



Utilice StorageGRID

StorageGRID

NetApp
November 04, 2025

Tabla de contenidos

| | |
|--|-----|
| Utilice StorageGRID | 1 |
| Usar una cuenta de inquilino | 1 |
| Usar una cuenta de inquilino: Descripción general | 1 |
| Cómo iniciar sesión y salir | 2 |
| Conozca la consola de tenant Manager | 7 |
| API de gestión de inquilinos | 10 |
| Utilizar conexiones de federación de grid | 15 |
| Gestionar grupos y usuarios | 28 |
| Gestión de claves de acceso de S3 | 47 |
| Gestión de bloques S3 | 52 |
| Gestione servicios de plataformas S3 | 73 |
| USE LA API DE REST DE S3 | 113 |
| Versiones y actualizaciones compatibles con la API de REST DE S3 | 113 |
| Referencia rápida: Solicitudes de API de S3 admitidas | 116 |
| Configure las conexiones y las cuentas de inquilino | 135 |
| Soporte para servicios de plataforma StorageGRID | 138 |
| Cómo StorageGRID implementa la API DE REST de S3 | 139 |
| Soporte para la API de REST DE Amazon S3 | 156 |
| Solicitudes de StorageGRID S3 | 206 |
| Políticas de acceso a bloques y grupos | 227 |
| Configure la seguridad de la API DE REST | 252 |
| Supervisar y auditar operaciones | 254 |
| Ventajas de las conexiones HTTP activas, inactivas y simultáneas | 257 |
| Usar la API REST DE Swift (obsoleto) | 260 |
| Use la API de REST DE Swift: Información general | 260 |
| Configure las conexiones y las cuentas de inquilino | 263 |
| Operaciones compatibles con la API REST de Swift | 267 |
| Operaciones de la API de REST de StorageGRID Swift | 280 |
| Configure la seguridad de la API DE REST | 284 |
| Supervisar y auditar operaciones | 286 |

Utilice StorageGRID

Usar una cuenta de inquilino

Usar una cuenta de inquilino: Descripción general

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

¿Qué es una cuenta de inquilino?

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

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

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



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

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

Cómo crear una cuenta de inquilino

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

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

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

Configure los inquilinos S3

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

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



Aunque puede crear y administrar buckets S3 con el administrador de inquilinos, debe usar un cliente S3 para procesar y gestionar objetos. Consulte ["USE LA API DE REST DE S3"](#) para obtener más detalles.

Configure los inquilinos Swift

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

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



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

Cómo iniciar sesión y salir

Inicie sesión en el Administrador de inquilinos

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

Antes de empezar

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

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

`https://FQDN_or_Admin_Node_IP:port/`

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

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

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

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

Pasos

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

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

No se utiliza SSO

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

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



NetApp StorageGRID®

Grid Manager

Username

Password

[Sign in](#)

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

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

The screenshot shows the NetApp StorageGRID Tenant Manager login interface. At the top is the NetApp StorageGRID logo. Below it is the title 'Tenant Manager'. The form includes a 'Recent' dropdown menu currently showing '-- Optional --'. Below that is an 'Account' field containing the 20-digit ID '64600207336181242061'. The 'Username' field is empty and highlighted with a blue border. The 'Password' field is also empty. A blue 'Sign in' button is located below the password field. At the bottom of the form, there are links for 'NetApp support' and 'NetApp.com'.

- i. Si no se muestra el ID de cuenta de 20 dígitos del arrendatario, seleccione el nombre de la cuenta de arrendatario si aparece en la lista de cuentas recientes o introduzca el ID de cuenta.
- ii. Introduzca su nombre de usuario y contraseña.
- iii. Seleccione **Iniciar sesión**.

Aparece el panel de control del gestor de inquilinos.

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

Uso de SSO

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

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

Sign in with your organizational account

someone@example.com

Password

Sign in

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

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

NetApp StorageGRID®

Tenant Manager

Recent

S3 tenant ▼

Account

62984032838045582045

Sign in

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

- 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.
- Seleccione **Iniciar sesión**.
- Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

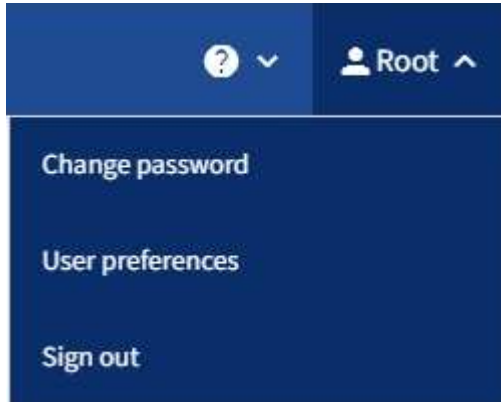
Aparece el panel de control del gestor de inquilinos.

Cierre la sesión del responsable de inquilinos

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

Pasos

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



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

- Si SSO no está en uso:

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



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

- Si SSO está habilitado:

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



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

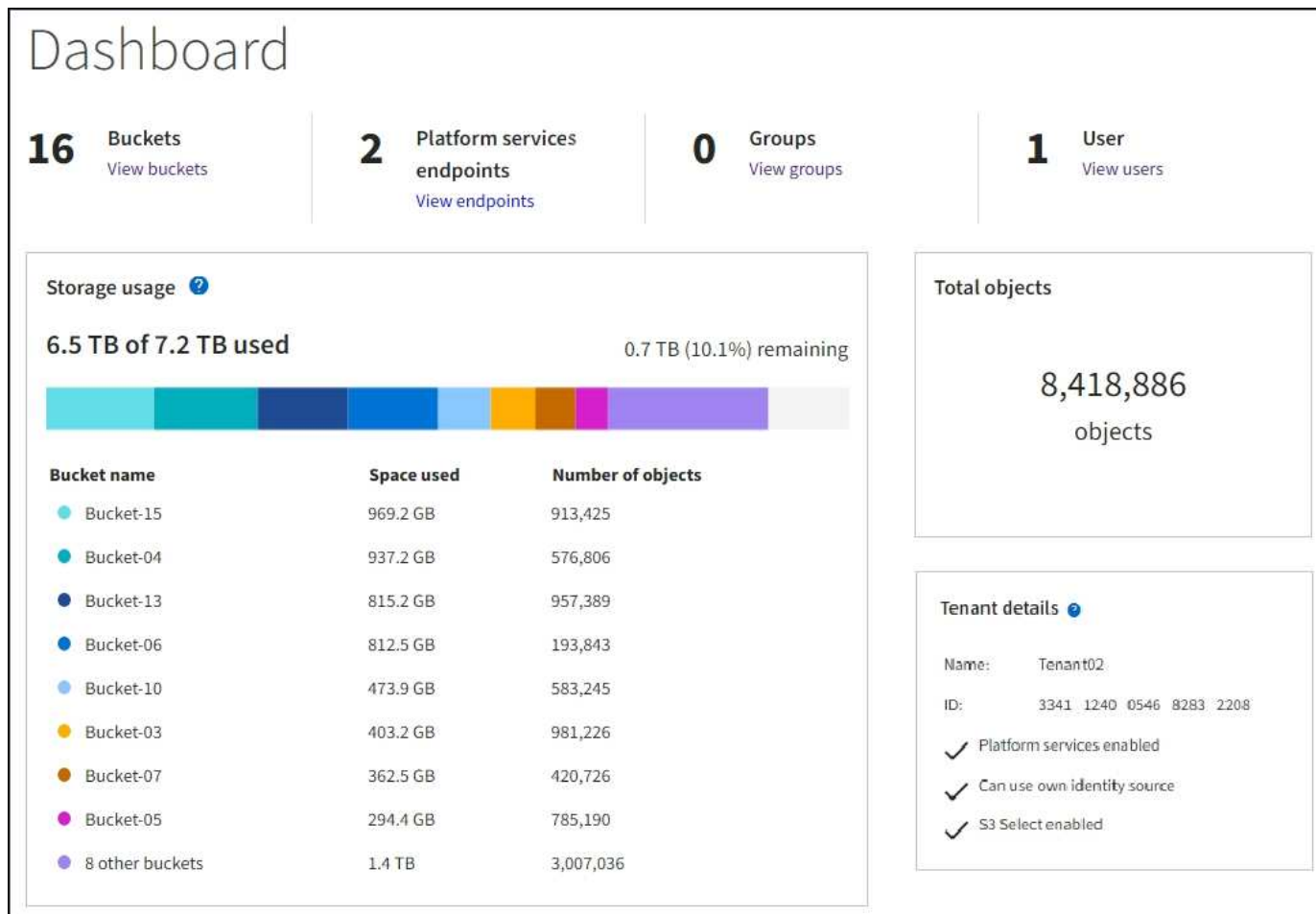
Conozca la consola de tenant Manager

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



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

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



Resumen de la cuenta de inquilino

La parte superior del panel contiene la siguiente información:

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

Puede seleccionar los enlaces para ver los detalles.

