XML opcional de SOLICITUDES PUT Bucket para crear un bloque compatible.

- "Obsoleto: OBTENER cumplimiento de bloques"

  La solicitud de cumplimiento de normativas GET Bucket quedó obsoleta. Sin embargo, puede seguir utilizando esta solicitud para determinar la configuración de cumplimiento actual para un bloque compatible heredado existente.

- "Obsoleto: Cumplimiento de PUT Bucket"

  La solicitud de cumplimiento de normativas PUT Bucket quedó obsoleta. Sin embargo, puede seguir utilizando esta solicitud para modificar la configuración de cumplimiento de un bloque compatible heredado existente. Por ejemplo, puede colocar un bloque existente en la retención legal o aumentar su período de retención.

Obsoleto: Modificaciones de la solicitud de CreateBucket para el cumplimiento

El elemento XML de SGCompliance está obsoleto. Anteriormente, podía incluir este elemento personalizado de StorageGRID en el cuerpo de solicitud XML opcional de las solicitudes de CreateBucket para crear un depósito compatible.

> La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3. En la siguiente sección, se ofrecen más detalles:
>
> - "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
> - "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

Ya no se pueden crear bloques nuevos con el cumplimiento de normativas habilitado. Se devuelve el siguiente mensaje de error si intenta utilizar las modificaciones de solicitud de CreateBucket para la conformidad con el fin de crear un nuevo depósito compatible:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsoleto: OBTENER solicitud de cumplimiento de bloques

La solicitud de cumplimiento de normativas GET Bucket quedó obsoleta. Sin embargo, puede seguir utilizando esta solicitud para determinar la configuración de cumplimiento actual para un bloque compatible heredado existente.

> ⓘ La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3. En la siguiente sección, se ofrecen más detalles:
>
> - "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
> - "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

Para completar esta operación, debe tener el permiso s3:GetBucketCompliance o ser la raíz de la cuenta.

Ejemplo de solicitud

Esta solicitud de ejemplo le permite determinar la configuración de cumplimiento para el depósito denominado `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

En el XML de respuesta, `<SGCompliance>` muestra la configuración de cumplimiento vigente para el bloque. Esta respuesta de ejemplo muestra la configuración de cumplimiento de un bloque en el que se conservará cada objeto durante un año (525,600 minutos), a partir del momento en que el objeto se ingiere en la cuadrícula. Actualmente, no existe ningún derecho legal en este segmento. Cada objeto se eliminará automáticamente después de un año.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nombre	Descripción
RetentionPeriodonMinutes	La duración del período de retención para los objetos que se añadió a este bloque, en minutos. El período de retención se inicia cuando el objeto se ingiere en la cuadrícula.
LegalHold	• Cierto: Este segmento está actualmente bajo un control legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la conservación legal, incluso si ha caducado su período de retención. • Falso: Este segmento no está actualmente bajo un derecho. Los objetos de este bloque se pueden eliminar cuando expire su período de retención.
Eliminación automática	• True: Los objetos de este bloque se eliminarán automáticamente cuando expire su período de retención, a menos que el bloque se encuentre bajo una retención legal. • False: Los objetos de este bloque no se eliminarán automáticamente cuando finalice el período de retención. Debe eliminar estos objetos manualmente si necesita eliminarlos.

Respuestas de error

Si el depósito no se ha creado para que sea compatible, el código de estado HTTP de la respuesta es `404 Not Found`, con un código de error S3 `XNoSuchBucketCompliance` .

Obsoleto: Solicitud de cumplimiento de bloques PUT

La solicitud de cumplimiento de normativas PUT Bucket quedó obsoleta. Sin embargo, puede seguir utilizando esta solicitud para modificar la configuración de cumplimiento de un bloque compatible heredado existente. Por ejemplo, puede colocar un bloque existente en la retención legal o aumentar su período de retención.

La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3. En la siguiente sección, se ofrecen más detalles:

- "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
- "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

Debe tener el permiso s3:PutBucketCompliance o ser la raíz de la cuenta para completar esta operación.

Debe especificar un valor para cada campo de la configuración de cumplimiento al emitir una solicitud DE cumplimiento PUT Bucket.

Ejemplo de solicitud

Esta solicitud de ejemplo modifica la configuración de cumplimiento para el depósito denominado `mybucket`. En este ejemplo, los objetos de `mybucket` ahora se conservarán durante dos años (1.051.200 minutos) en lugar de un año, a partir del momento en que el objeto se ingiere en la cuadrícula. No existe ningún derecho legal en este segmento. Cada objeto se eliminará automáticamente después de dos años.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nombre	Descripción
RetentionPeriodonMinutes	La duración del período de retención para los objetos que se añadió a este bloque, en minutos. El período de retención se inicia cuando el objeto se ingiere en la cuadrícula. **Importante** Al especificar un nuevo valor para RetentionPeriodMinutes, debe especificar un valor que sea igual o mayor que el período de retención actual del bucket. Después de definir el período de retención del depósito, no puede disminuir ese valor; solo puede aumentarlo.