La parte derecha del panel contiene la siguiente información:

- Número total de objetos para el arrendatario.

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

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

Aprovechamiento del almacenamiento y de la cuota

El panel uso del almacenamiento contiene la siguiente información:

- La cantidad de datos de objeto para el inquilino.



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

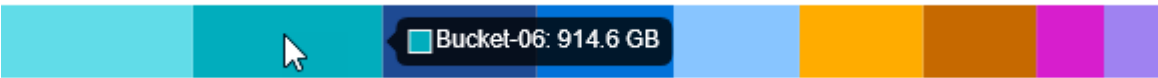
- Si se establece una cuota, la cantidad total de espacio disponible para los datos del objeto y la cantidad y el porcentaje de espacio restante. La cuota limita la cantidad de datos de objetos que se pueden procesar.












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

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

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



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

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

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



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


Alertas de uso de cuotas

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

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


 Only 0.6% of the quota is remaining. If the quota is exceeded, you can no longer upload new objects.

Si excedes tu cuota, no podrás cargar nuevos objetos.

 The quota has been met. You cannot upload new objects.

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.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

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

API de gestión de inquilinos

Comprender la API de gestión de inquilinos

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

API de gestión de inquilinos:

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

- Utiliza ["creación de versiones para dar cabida a actualizaciones no disruptivas"](#).

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

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

Operaciones de API

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

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

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

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



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

- **Config:** Operaciones relacionadas con el lanzamiento del producto y versiones de la API de Gestión de Inquilinos. Puede mostrar la versión de la versión del producto y las versiones principales de la API que admite esa versión.
- **Contenedores:** Operaciones en S3 cubos o contenedores Swift.
- **Funciones desactivadas:** Operaciones para ver características que podrían haber sido desactivadas.
- **Endpoints:** Operaciones para gestionar un endpoint. Los extremos permiten que un bloque de S3 use un servicio externo para la replicación de CloudMirror de StorageGRID, notificaciones o integración de búsqueda.
- **Grid-federation-connections:** Operaciones en conexiones de federación de grid y replicación entre grid.
- **GRUPOS:** Operaciones para administrar grupos de inquilinos locales y para recuperar grupos de inquilinos federados de una fuente de identidad externa.
- **Identity-source:** Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información federada del grupo y del usuario.
- **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.

groups Operations on groups

GET /org/groups Lists Tenant User Groups

Parameters Try it out

| Name | Description |
|-------------------------------------|---|
| type string (query) | filter by group type |
| limit integer (query) | maximum number of results |
| marker string (query) | marker-style pagination offset (value is Group's URN) |
| includeMarker boolean (query) | if set, the marker element is also returned |
| order string (query) | pagination order (desc requires marker) |

Responses Response content type **application/json**

| Code | Description |
|------|--|
| 200 | <div><div>Example Value</div><div>Model</div><pre>{ "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.2" }</pre></div> |

Emita solicitudes API



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

Pasos

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

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

Creación de versiones de la API de gestión de inquilinos

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

Por ejemplo, esta URL de solicitud especifica la versión 3 de la API.

`https://hostname_or_ip_address/api/v3/authorize`

La versión principal de la API de administración de inquilinos se salta cuando se realizan cambios que son *no compatibles* con versiones anteriores. La versión secundaria de la API de gestión de inquilinos 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 |

Cuando el software StorageGRID se instala por primera vez, solo se habilita la versión más reciente de la API de gestión de inquilinos. Sin embargo, cuando StorageGRID se actualiza a una versión de función nueva, sigue teniendo acceso a la versión de API anterior para al menos una versión de la función StorageGRID.

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

Determine qué versiones de API son compatibles en la versión actual

Utilice la siguiente solicitud de API para devolver una lista de las versiones principales de API admitidas:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Especifique la versión de API para la solicitud

Puede especificar la versión de API mediante un parámetro path (/api/v3) o un encabezado (Api-Version: 3). Si proporciona ambos valores, el valor de encabezado anula el valor de ruta de acceso.

```
curl https://<IP-Address>/api/v3/grid/accounts
```

```
curl -H "Api-Version: 3" https://<IP-Address>/api/grid/accounts
```

Protección contra falsificación de solicitudes entre sitios (CSRF)

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

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

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

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

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


Cuando es verdadero, un `GridCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en Grid Manager y en `AccountCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en el Administrador de inquilinos.

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

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

Para configurar la protección CSRF, utilice ["API de gestión de grid"](#) o ["API de gestión de inquilinos"](#).



Las solicitudes que tienen un conjunto de cookies de token CSRF también harán cumplir el `"Content-Type: application/json"` Encabezado para cualquier solicitud que espera un cuerpo de solicitud JSON como protección adicional contra ataques CSRF.

Utilizar conexiones de federación de grid

Clone los usuarios y los grupos de inquilinos

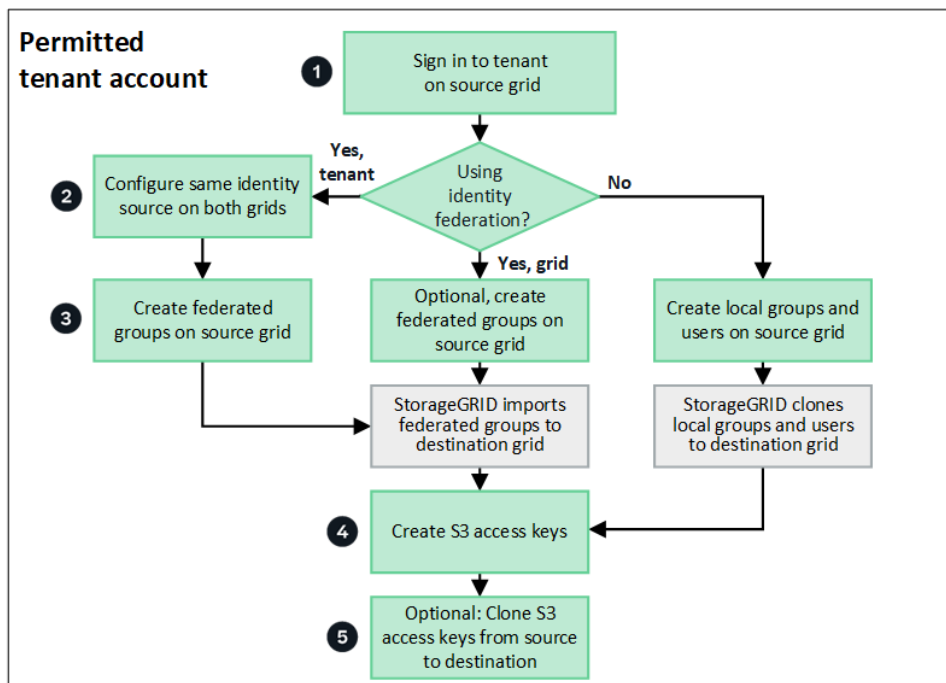
Si un nuevo inquilino tiene permiso para utilizar una conexión de federación de grid, ese inquilino se replica desde un sistema StorageGRID a otro sistema StorageGRID cuando se crea. Una vez que se ha replicado el inquilino, todos los grupos y usuarios que se añadan al inquilino de origen se clonan en el inquilino de destino.

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

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

Flujo de trabajo de inquilino para el clon de cuenta

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



Estos son los pasos principales del flujo de trabajo:

1

Inicie sesión en el inquilino

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

2

Opcionalmente, configure la federación de identidades

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

3

Crear grupos y usuarios

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

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

4

Crear claves de acceso S3

Puede hacerlo "[cree sus propias claves de acceso](#)" o hasta "[crear claves de acceso de otro usuario](#)" en la

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

5

Opcionalmente, clone las claves de acceso S3

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

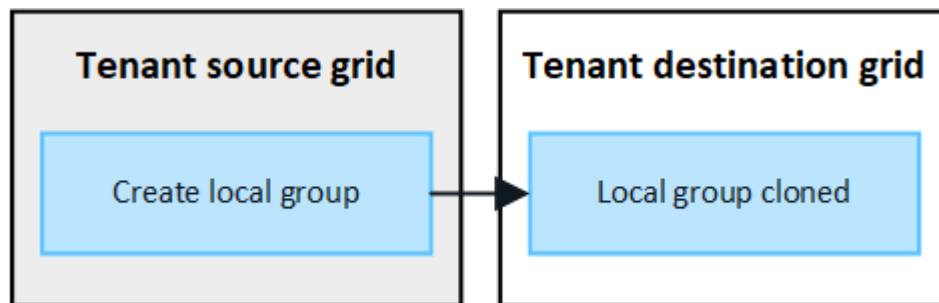
¿Cómo se clonan los grupos, los usuarios y las claves de acceso de S3?