Nombre	Descripción
LegalHold	• Cierto: Este segmento está actualmente bajo un control legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la conservación legal, incluso si ha caducado su período de retención. • Falso: Este segmento no está actualmente bajo un derecho. Los objetos de este bloque se pueden eliminar cuando expire su período de retención.
Eliminación automática	• True: Los objetos de este bloque se eliminarán automáticamente cuando expire su período de retención, a menos que el bloque se encuentre bajo una retención legal. • False: Los objetos de este bloque no se eliminarán automáticamente cuando finalice el período de retención. Debe eliminar estos objetos manualmente si necesita eliminarlos.

Consistencia para la configuración de cumplimiento

Cuando se actualiza la configuración de cumplimiento de normativas para un bloque de S3 con una solicitud DE cumplimiento PUT Bucket, StorageGRID intenta actualizar los metadatos del bloque en el grid. De forma predeterminada, StorageGRID utiliza la consistencia **strong-global** para garantizar que todos los sitios del centro de datos y todos los nodos de almacenamiento que contienen metadatos del depósito tengan consistencia de lectura tras escritura para los ajustes de cumplimiento modificados.

Si StorageGRID no puede lograr la consistencia **fuerte-global** porque un sitio de centro de datos o varios nodos de almacenamiento en un sitio no están disponibles, el código de estado HTTP para la respuesta es `503 Service Unavailable.`

Si recibe esta respuesta, debe ponerse en contacto con el administrador de grid para garantizar que los servicios de almacenamiento requeridos estén disponibles en Lo antes posible.. Si el administrador de grid no puede poner a disposición suficientes nodos de almacenamiento en cada sitio, el soporte técnico puede indicarle que vuelva a intentar la solicitud fallida forzando la consistencia del **sitio fuerte**.

> Nunca fuerce la consistencia de **strong-site** para el cumplimiento de PUT bucket a menos que se le haya indicado hacerlo por el soporte técnico y a menos que comprenda las posibles consecuencias de usar este nivel.

Cuando la consistencia se reduce a **strong-site**, StorageGRID garantiza que la configuración de cumplimiento actualizada tendrá consistencia de lectura tras escritura solo para las solicitudes de los clientes dentro de un sitio. Esto significa que el sistema StorageGRID podría tener temporalmente varias configuraciones incoherentes para este bloque hasta que todos los sitios y nodos de almacenamiento estén disponibles. La configuración incoherente puede dar como resultado un comportamiento inesperado y no deseado. Por ejemplo, si va a colocar un bloque bajo una conservación legal y fuerza una menor coherencia, la configuración de cumplimiento anterior del bloque (es decir, la retención legal) puede seguir vigente en algunos sitios del centro de datos. Como resultado, los objetos que cree que están en retención legal se pueden eliminar cuando caduque su período de retención, ya sea por el usuario o por AutoDelete, si está activado.

Para forzar el uso de la consistencia **strong-site**, vuelva a emitir la solicitud de cumplimiento de PUT Bucket e incluya `Consistency-Control` el encabezado de solicitud HTTP, de la siguiente manera:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Respuestas de error

- Si el depósito no se ha creado para ser compatible, el código de estado HTTP para la respuesta es `404 Not Found`.
- Si `RetentionPeriodMinutes` en la solicitud es inferior al período de retención actual del depósito, el código de estado HTTP es `400 Bad Request`.

Información relacionada

"Obsoleto: PONGA modificaciones de solicitud de cucharón para el cumplimiento"

Administrar políticas de acceso

Utilizar políticas de acceso

StorageGRID utiliza el lenguaje de políticas de Amazon Web Services (AWS) para permitir que los inquilinos S3 controlen el acceso a bloques y objetos dentro de esos bloques. El sistema StorageGRID implementa un subconjunto del lenguaje de políticas de la API DE REST de S3. Las políticas de acceso para la API de S3 se escriben en JSON.

Información general sobre las políticas de acceso

StorageGRID admite tres tipos de políticas de acceso:

- **Políticas de cubo**, que se administran mediante las operaciones de la API GetBucketPolicy, PutBucketPolicy y DeleteBucketPolicy S3 o el administrador de inquilinos o la API de administración de inquilinos. Las políticas de bloque se asocian a bloques, por lo que se configuran para controlar el acceso de los usuarios de la cuenta de propietario del bloque u otras cuentas al bloque y a los objetos en él. La política de bloques se aplica únicamente a un bloque y, posiblemente, a varios grupos.
- **Políticas de grupo**, que se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Las directivas de grupo se asocian a un grupo de la cuenta, por lo que se configuran para permitir que dicho grupo tenga acceso a recursos específicos propiedad de dicha cuenta. La política de grupo se aplica únicamente a un grupo y, posiblemente, a varios bloques.
- **Políticas de sesión**, que se incluyen como parte de la realización de una solicitud AssumeRole. Las políticas de sesión solo se aplican a la sesión determinada, definiendo además los permisos que tiene el usuario, además de aquellos otorgados por la política de grupo y de depósito.

No hay diferencia de prioridad entre las políticas de grupo, de depósito y de sesión.