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

Los grupos locales creados en la cuadrícula de origen se clonan

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

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

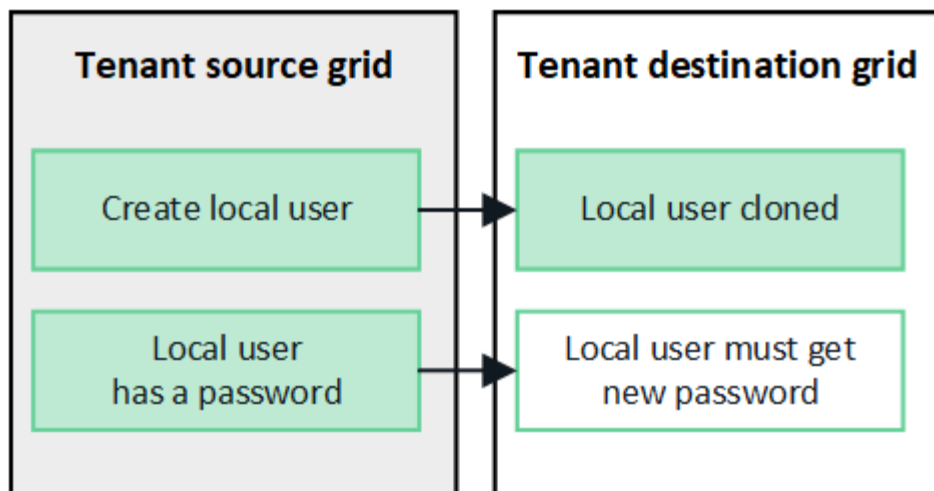


Los usuarios que seleccione al crear un grupo local en la cuadrícula de origen no se incluyen cuando el grupo se clona en la cuadrícula de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Los usuarios locales creados en la cuadrícula de origen se clonan

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

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

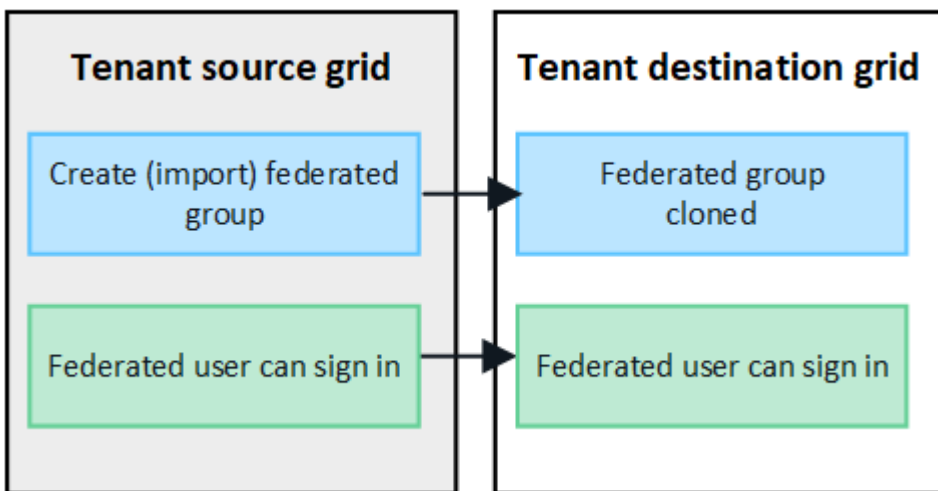


Los grupos federados creados en la cuadrícula de origen se clonan

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

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

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

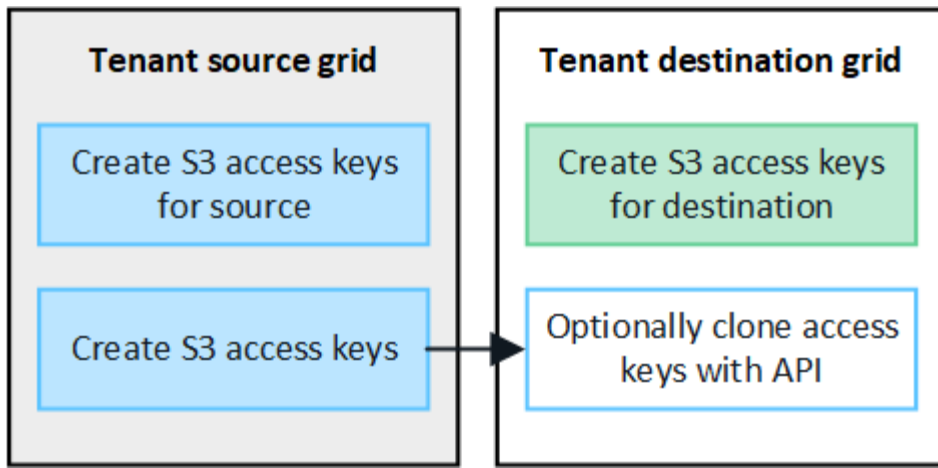


Las claves de acceso S3 se pueden clonar manualmente

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

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

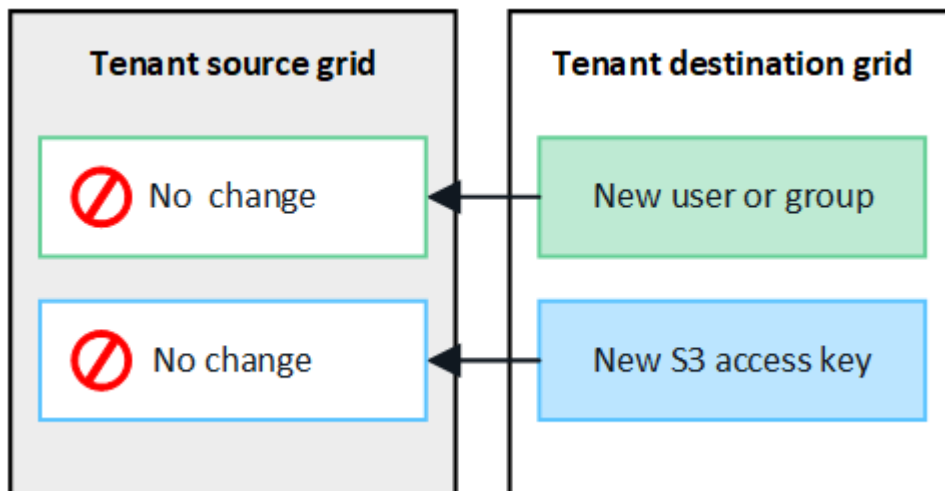
- Si no necesita utilizar las mismas claves para cada cuadrícula, puede hacerlo "cree sus propias claves de acceso" o. "crear claves de acceso de otro usuario" en cada cuadrícula.
- Si necesita utilizar las mismas claves en ambas cuadrículas, puede crear claves en la cuadrícula de origen y, a continuación,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



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

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

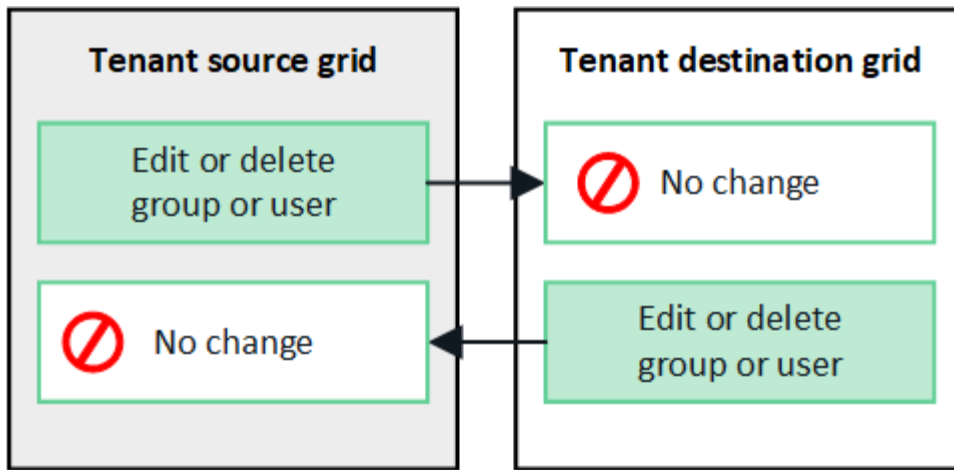
La clonación solo se produce desde la cuadrícula de origen del inquilino al grid de destino del inquilino. Si crea o importa grupos y usuarios en la cuadrícula de destino del inquilino, StorageGRID no clonará estos elementos de vuelta a la cuadrícula de origen del inquilino.