Las políticas de bloque y grupo de StorageGRID siguen una gramática específica definida por Amazon. Dentro de cada política hay una serie de declaraciones de política y cada sentencia contiene los siguientes elementos:

- ID de sentencia (Sid) (opcional)
- Efecto

- Principal/NotPrincipal
- Recurso/NotResource
- Acción/NotAction
- Condición (opcional)

Las sentencias de directiva se crean utilizando esta estructura para especificar permisos: Conceda <Effect> para permitir/denegar que <Principal> ejecute <Action> en <Resource> cuando se aplique <Condition>.

Cada elemento de directiva se utiliza para una función específica:

Elemento	Descripción
SID	El elemento Sid es opcional. El Sid sólo se ha diseñado como una descripción para el usuario. El sistema StorageGRID lo almacena pero no lo interpreta.
Efecto	Utilice el elemento Effect para establecer si se permiten o deniegan las operaciones especificadas. Debe identificar las operaciones que permite (o deniega) en cubos u objetos utilizando las palabras clave del elemento Acción admitido.
Principal/NotPrincipal	Puede permitir a los usuarios, grupos y cuentas acceder a recursos específicos y realizar acciones específicas. Si no se incluye ninguna firma S3 en la solicitud, se permite el acceso anónimo especificando el carácter comodín (*) como principal. De forma predeterminada, sólo la raíz de la cuenta tiene acceso a los recursos que pertenecen a la cuenta. Sólo es necesario especificar el elemento Principal en una política de bloque. Para las directivas de grupo, el grupo al que se asocia la directiva es el elemento Principal implícito.
Recurso/NotResource	El elemento Resource identifica los bloques y los objetos. Puede permitir o denegar permisos para cubos y objetos utilizando el nombre de recurso de Amazon (ARN) para identificar el recurso.
Acción/NotAction	Los elementos Acción y efecto son los dos componentes de los permisos. Cuando un grupo solicita un recurso, se le concede o se le deniega el acceso al recurso. Se deniega el acceso a menos que asigne permisos de forma específica, pero puede utilizar Denegar explícito para anular un permiso otorgado por otra directiva.
Condición	El elemento Condition es opcional. Las condiciones permiten crear expresiones para determinar cuándo se debe aplicar una directiva.

En el elemento Action , puede utilizar el carácter comodín (*) para especificar todas las operaciones o un subconjunto de operaciones. Por ejemplo, esta acción coincide con permisos como s3:GetObject, s3:PutObject y s3:DeleteObject.

```
s3:*Object
```

En el elemento Resource , puede utilizar los caracteres comodín (*) y (?). Aunque el asterisco (*) coincide con 0 o más caracteres, el signo de interrogación (?) coincide con cualquier carácter.

En el elemento Principal, no se admiten caracteres comodín excepto para establecer el acceso anónimo, que otorga permiso a todos. Por ejemplo, el comodín (*) se establece como el valor Principal.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

En el ejemplo siguiente, la instrucción utiliza los elementos Effect, Principal, Acción y recurso. En este ejemplo se muestra una sentencia de política de bloque completa que utiliza el efecto Permitir para otorgar a los principales, al grupo de administración `federated-group/admin` y al grupo financiero `federated-group/finance` , permisos para realizar la acción `s3:ListBucket` en el bloque denominado `mybucket` y la acción `s3:GetObject` en todos los objetos de ese bloque.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

La política de bloque tiene un límite de tamaño de 20,480 bytes y la política de grupo tiene un límite de tamaño de 5,120 bytes.

Coherencia de las políticas

De forma predeterminada, cualquier actualización que realice a las directivas de grupo será consistente. Cuando una normativa de grupo es coherente, los cambios pueden tardar 15 minutos adicionales en aplicarse debido al almacenamiento en caché de la política. Por defecto, cualquier actualización que realice en las políticas de depósito es fuertemente coherente.

Según sea necesario, puede cambiar las garantías de coherencia para las actualizaciones de la política de bloques. Por ejemplo, es posible que desee que un cambio en una política de bloque esté disponible durante una interrupción del servicio del sitio.

En este caso, puede establecer `Consistency-Control` el encabezado en la solicitud PutBucketPolicy, o puede utilizar la solicitud de consistencia PUT Bucket. Cuando una política de depósito es coherente, los cambios pueden tardar 8 segundos adicionales en aplicarse debido al almacenamiento en caché de la política.

> Si establece la consistencia en un valor diferente para resolver una situación temporal, asegúrese de volver a establecer el valor de nivel de cubo en su valor original cuando haya terminado. De lo contrario, todas las solicitudes de bloque futuras utilizarán la configuración modificada.

¿Qué es la política de sesión?

Una política de sesión es una política de acceso que restringe temporalmente los permisos disponibles durante una sesión específica, como cuando un usuario asume un grupo. Una política de sesión solo puede permitir un subconjunto de permisos y no puede otorgar permisos adicionales. El propio grupo podría tener permisos más amplios.

Utilice ARN en las declaraciones de política

En las declaraciones de política, el ARN se utiliza en los elementos Principal y Recursos.

- Utilice esta sintaxis para especificar el recurso ARN de S3:

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

- Utilice esta sintaxis para especificar el recurso de identidad ARN (usuarios y grupos):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Otras consideraciones:

- Puede utilizar el asterisco (*) como comodín para que coincida con cero o más caracteres dentro de la clave de objeto.
- Los caracteres internacionales, que se pueden especificar en la clave de objeto, deben codificarse

mediante JSON UTF-8 o mediante secuencias de escape JSON \u. No se admite el porcentaje de codificación.

"Sintaxis de URN RFC 2141"

El cuerpo de la solicitud HTTP para la operación PutBucketPolicy debe estar codificado con charset=UTF-8.

Especifique recursos en una política

En las sentencias de directiva, puede utilizar el elemento Resource para especificar el bloque o el objeto para el que se permiten o deniegan los permisos.

- Cada instrucción de directiva requiere un elemento Resource. En una política, los recursos se indican con el elemento `Resource`, o alternativamente, `NotResource` para la exclusión.
- Se especifican recursos con un ARN de recurso S3. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- También puede usar variables de política dentro de la clave de objeto. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- El valor del recurso puede especificar un bucket que todavía no existe cuando se crea una política de grupo.

Especifique los principales en una directiva

Utilice el elemento Principal para identificar al usuario, grupo o cuenta de arrendatario que la sentencia de directiva permite o deniega el acceso al recurso.

- Cada sentencia de política de una política de bloque debe incluir un elemento Principal. Las sentencias de política de una política de grupo no necesitan el elemento Principal porque se entiende que el grupo es el principal.
- En una política, los principales se denotan por el elemento Principal o, alternativamente, NotPrincipal para la exclusión.
- Las identidades basadas en cuentas se deben especificar mediante un ID o un ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- En este ejemplo se utiliza el ID de cuenta de inquilino 27233906934684427525, que incluye la raíz de la cuenta y todos los usuarios de la cuenta:

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Puede especificar sólo la raíz de la cuenta:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Puede especificar un usuario federado específico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Puede especificar un grupo federado específico ("managers"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Puede especificar un principal anónimo:

```
"Principal": "*"
```

- Para evitar ambigüedades, puede utilizar el UUID de usuario en lugar del nombre de usuario:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Por ejemplo, supongamos que Alex abandona la organización y se elimina el nombre de usuario `Alex`. Si un nuevo Alex se une a la organización y se le asigna el mismo `Alex` nombre de usuario, el nuevo usuario podría heredar involuntariamente los permisos otorgados al usuario original.

- El valor principal puede especificar un nombre de grupo/usuario que aún no existe cuando se crea una directiva de bloque.

Especificar permisos en una directiva

En una directiva, el elemento Acción se utiliza para permitir/denegar permisos a un recurso. Hay un conjunto de permisos que puede especificar en una directiva, que se indican mediante el elemento "Acción" o, alternativamente, "NotAction" para la exclusión. Cada uno de estos elementos se asigna a operaciones de API de REST de S3 específicas.

En las tablas se enumeran los permisos que se aplican a los bloques y los permisos que se aplican a los objetos.

> Amazon S3 ahora usa el permiso S3:PutReplicationConfiguration para las acciones PutBucketReplication y DeleteBucketReplication. StorageGRID utiliza permisos independientes para cada acción, que coinciden con la especificación original de Amazon S3.

Se realiza una supresión cuando se utiliza una PUT para sobrescribir un valor existente.

Permisos que se aplican a los bloques

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:CreateBucket	CreateBucket	Sí. **Nota**: Usar solo en la política de grupo.
s3:DeleteBucket	DeleteBucket	
s3:DeleteBucketMetadataNotification	Configuración de notificaciones de metadatos de DELETE Bucket	Sí
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBucketReplication	Sí, separe los permisos para PUT y DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	CUMPLIMIENTO de GET Bucket (obsoleto)	Sí
s3:GetBucketConsistency	OBTENGA coherencia de bloques	Sí
s3: GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	GET Bucket última hora de acceso	Sí
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	OBTENGA la configuración de notificación de metadatos del bloque de datos	Sí
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:GetBucketTagging	Etiquetado de GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListAllMyBuckets	• ListCuchers • Obtenga el uso del almacenamiento	Sí, para OBTENER uso de almacenamiento. **Nota**: Usar solo en la política de grupo.
s3:ListBucket	• ListObjects • Segmento de cabeza • RestoreObject	
s3:ListBucketMultipartUploads	• ListCargas multipartitas • RestoreObject	
s3:ListBucketVersions	OBTENGA las versiones DE Bucket	
s3:PutBucketCompliance	CUMPLIMIENTO de PUT Bucket (obsoleto)	Sí
s3:PutBucketConsistency	PONGA la consistencia del cucharón	Sí
s3: PutBucketCORS	• DeleteBucketCors† • A cargo de PutBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:PutBucketLastAccessTime	PUT Bucket última hora de acceso	Sí
s3:PutBucketMetadataNotification	Configuración de notificaciones de metadatos de PUT Bucket	Sí
s3:PutBucketNotification	PutBucketNotificationConfiguration	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:PutBucketObjectLockConfiguration	• CreateBucket con `x-amz-bucket-object-lock-enabled: true` el encabezado de solicitud (también requiere el permiso S3:CreateBucket) • PutObjectLockConfiguration	
s3:PutBucketPolicy	Política de PutBucketPolicy	
s3:PutBucketEtiquetado	• DeleteBucketTagging† • PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLipeycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	Sí, separe los permisos para PUT y DELETE