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

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

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



Clone las claves de acceso S3 mediante la API

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

Antes de empezar

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



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

Clone sus propias claves de acceso

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

Pasos

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

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

POST

`/org/users/current-user/replicate-s3-access-key` Clone the current user's S3 key to the other grids.



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.



The screenshot shows a REST client interface with a green header bar. On the left, the word "body" is followed by a red asterisk and the word "required". Below it, "(body)" is written. To the right of the header bar are two tabs: "Edit Value" and "Model". The "Model" tab is selected, and it displays a JSON object with three key-value pairs: "accessKey" with a long alphanumeric string, "secretAccessKey" with another long alphanumeric string, and "expires" with an ISO 8601 timestamp.

```
{
  "accessKey": "AKIAIOSFODNN7EXAMPLE",
  "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
  "expires": "2028-09-04T00:00:00.000Z"
}
```

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

Clonar las claves de acceso de otro usuario

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

Pasos

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

```
GET /org/users
```

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

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



The screenshot shows a REST client interface with a green header bar. On the left, the word "POST" is written in white on a green background. To the right of the header bar is the URL "/org/users/{userId}/replicate-s3-access-key". To the right of the URL is the text "Clone an S3 key to the other grids." followed by a lock icon.

5. Seleccione **probar**.

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

Asegúrese de conservar las comillas dobles alrededor de la cadena.

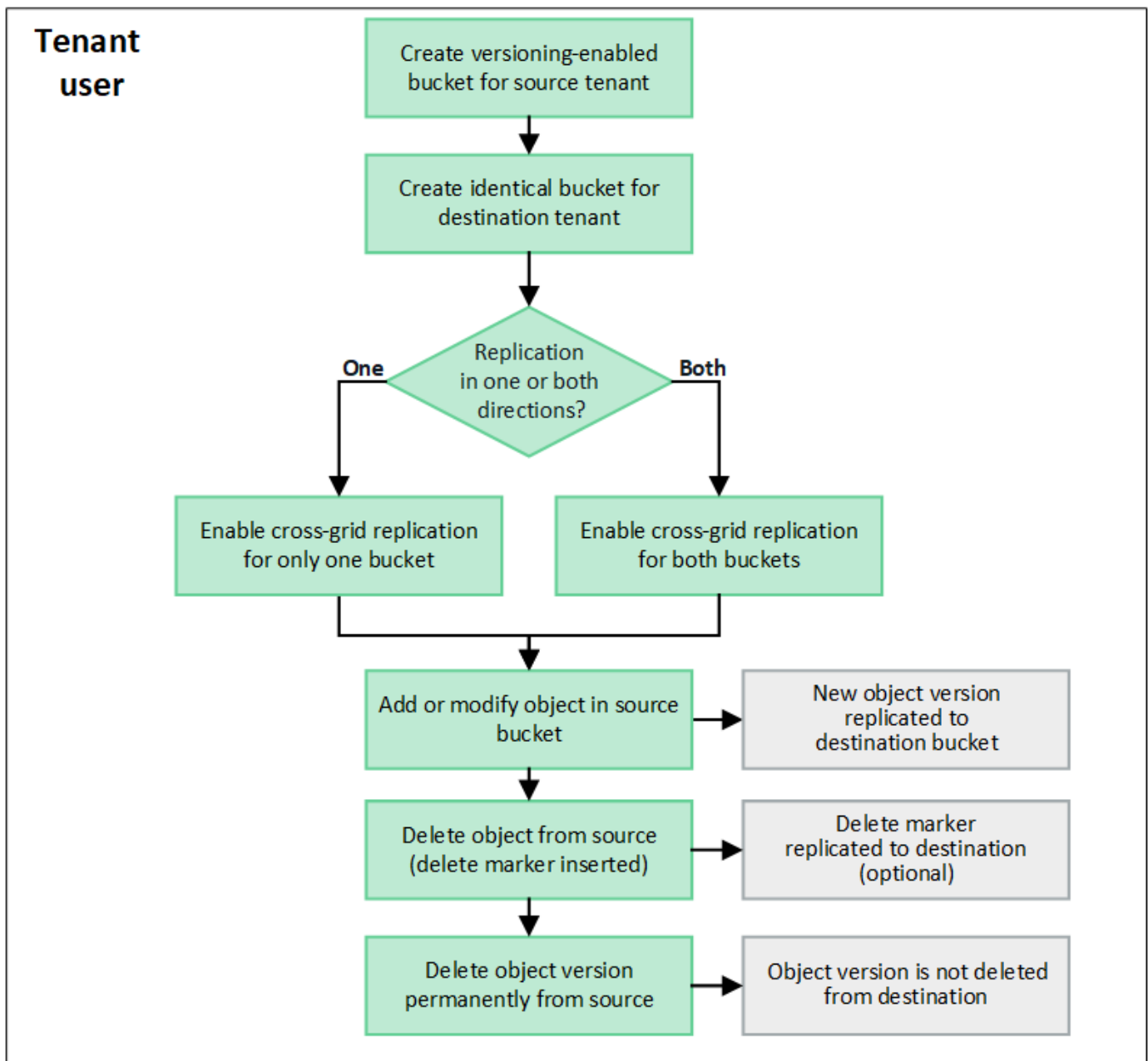
8. Si la clave caduca, reemplace la entrada de ejemplo para **Expires** con la fecha y hora de vencimiento como una cadena en formato de datos-tiempo ISO 8601 (por ejemplo, `2023-02-28T22:46:33-08:00`). Si la clave no caduca, introduzca **null** como valor para la entrada **Expires** (o elimine la línea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

Gestionar la replicación entre grid

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

Flujo de trabajo de replicación entre grid

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



Configurar la replicación entre grid

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

Antes de empezar

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

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

Cree dos cubos idénticos

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

Pasos

1. A partir de cualquier cuadrícula de la conexión de federación de grid, cree un nuevo bucket:

- a. Inicie sesión en la cuenta de inquilino con las credenciales de un usuario de inquilino que existe en ambas cuadrículas.



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

- b. Siga las instrucciones a. "[Cree un bucket de S3](#)".

- c. En la pestaña **Administrar configuración de objetos**, seleccione **Activar control de versiones de objetos**.

- d. Si el bloqueo de objetos S3 está activado para el sistema StorageGRID, no habilite el bloqueo de objetos S3 para el depósito.

- e. Seleccione **Crear cucharón**.

- f. Seleccione **Finalizar**.

2. Repita estos pasos para crear un depósito idéntico para la misma cuenta de inquilino en el otro grid de la conexión de federación de grid.

Habilite la replicación entre grid

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

Pasos

1. A partir de una cuadrícula cuyos objetos desea replicar, active "[replicación entre grid en una dirección](#)":

- a. Inicie sesión en la cuenta de inquilino del bloque.

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

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

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

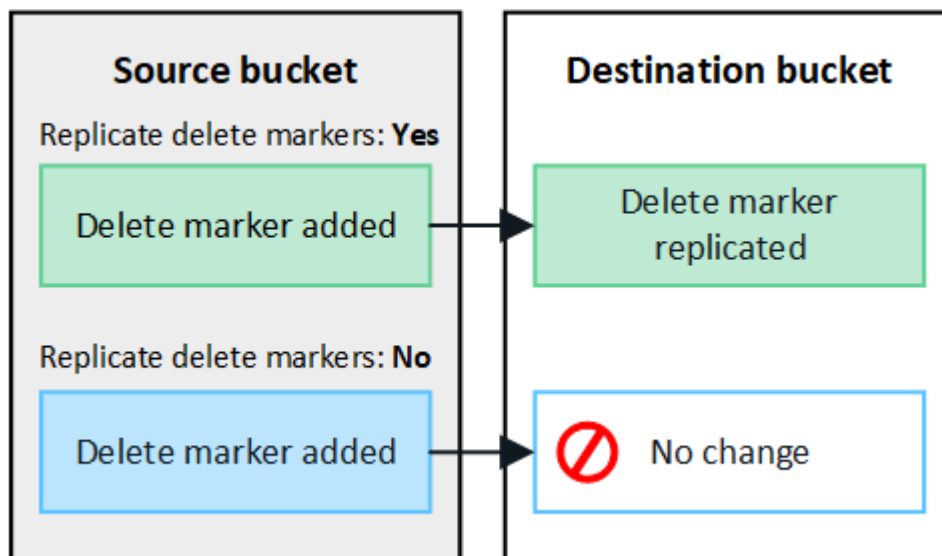
- e. Seleccione **Activar** y revise la lista de requisitos.

- f. Si se han cumplido todos los requisitos, seleccione la conexión de federación de grid que desea utilizar.

- g. Opcionalmente, cambie la configuración de **replicar marcadores de eliminación** para determinar qué sucede en la cuadrícula de destino si un cliente S3 emite una solicitud de eliminación a la cuadrícula de origen que no incluye un ID de versión:

- Si **Sí** (predeterminado), se agrega un marcador de borrado al depósito de origen y se replica en el depósito de destino.

- Si **No**, se agrega un marcador de borrado 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 de objeto se elimina permanentemente del depósito de origen. StorageGRID no replica las solicitudes de eliminación que incluyen un identificador de versión, por lo que la misma versión de objeto no se elimina del destino.

Consulte ["Qué es la replicación entre grid"](#) para obtener más detalles.

- Revise las selecciones. No puede cambiar esta configuración a menos que ambos cubos estén vacíos.
- Seleccione **Habilitar y probar**.

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

- Opcionalmente, vaya al cucharón correspondiente en la otra cuadrícula y. ["permita la replicación entre grid en ambas direcciones"](#).

Probar la replicación entre grids

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

Antes de empezar

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

Pasos

- Inicie sesión en la cuenta de inquilino del bloque.
- Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Buckets**.
- Seleccione el nombre del cubo de la tabla para acceder a la página de detalles del cubo.

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

5. Seleccione **probar conexión**.

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

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

Desactive la replicación entre grid

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

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

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



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

Antes de empezar

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

Pasos

1. A partir de la cuadrícula cuyos objetos ya no desea replicar, detenga la replicación entre grid del bloque:
 - a. Inicie sesión en la cuenta de inquilino del bloque.
 - b. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Buckets**.
 - c. Seleccione el nombre del cubo de la tabla para acceder a la página de detalles del cubo.
 - d. Seleccione la pestaña **Replicación de cuadrícula**.
 - e. Seleccione **Desactivar replicación**.
 - f. Si está seguro de que desea deshabilitar la replicación entre redes para este depósito, escriba **Sí** en el cuadro de texto y seleccione **Desactivar**.

Después de unos momentos, aparece un mensaje de éxito. Los nuevos objetos agregados a este

depósito ya no se pueden replicar automáticamente en el otro grid. **La replicación entre redes** ya no se muestra como una característica habilitada en la página Buckets.

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

Ver conexiones de federación de grid

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

Antes de empezar

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

Pasos

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

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

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

2. Si lo desea, seleccione un nombre de cubo a. ["ver detalles del período"](#).

Borrar el último error

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

- No se ha encontrado la versión del objeto de origen.
- No se ha encontrado el depósito de origen.
- Se ha suprimido el depósito de destino.
- Una cuenta diferente ha vuelto a crear el bloque de destino.
- Se ha suspendido el control de versiones del bloque de destino.
- La misma cuenta ha vuelto a crear el depósito de destino, pero ahora no tiene versiones.

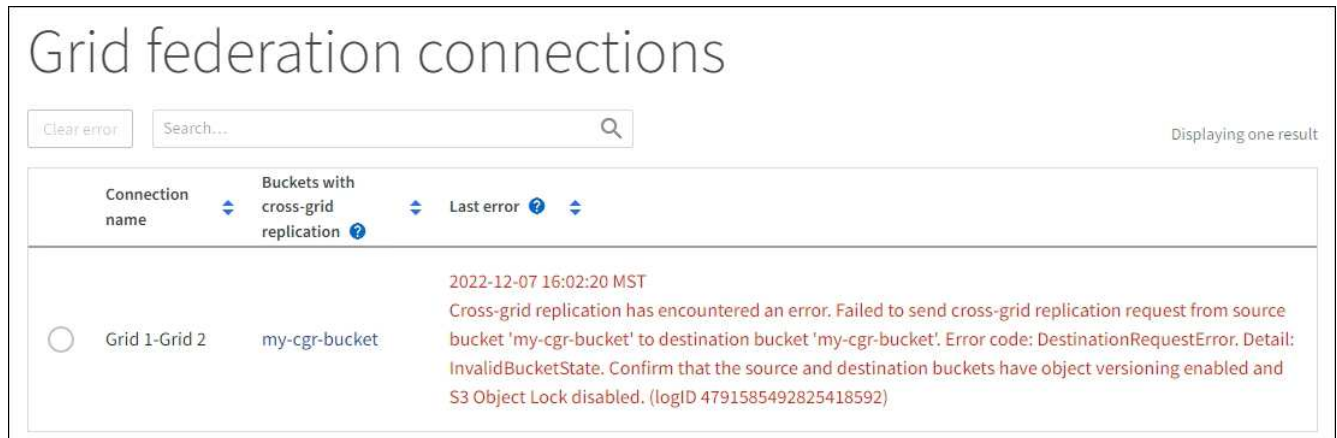


Esta columna solo muestra el último error de replicación entre cuadrículas que se produce; no se mostrarán los errores anteriores que podrían haberse producido.

Pasos

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

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



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



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

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

Gestionar grupos y usuarios

Usar la federación de identidades

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

Configurar la federación de identidades para el Administrador de inquilinos

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

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un ["navegador web compatible"](#).

- Pertenece a un grupo de usuarios que tiene el "[Permiso de acceso raíz](#)".
- Se utiliza Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidades.



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

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

Acerca de esta tarea

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



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

Introducir configuración

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

Pasos

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

Ldap service type

Select the type of LDAP service you want to configure.

| | | | |
|------------------|-------|----------|-------|
| Active Directory | Azure | OpenLDAP | Other |
|------------------|-------|----------|-------|

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

4. Si ha seleccionado **otros**, complete los campos de la sección atributos LDAP . De lo contrario, vaya al paso siguiente.
 - **Nombre único de usuario:** Nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `uid` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `uid`.

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

5. Para todos los tipos de servicio LDAP, introduzca la información de servidor LDAP y conexión de red necesaria en la sección Configure LDAP Server.

- **Hostname:** El nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
- **Puerto:** El puerto utilizado para conectarse al servidor LDAP.



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

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

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

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

- `sAMAccountName` o. `uid`
- `objectGUID`, `entryUUID`, o. `nsuniqueid`
- `cn`
- `memberOf` o. `isMemberOf`
- **Active Directory:** `objectSid`, `primaryGroupID`, `userAccountControl`, y. `userPrincipalName`
- **Azure:** `accountEnabled` y. `userPrincipalName`
- **Contraseña:** La contraseña asociada al nombre de usuario.
- **DN base de grupo:** La ruta completa del nombre distinguido (DN) para un subárbol LDAP que desea buscar grupos. En el ejemplo de Active Directory (a continuación), se pueden usar como grupos federados todos los grupos cuyo nombre distintivo sea relativo al DN base (`DC=storagegrid,DC=example,DC=com`).