Permisos que se aplican a objetos

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:AbortMultipartUpload	• AbortMultipartUpload • RestoreObject	
s3:BypassGovernanceRetention	• DeleteObject • DeleteObjects • PutObjectRetention	
s3:DeleteObject	• DeleteObject • DeleteObjects • RestoreObject	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (una versión específica del objeto)	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:DeleteObjectVersion	DeleteObject (una versión específica del objeto)	
s3:GetObject	• GetObject • Objeto principal • RestoreObject • SelectObjectContent	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectEtiquetado	
s3:GetObjectVersionTagging	GetObjectTagging (una versión específica del objeto)	
s3:GetObjectVersion	GetObject (una versión específica del objeto)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• Objeto de puta • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectEtiquetado	PutObjectEtiquetado	
s3:PutObjectVersionEtiquetado	PutObjectTagging (una versión específica del objeto)	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:PutOverwriteObject	• Objeto de puta • CopyObject • PutObjectEtiquetado • DeleteObjectTagging • CompleteMultipartUpload	Sí
s3:RestoreObject	RestoreObject	

Utilice el permiso PutOverwriteObject

el permiso s3:PutOverwriteObject es un permiso StorageGRID personalizado que se aplica a operaciones que crean o actualizan objetos. La configuración de este permiso determina si el cliente puede sobrescribir los datos de un objeto, metadatos definidos por el usuario o el etiquetado de objetos S3.

Entre los posibles ajustes para este permiso se incluyen:

- **Permitir**: El cliente puede sobrescribir un objeto. Esta es la configuración predeterminada.
- **Denegar**: El cliente no puede sobrescribir un objeto. Cuando se establece en Denegar, el permiso PutOverwriteObject funciona de la siguiente manera:
  - Si se encuentra un objeto existente en la misma ruta:
    - Los datos del objeto, los metadatos definidos por el usuario o el etiquetado de objetos S3 no se pueden sobrescribir.
    - Se cancela cualquier operación de ingesta en curso y se devuelve un error.
    - Si el control de versiones S3 está activado, la configuración Denegar impide que las operaciones PutObjectTagging o DeleteObjectTagging modifiquen el TagSet para un objeto y sus versiones no actuales.
  - Si no se encuentra un objeto existente, este permiso no tiene efecto.
- Cuando este permiso no está presente, el efecto es el mismo que si se estableció permitir.

> Si la política S3 actual permite sobrescribir y el permiso PutOverwriteObject está configurado en Denegar, el cliente no puede sobrescribir los datos de un objeto, los metadatos definidos por el usuario ni el etiquetado de objetos. Además, si la casilla de verificación **Impedir modificación del cliente** está seleccionada (**Configuración** > **Configuración de seguridad** > **Red y objetos**), esa configuración anula la configuración del permiso PutOverwriteObject.

Especificar condiciones en una política

Las condiciones definen cuándo estará en vigor una política. Las condiciones consisten en operadores y pares clave-valor.

Condiciones Utilice pares clave-valor para la evaluación. Un elemento Condition puede contener varias condiciones y cada condición puede contener varios pares clave-valor. El bloque Condition utiliza el siguiente formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

En el ejemplo siguiente, la condición ipaddress utiliza la clave de condición SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Operadores de condición admitidos

Los operadores de condición se categorizan de la siguiente manera:

- Cadena
- Numérico
- Booleano
- Dirección IP
- Comprobación nula

Operadores de condición	Descripción
StringEquals	Compara una clave con un valor de cadena basado en la coincidencia exacta (distingue entre mayúsculas y minúsculas).
StringNotEquals	Compara una clave con un valor de cadena basado en la coincidencia negada (distingue entre mayúsculas y minúsculas).
StringEqualizsIgnoreCase	Compara una clave con un valor de cadena basado en la coincidencia exacta (omite Case).
StringNotEqualizsIgnoreCase	Compara una clave con un valor de cadena basado en la coincidencia negada (omite Case).
StringLike	Compara una clave con un valor de cadena basado en la coincidencia exacta (distingue entre mayúsculas y minúsculas). Puede incluir caracteres comodín * y ?.
StringNotLike	Compara una clave con un valor de cadena basado en la coincidencia negada (distingue entre mayúsculas y minúsculas). Puede incluir caracteres comodín * y ?.

Operadores de condición	Descripción
Valores numéricos	Compara una clave con un valor numérico basado en la coincidencia exacta.
NumericNotEquals	Compara una clave con un valor numérico basado en la coincidencia negada.
NumericGreatertan	Compara una clave con un valor numérico basado en la coincidencia mayor que.
NumericGreaterThanEquals	Compara una clave con un valor numérico en función de la coincidencia mayor o igual que.
NumericLessThan	Compara una clave con un valor numérico basado en la coincidencia menor que.
NumericLesThanEquals	Compara una clave con un valor numérico en función de la coincidencia menor o igual que.
Bool	Compara una clave con un valor booleano basado en la coincidencia “true o false”.
IPAddress	Compara una clave con una dirección IP o un rango de direcciones IP.
NotIpAddress	Compara una clave con una dirección IP o un intervalo de direcciones IP basándose en la coincidencia negada.
Nulo	Comprueba si hay una clave de condición en el contexto actual de la solicitud.
Si existe	Se agrega a cualquier operador de condición, excepto la condición Nula, para verificar la ausencia de esa clave de condición. Devuelve VERDADERO si la clave de condición no está presente.