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

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



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

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

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

Introduzca uno de estos patrones:

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

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

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



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

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

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

Pruebe la conexión y guarde la configuración

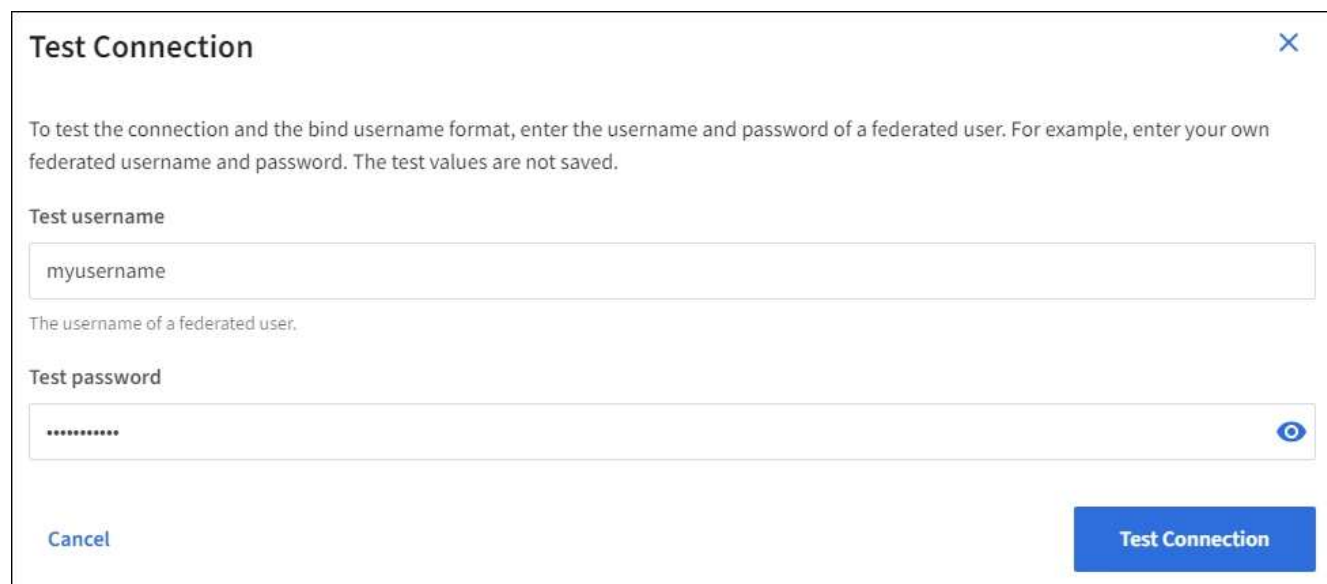
Después de introducir todos los valores, es necesario probar la conexión para poder guardar la configuración. StorageGRID verifica la configuración de conexión del servidor LDAP y el formato de nombre de usuario de enlace, si proporcionó uno.

Pasos

1. Seleccione **probar conexión**.

2. Si no se proporciona un formato de nombre de usuario de enlace:
 - Aparecerá el mensaje «"probar conexión correcta"» si los ajustes de conexión son válidos. Seleccione **Guardar** para guardar la configuración.
 - Aparece el mensaje «"no se ha podido establecer la conexión de prueba"» si los ajustes de conexión no son válidos. 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 /.



- Aparecerá el mensaje «"probar conexión correcta"» si los ajustes de conexión son válidos. Seleccione **Guardar** para guardar la configuración.
- Aparecerá un mensaje de error si las opciones de conexión, el formato de nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva los problemas y vuelva a probar la conexión.

Forzar la sincronización con el origen de identidades

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

Pasos

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

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



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

Deshabilitar la federación de identidades

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

Acercas de esta tarea

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

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

Pasos

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

Instrucciones para configurar el servidor OpenLDAP

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



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

Revestimientos memberOf y ref

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

Indización

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

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

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

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

Gestionar grupos de inquilinos

Cree grupos para un inquilino de S3

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

Antes de empezar

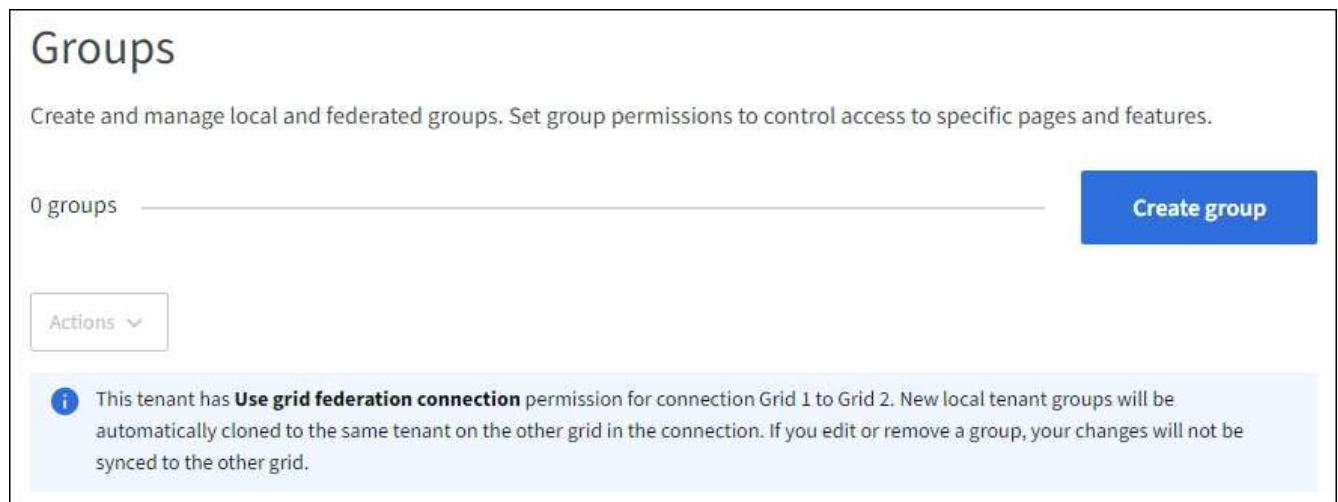
- Ha iniciado sesión en el administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Permiso de acceso raíz"](#).
- Si planea importar un grupo federado, tiene ["federación de identidades configurada"](#), y el grupo federado ya existe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

Acceda al asistente Crear grupo

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

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > grupos**.
2. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, confirme que aparece un banner azul, indicando que los nuevos grupos creados en esta cuadrícula se clonarán en el mismo inquilino en la otra cuadrícula de la conexión. Si este banner no aparece, puede que haya iniciado sesión en la cuadrícula de destino del inquilino.



3. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

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

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

2. Introduzca el nombre del grupo.

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



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

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

3. Seleccione **continuar**.

Administrar permisos de grupo

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

Pasos

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



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

2. Seleccione uno o más permisos para este grupo.

Consulte "[Permisos de gestión de inquilinos](#)".

3. Seleccione **continuar**.

Establezca la política de grupo S3

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

Pasos

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

| Política de grupo | Descripción |
|---------------------------|---|
| Sin acceso S3 | Predeterminado. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que el acceso se conceda con una política de bloque. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3. |
| Acceso de sólo lectura | Los usuarios de este grupo tienen acceso de solo lectura a los recursos de S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puede editar esta cadena. |
| Acceso total | Los usuarios de este grupo tienen acceso completo a recursos de S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena. |
| Mitigación del ransomware | <p>Esta política de ejemplo se aplica a todos los depósitos de este arrendatario. 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.</p> <p>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.</p> |
| Personalizado | A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto. |

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

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

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

Añadir usuarios (sólo grupos locales)

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



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

Pasos

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

El grupo creado aparece en la lista de grupos.

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

Cree grupos para un inquilino de Swift

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



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

Antes de empezar

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

Acceda al asistente Crear grupo

Pasos

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

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

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

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

Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las

aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

2. Introduzca el nombre del grupo.

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

3. Seleccione **continuar**.

Administrar permisos de grupo

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

Pasos

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

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



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

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

3. Seleccione **continuar**.

Configure la política de grupo de Swift

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

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

Añadir usuarios (sólo grupos locales)

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

Pasos

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

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

Consulte "[Gestionar usuarios locales](#)".

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

El grupo creado aparece en la lista de grupos.