Teclas de condición compatibles

Teclas de condición	Acciones	Descripción
aws:SourceIp	Operadores IP	Comparará con la dirección IP desde la que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos. **Nota:** Si la solicitud S3 se envió a través del servicio Load Balancer en nodos Admin y nodos de Gpuertas de enlace, se comparará con la dirección IP anterior al servicio Load Balancer. **Nota**: Si se utiliza un equilibrador de carga no transparente de terceros, se comparará con la dirección IP de ese equilibrador de carga. Cualquier `X-Forwarded-For` encabezado se ignorará porque no se puede determinar su validez.
aws:nombre de usuario	Recurso/identidad	Comparará con el nombre de usuario del remitente desde el que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos.
s3:delimitador	s3:ListBucket y. s3:ListBucketVersions permisos	Se comparará con el parámetro delimitador especificado en una solicitud ListObjects o ListObjectVersions.
S3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging S3:PutObjectAcl s3:PutObjectEtiquetado S3:PutObjectVersionAcl s3:PutObjectVersionEtiquetado	Requerirá que el objeto existente tenga la clave de etiqueta y el valor específicos.

Teclas de condición	Acciones	Descripción
s3:max-keys	s3:ListBucket y. s3:ListBucketVersions permisos	Se compara con el parámetro max-keys especificado en una solicitud ListObjects o ListObjectVersions.
s3: modo de bloqueo de objeto	s3:PutObject	Se compara con el `object-lock-mode` ampliado desde el encabezado de solicitud en la solicitud PutObject, CopyObject y CreateMultipartUpload.
s3: modo de bloqueo de objeto	s3:PutObjectRetention	Se compara con el `object-lock-mode` ampliado desde el cuerpo XML en la solicitud PutObjectRetention.
s3:retención-días restante del bloqueo de objetos	s3:PutObject	Se compara con la fecha de retención especificada en `x-amz-object-lock-retain-until-date` la cabecera de solicitud o calculada a partir del período de retención por defecto de período para asegurarse de que estos valores se encuentran dentro del rango permitido para las siguientes solicitudes: • Objeto de puta • CopyObject • CreateMultipartUpload
s3:retención-días restante del bloqueo de objetos	s3:PutObjectRetention	Se compara con la fecha de retención especificada en la solicitud PutObjectRetention para asegurarse de que se encuentra dentro del rango permitido.
s3:prefijo	s3:ListBucket y. s3:ListBucketVersions permisos	Se comparará con el parámetro PreFIX especificado en una solicitud ListObjects o ListObjectVersions.
S3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectEtiquetado s3:PutObjectVersionEtiquetado	Requerirá una clave y un valor de etiqueta específicos cuando la solicitud del objeto incluya el etiquetado.
algoritmo de cifrado del lado del servidor s3:x-amz para el cliente	s3:PutObject	Se compara con el `sse-customer-algorithm` o al `copy-source-sse-customer-algorithm` ampliado desde el encabezado de solicitud en la solicitud PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy y CompleteMultipartUpload.

Especifique las variables en una política

Las variables de las directivas se pueden utilizar para rellenar la información de directivas cuando esté disponible. Puede utilizar variables de política en el `Resource` elemento y en comparaciones de cadenas en el `Condition` elemento.

En este ejemplo, la variable `${aws:username}` forma parte del elemento Resource:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

En este ejemplo, la variable `${aws:username}` forma parte del valor de condición en el bloque de condición:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variable	Descripción
`${aws:SourceIp}`	Utiliza la clave SourceIp como la variable proporcionada.
`${aws:username}`	Utiliza la clave de nombre de usuario como la variable proporcionada.
`${s3:prefix}`	Utiliza la clave de prefijo específica del servicio como variable proporcionada.
`${s3:max-keys}`	Utiliza la clave de max-keys específica del servicio como la variable proporcionada.
`${*}`	Carácter especial. Utiliza el carácter como carácter literal *.
`${?}`	Carácter especial. Utiliza el carácter como un carácter literal ?.
`${$}`	Carácter especial. Utiliza el carácter como carácter literal $.

Crear directivas que requieran un manejo especial

A veces, una directiva puede otorgar permisos peligrosos para la seguridad o para operaciones continuas, como bloquear al usuario raíz de la cuenta. La implementación de la API REST de StorageGRID S3 es menos restrictiva durante la validación de políticas que Amazon, pero igual de estricta durante la evaluación de la política.

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
Denegar a sí mismo cualquier permiso a la cuenta raíz	Cucharón	Válido y reforzado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bloques de S3	Igual
Denegar a sí mismo cualquier permiso al usuario o grupo	Grupo	Válido y reforzado	Igual
Permitir cualquier permiso para un grupo de cuentas externo	Cucharón	Principal no válido	Válidos, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un método 405 no permitido cuando lo permite una política
Permitir cualquier permiso para una raíz de cuenta externa o para un usuario	Cucharón	Válidos, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un método 405 no permitido cuando lo permite una política	Igual
Permitir que todos tengan permisos para todas las acciones	Cucharón	Válido, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un error de método 405 no permitido para la raíz de cuenta externa y los usuarios	Igual
Denegar a todos los permisos a todas las acciones	Cucharón	Válido y reforzado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bloques de S3	Igual
Principal es un usuario o grupo inexistente	Cucharón	Principal no válido	Válido
El recurso es un bloque de S3 que no existe	Grupo	Válido	Igual
El director es un grupo local	Cucharón	Principal no válido	Válido

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
Policy otorga a una cuenta no propietaria (incluidas las cuentas anónimas) permisos para colocar objetos.	Cucharón	Válido. Los objetos son propiedad de la cuenta creadora y la política de bucket no se aplica. La cuenta de creador debe otorgar permisos de acceso al objeto mediante ACL de objeto.	Válido. Los objetos son propiedad de la cuenta de propietario del bloque. Se aplica la política de bloques.

Protección WORM (escritura única lectura múltiple)

Se pueden crear bloques DE escritura única y lectura múltiple (WORM) para proteger los datos, los metadatos de objetos definidos por el usuario y el etiquetado de objetos de S3. Puede configurar los bloques WORM para permitir la creación de objetos nuevos y evitar sobrescrituras o eliminaciones del contenido existente. Utilice uno de los enfoques aquí descritos.

Para asegurarse de que las sobrescrituras se deniegan siempre, puede:

- Desde el Administrador de red, vaya a **Configuración** > **Seguridad** > **Configuración de seguridad** > **Red y objetos** y seleccione la casilla de verificación **Evitar modificación del cliente**.
- Aplique las siguientes reglas y políticas de S3:
  - Agregue una operación PUTOVERWRITEOBJECT DENY a la directiva S3.
  - Agregue una operación DeleteObject DENY a la directiva S3.
  - Agregue una operación PutObject ALLOW a la política S3.

> Si se configura DeleteObject como DENEGADO en una política de S3, ILM no impide que elimine objetos cuando existe una regla como «copias cero tras 30 días».

> Incluso cuando se aplican todas estas reglas y políticas, no protegen frente a escrituras simultáneas (consulte la situación A). Protegen contra sobrescrituras completadas secuenciales (consulte la situación B).

Situación A: Escrituras simultáneas (no protegidas contra)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situación B: Sobrescrituras completadas secuenciales (protegidas contra)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Información relacionada

- "Cómo gestionan las reglas de ILM de StorageGRID los objetos"
- "Ejemplo de políticas de bloque"
- "Ejemplo de políticas de grupo"
- "Ejemplo de política de sesión"
- "Gestión de objetos con ILM"
- "Usar una cuenta de inquilino"

Ejemplo de política de sesión

Utilice el siguiente ejemplo para crear una política de sesión StorageGRID .

Ejemplo: Configurar una política de sesión que permita la recuperación de objetos

En este ejemplo, al principal de la sesión solo se le permite recuperar objetos del bucket1. Todas las demás acciones se deniegan implícitamente, excepto las acciones específicas de StorageGRID, como el uso de"s3:PutOverwriteObject" permiso. La política de sesión se puede proporcionar como un archivo JSON al llamar a la API AssumeRole.

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

Ejemplo de políticas de bloque

Utilice los ejemplos de esta sección para crear políticas de acceso StorageGRID para buckets.

Las políticas de bloque especifican los permisos de acceso para el bloque al que está asociada la directiva. Puede configurar una política de depósito mediante la API PutBucketPolicy de S3 a través de una de estas herramientas:

- "Administrador de inquilinos".
- CLI de AWS con este comando (consulte "Operaciones en bloques"):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Ejemplo: Permitir que todos tengan acceso de solo lectura a un bloque

En este ejemplo, a todos, incluido el anónimo, se les permite enumerar objetos en el depósito y realizar operaciones GetObject en todos los objetos del depósito. Se denegarán todas las demás operaciones. Tenga en cuenta que esta política puede no ser particularmente útil porque nadie, excepto la raíz de la cuenta, tiene permisos para escribir en el depósito.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Ejemplo: Permitir que todos en una cuenta tengan acceso total y que todas las personas de otra cuenta tengan acceso de solo lectura a un bloque

En este ejemplo, todos los usuarios de una cuenta especificada tienen acceso completo a un depósito, mientras que todos los usuarios de otra cuenta especificada solo pueden listar el depósito y realizar operaciones GetObject en objetos del depósito empezando por el `shared/` prefijo de clave de objeto.