Permisos de gestión de inquilinos

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

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

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

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



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

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

| Permiso | Descripción |
|---|---|
| Acceso raíz | Proporciona acceso completo al administrador de inquilinos y a la API de gestión de inquilinos. Nota: Los usuarios de Swift deben tener permiso de acceso root para iniciar sesión en la cuenta del inquilino. |
| Administrador | Solo para inquilinos Swift. Proporciona acceso completo a los contenedores y objetos de Swift para esta cuenta de inquilino Nota: los usuarios de Swift deben tener el permiso de Administrador de Swift para realizar cualquier operación con la API de REST de Swift. |
| Gestione sus propias credenciales de S3 | Permite a los usuarios crear y eliminar sus propias claves de acceso S3. Los usuarios que no tienen este permiso no ven la opción de menú STORAGE (S3) > My S3 access keys . |

| Permiso | Descripción |
|----------------------------------|--|
| Gestionar todos los cucharones | <ul style="list-style-type: none"> Inquilinos S3: Permite a los usuarios usar el administrador de inquilinos y la API de gestión de inquilinos para crear y eliminar bloques S3, así como para gestionar la configuración de todos los bloques de S3 de la cuenta del inquilino, independientemente de las políticas de grupo o bloque de S3. <p>Los usuarios que no tienen este permiso no ven la opción de menú Buckets.</p> <ul style="list-style-type: none"> Inquilinos Swift: Permite a los usuarios de Swift controlar el nivel de coherencia de los contenedores Swift mediante la API de gestión de inquilinos. <p>Nota: Solo puede asignar el permiso Administrar todos los cubos a grupos Swift desde la API de administración de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.</p> |
| Gestionar puntos finales | <p>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.</p> <p>Los usuarios que no tienen este permiso no ven la opción de menú Platform services endpoints.</p> |
| Gestionar objetos con S3 Console | <p>Cuando se combina con el permiso Gestionar todos los depósitos, permite a los usuarios acceder a la Consola Experimental S3 desde la página Buckets. Los usuarios que tienen este permiso pero que no tienen el permiso Administrar todos los depósitos pueden navegar directamente a la Consola Experimental S3.</p> |

Gestionar grupos

Puede ver un grupo; editar el nombre, los permisos, las políticas y los usuarios de un grupo; duplicar un grupo; o eliminar un grupo.

Antes de empezar

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


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 **Usar conexión de federación de grid** y está viendo grupos en la cuadrícula de origen del inquilino, un banner azul indica que si edita o elimina un grupo, sus cambios no se sincronizarán con la otra cuadrícula. Consulte ["Clone los usuarios y los grupos de inquilinos"](#).

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

Manage users

You can add users to this group or remove users from this group.

Add users

Remove Users

Search Groups...

Displaying 1 results

| Username | Full Name | Denied |
|----------|------------------|--------|
| User_02 | User_02_Managers | |

b. Selecciona **Añadir usuarios**.

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

Aparece un mensaje de éxito en la parte superior derecha.

8. Para eliminar usuarios locales del grupo:

a. Seleccione la ficha Usuarios.

b. Selecciona **Eliminar usuarios**.

c. Seleccione los usuarios que desea eliminar y seleccione **Eliminar usuarios**.

Aparece un mensaje de éxito en la parte superior derecha.

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

Grupo duplicado

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



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

Pasos

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

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. Seleccione **Acciones > Eliminar grupo** o **Acciones > Eliminar grupos**.

Se muestra un cuadro de diálogo de confirmación.

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

Gestionar usuarios locales

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



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

Antes de empezar

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

Cree un usuario local

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

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

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

Acceda al asistente Crear usuario

Pasos

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

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, un banner azul indica

que esta es la cuadrícula de origen del inquilino. Todos los usuarios locales que cree en esta cuadrícula se clonarán en la otra cuadrícula de la conexión.

Users

View local and federated users. Edit properties and group membership of local users.

1 user

Create user

Actions ▾

i This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New local tenant users will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid.

2. Seleccione **Crear usuario**.

Introduzca las credenciales

Pasos

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

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

2. Seleccione **continuar**.

Asignar a grupos

Pasos

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

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

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

2. Seleccione **Crear usuario**.

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


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

Ver o editar usuario local

Pasos

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

Si la cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y está viendo al usuario en la cuadrícula de origen del inquilino, un banner azul indica que si edita o elimina el usuario, sus cambios no se sincronizarán con la otra cuadrícula.
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. Seleccione **Guardar cambios**.
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
 - Seleccione el nombre de usuario.
 - Seleccione la casilla de verificación para el usuario y seleccione **Acciones > Ver detalles de usuario**.
5. Revise la sección Visión General, que muestra la siguiente información para cada usuario:
 - Nombre completo
 - Nombre de usuario
 - Tipo de usuario
 - Acceso denegado
 - Modo de acceso
 - Pertenencia a grupos
 - Campos adicionales si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo al usuario en la cuadrícula de origen del inquilino:
 - Estado de clonación, ya sea **Success** o **Failure**

- Un banner azul que indica que si edita este usuario, los cambios no se sincronizarán con la otra cuadrícula.
6. Edite la configuración del usuario según sea necesario. Consulte [Crear usuario local](#) para obtener más información acerca de lo que se debe introducir.
 - a. En la sección Descripción general, cambie el nombre completo seleccionando el nombre o el icono de edición .

No puede cambiar el nombre de usuario.

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

Usuario local duplicado

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



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

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > usuarios**.
2. Seleccione la casilla de control para el usuario que desea duplicar.
3. Seleccione **acciones > Duplicar usuario**.
4. Consulte [Crear usuario local](#) para obtener más información acerca de lo que se debe introducir.
5. Seleccione **Crear usuario**.

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. Seleccione **Acciones > Eliminar usuario** o **Acciones > Eliminar usuarios**.

Se muestra un cuadro de diálogo de confirmación.

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

Gestión de claves de acceso de S3

Gestionar claves de acceso S3: Descripción general

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

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

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

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

Cree sus propias claves de acceso S3

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

Antes de empezar

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

Acerca de esta tarea

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

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

- Establezca un tiempo de caducidad para sus llaves para limitar su acceso a un período de tiempo determinado. Establecer un tiempo de caducidad corto puede ayudar a reducir el riesgo si el ID de clave de acceso y la clave de acceso secreta están expuestos accidentalmente. Las claves caducadas se

eliminan automáticamente.

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



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

Pasos

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

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

2. Seleccione **Crear clave**.

3. Debe realizar una de las siguientes acciones:

- Seleccione **no establezca un tiempo de caducidad** para crear una clave que no caducará. (Predeterminado)
- Seleccione **establecer un tiempo de caducidad** y establezca la fecha y la hora de caducidad.



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

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

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

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



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

6. Seleccione **Finalizar**.

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

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

Consulte las claves de acceso de S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede ver una lista de sus claves de acceso S3. Puede ordenar la lista por tiempo de caducidad, de modo que puede determinar qué claves caducarán pronto. Según sea necesario, puedes ["crear](#)

nuevas claves" o. "teclas de eliminación" que ya no utiliza.



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

Antes de empezar

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

Pasos

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

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

Las claves caducadas se eliminan automáticamente.

Elimine sus propias claves de acceso de S3

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

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un ["navegador web compatible"](#).
- Tiene el permiso gestionar sus propias credenciales de S3. Consulte ["Permisos de gestión de inquilinos"](#).



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

Pasos

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

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

Cree las claves de acceso S3 de otro usuario

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

Antes de empezar

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

Acerca de esta tarea

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

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

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



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

Pasos

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

Aparece la página de detalles del usuario.

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



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

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

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

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



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

7. Seleccione **Finalizar**.

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

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

Ver las claves de acceso S3 de otro usuario

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

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "[navegador web compatible](#)".
- Tiene el permiso 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

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

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un ["navegador web compatible"](#).
- Tiene el permiso acceso raíz. Consulte ["Permisos de gestión de inquilinos"](#).



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 administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene acceso raíz o Gestionar todos los bloques ["permiso"](#). Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.



Los permisos para establecer o modificar las propiedades de Object Lock de grupos o objetos de S3 pueden ser concedidos por ["política de bloques o política de grupo"](#).

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

Acceda al asistente

Pasos

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

Introduzca los detalles

Pasos

1. Introduzca los detalles del cucharón.

| Campo | Descripción |
|-------------------|---|
| Nombre del bloque | <p>Un nombre para el depósito que cumple con estas reglas:</p> <ul style="list-style-type: none">• Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino).• Debe ser compatible con DNS.• Debe incluir al menos 3 y no más de 63 caracteres.• Cada etiqueta debe comenzar y terminar con una letra minúscula o un número y solo puede utilizar letras minúsculas, números y guiones.• No debe utilizar periodos en solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor. <p>Para obtener más información, consulte "Documentación de Amazon Web Services (AWS) sobre reglas de nomenclatura de bloques".</p> <p>Nota: No puedes cambiar el nombre del cubo después de crear el cubo.</p> |
| Región | <p>La región del cubo.</p> <p>El administrador de StorageGRID gestiona las regiones disponibles. La región de un bloque puede afectar la política de protección de datos aplicada a los objetos. De forma predeterminada, todos los bloques se crean en la <code>us-east-1</code> región.</p> <p>Nota: No puedes cambiar la región después de crear el cubo.</p> |

2. Seleccione **continuar**.

Gestionar la configuración del objeto

Pasos

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

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

2. Si la opción Bloqueo de objetos S3 global está habilitada, habilite opcionalmente Bloqueo de objetos S3

para que el depósito almacene objetos utilizando un modelo WORM.