> En StorageGRID, los objetos creados por una cuenta que no es propietaria (incluidas las cuentas anónimas) son propiedad de la cuenta de propietario del bloque. La política de bloque se aplica a estos objetos.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Ejemplo: Permitir que todo el mundo tenga acceso de solo lectura a un bloque y acceso completo por un grupo especificado

En este ejemplo, todos, incluidos los anónimos, pueden enumerar el depósito y realizar operaciones GetObject en todos los objetos del depósito, mientras que solo los usuarios que pertenecen al grupo `Marketing` en la cuenta especificada tienen acceso completo.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Ejemplo: Permitir que todo el mundo tenga acceso de lectura y escritura a un bloque si un cliente se encuentra en el rango de IP

En este ejemplo, todos, incluido el anónimo, pueden enumerar el bloque y realizar cualquier operación Object en todos los objetos del bloque, siempre que las solicitudes provengan de un intervalo IP especificado (54.240.143.0 a 54.240.143.255, excepto 54.240.143.188). Se denegarán todas las demás operaciones y se denegarán todas las solicitudes que estén fuera del rango de IP.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Ejemplo: Permitir el acceso completo a un bloque exclusivamente por un usuario federado especificado

En este ejemplo, al usuario federado Alex se le permite el acceso completo al `examplebucket` bucket y sus objetos. A todos los demás usuarios, incluido "root", se les deniega explícitamente todas las operaciones. Tenga en cuenta, sin embargo, que "root" nunca se le deniegan los permisos para poner/obtener/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Ejemplo: Permiso PutOverwriteObject

En este ejemplo, el `Deny` efecto para PutOverwriteObject y DeleteObject garantiza que nadie pueda sobrescribir o eliminar los datos del objeto, los metadatos definidos por el usuario y el etiquetado de objetos S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Ejemplo de políticas de grupo

Utilice los ejemplos de esta sección para crear políticas de acceso StorageGRID para grupos.

Las directivas de grupo especifican los permisos de acceso para el grupo al que está asociada la directiva. No hay `Principal` ningún elemento en la política porque está implícito. Las políticas de grupo se configuran con el administrador de inquilinos o la API.

Ejemplo: Establecer la directiva de grupo mediante el Administrador de inquilinos

Al agregar o editar un grupo en el Gestor de inquilinos, puede seleccionar una política de grupo para determinar qué permisos de acceso S3 tendrán los miembros de este grupo. Consulte "Cree grupos para un inquilino de S3".

- **Sin acceso S3**: Opción predeterminada. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que el acceso se conceda con una política de bloque. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3.
- **Acceso de sólo lectura**: Los usuarios de este grupo tienen acceso de sólo lectura a los recursos S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puede editar esta cadena.
- **Acceso completo**: Los usuarios de este grupo tienen acceso completo a los recursos S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena.
- **Ransomware Mitigation**: Esta política de muestra se aplica a todos los cubos para este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden suprimir de forma permanente objetos de los bloques que tienen activado el control de versiones de objetos.

  Los usuarios del gestor de inquilinos que tengan el permiso Gestionar todos los bloques pueden sustituir esta política de grupo. Limite el permiso Gestionar todos los buckets a usuarios de confianza y use la autenticación multifactor (MFA) cuando esté disponible.

- **Personalizado**: A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

Ejemplo: Permite el acceso total de grupos a todos los bloques

En este ejemplo, a todos los miembros del grupo se les permite el acceso completo a todos los segmentos que pertenecen a la cuenta de inquilino, a menos que la política de bloque lo deniegue explícitamente.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Ejemplo: Permitir el acceso de solo lectura de grupo a todos los bloques

En este ejemplo, todos los miembros del grupo tienen acceso de solo lectura a recursos S3, a menos que la política de bloque lo deniegue explícitamente. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Ejemplo: Permitir a los miembros del grupo acceso completo solo a su carpeta en un depósito

En este ejemplo, sólo se permite a los miembros del grupo que enumeren y tengan acceso a su carpeta específica (prefijo de clave) en el bloque especificado. Tenga en cuenta que los permisos de acceso de otras políticas de grupo y la directiva de bloque deben tenerse en cuenta al determinar la privacidad de estas carpetas.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

Los servicios de StorageGRID generan los mensajes de auditoría y se almacenan en archivos de registro de texto. Es posible revisar los mensajes de auditoría específicos de S3 en el registro de auditoría para obtener detalles sobre las operaciones de bloques y objetos.

Se realizó un seguimiento de las operaciones de bloque en los registros de auditoría

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- Etiquetado de GetBucketTagging
- Segmento de cabeza
- ListObjects
- ListObjectVersions
- CUMPLIR con la normativa de los bloques
- PutBucketTagging
- PutBucketVersioning

Se realizó un seguimiento de las operaciones de objetos en los registros de auditoría

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- Objeto principal
- Objeto de puta
- RestoreObject
- Seleccionar objeto
- UploadPart (cuando una regla de ILM utiliza una ingesta equilibrada o estricta)
- UploadPartCopy (cuando una regla de ILM utiliza una ingesta equilibrada o estricta)

Información relacionada

- "Acceda al archivo de registro de auditoría"
- "El cliente escribe mensajes de auditoría"
- "El cliente lee los mensajes de auditoría"

Usar la API de REST de Swift (fin de vida útil)

Use la API DE REST de Swift

La compatibilidad con la API de Swift ha llegado al final de su vida útil y se quitará en una futura versión.

Se han eliminado los detalles de Swift de esta versión del sitio del documento. Consulte "StorageGRID 11,8: Use la API REST DE Swift".