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



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

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

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

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

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

| Modo de retención predeterminado | Descripción |
|----------------------------------|--|
| Cumplimiento de normativas | <ul style="list-style-type: none">• El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta.• La fecha de retención del objeto se puede aumentar, pero no se puede reducir.• No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha. |
| Gobernanza | <ul style="list-style-type: none">• Usuarios con <code>s3:BypassGovernanceRetention</code> el permiso puede utilizar el <code>x-amz-bypass-governance-retention: true</code> solicitar cabecera para omitir la configuración de retención.• Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha.• Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto. |

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

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

4. Seleccione **Crear cucharón**.

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

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

Ver detalles del período

Puede ver los depósitos en su cuenta de inquilino.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "[navegador web compatible](#)".

Pasos

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

Aparecerá la página Buckets.

2. Revise la información de resumen de cada bloque.

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



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

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

| Columna | Descripción |
|-------------------|---|
| Fecha de creación | La fecha y la hora en la que se creó el bloque. |

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

Aparece la página de detalles bucket. En esta página, puede realizar las siguientes tareas:

- Configure y gestione opciones de bloque, como ["nivel de coherencia"](#), ["últimas actualizaciones de hora de acceso"](#), ["versionado de objetos"](#), ["Bloqueo de objetos de S3"](#) y.. ["retención de cucharón por defecto"](#)
- Configurar el acceso al bloque, por ejemplo ["Uso compartido de recursos de origen cruzado \(CORS\)"](#)
- Gestione ["servicios de plataforma"](#) (si se permite para el inquilino), incluida replicación, notificaciones de eventos e integración de búsqueda
- Habilite y. ["gestionar la replicación entre grid"](#) (Si se permite para el inquilino) replicar los objetos ingeridos en este bucket en otro sistema StorageGRID
- Acceda a ["Consola experimental S3"](#) para gestionar los objetos del depósito
- ["Eliminar todos los objetos de un depósito"](#)
- ["Eliminar un cubo"](#) eso ya está vacío

Cambiar el nivel de coherencia de un bloque

Si está usando un inquilino de S3, puede cambiar el nivel de coherencia de las operaciones realizadas en los objetos en los bloques S3.

Antes de empezar

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

Acerca de esta tarea

Los controles de consistencia proporcionan un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios. En general, debe utilizar el nivel de consistencia de **lectura tras escritura nueva** para sus cucharones.

Si el nivel de consistencia de **lectura tras escritura nueva** no cumple los requisitos de la aplicación cliente, puede cambiar el nivel de consistencia estableciendo el nivel de consistencia de la cuchara o utilizando la `Consistency-Control` encabezado. La `Consistency-Control` el encabezado anula el nivel de consistencia del cucharón.



Cuando se cambia el nivel de consistencia de un cubo, solo se garantiza que los objetos que se ingieren después del cambio alcancen el nivel revisado.

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 **Nivel de consistencia**.
4. Seleccione un nivel de 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**.

Activar o desactivar las actualizaciones de la hora del último acceso

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

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

Antes de empezar

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

Acerca de esta tarea

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

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

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

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



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

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

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

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

| Tipo de solicitud | Comportamiento si la hora del último acceso está desactivada (valor predeterminado) | | Comportamiento si la hora del último acceso está activada | |
|---|---|---|---|---|
| | ¿Hora de último acceso actualizada? | ¿Objeto añadido a la cola de evaluación de ILM? | ¿Hora de último acceso actualizada? | ¿Objeto añadido a la cola de evaluación de ILM? |
| Solicitud para recuperar un objeto, su lista de control de acceso o sus metadatos | No | No | Sí | Sí |
| Solicitud para actualizar los metadatos de un objeto | Sí | Sí | Sí | Sí |
| Solicite copiar un objeto de un bloque a otro | <ul style="list-style-type: none"> • No, para la copia de origen • Sí, para la copia de destino | <ul style="list-style-type: none"> • No, para la copia de origen • Sí, para la copia de destino | <ul style="list-style-type: none"> • Sí, para la copia de origen • Sí, para la copia de destino | <ul style="list-style-type: none"> • Sí, para la copia de origen • Sí, para la copia de destino |
| Solicitud para completar una carga de varias partes | Sí, para el objeto ensamblado | Sí, para el objeto ensamblado | Sí, para el objeto ensamblado | Sí, para el objeto ensamblado |

Pasos

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

Aparece la página de detalles bucket.

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

Cambiar el control de versiones del objeto para un bloque

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

Antes de empezar

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

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 | <p>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.</p> <p>Los objetos que ya estaban en el bloque se versionarán cuando los modifique un usuario.</p> |
| Suspender las versiones | Suspenda el control de versiones de objetos si ya no desea crear nuevas versiones de objetos. Aún puede recuperar cualquier versión de objeto existente. |

5. Seleccione **Guardar cambios**.

Utilice Bloqueo de objetos S3 para retener objetos

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

¿Qué es el bloqueo de objetos de S3?

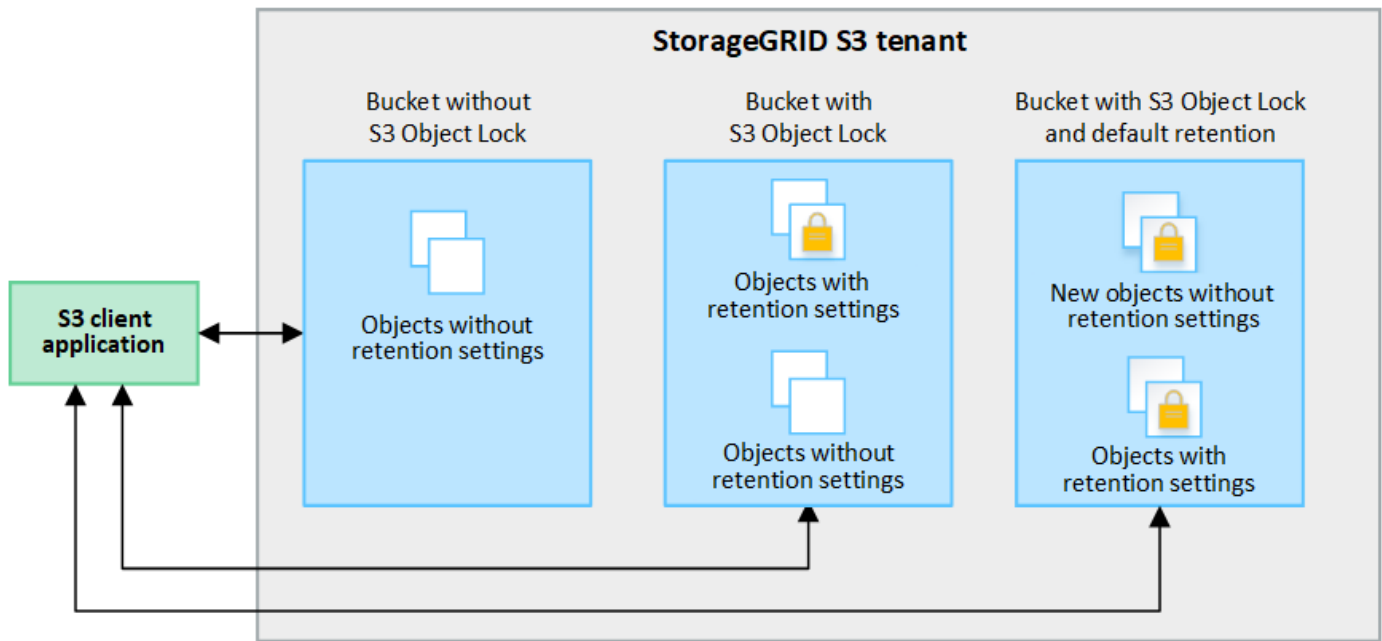
La función StorageGRID S3 Object Lock es una solución de protección de objetos equivalente a S3 Object Lock en Amazon simple Storage Service (Amazon S3).

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

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

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

StorageGRID with S3 Object Lock setting enabled



Modos de retención

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

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

Configuración de retención para versiones de objetos

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

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



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

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

Valor de retención predeterminado para los depósitos

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

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

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

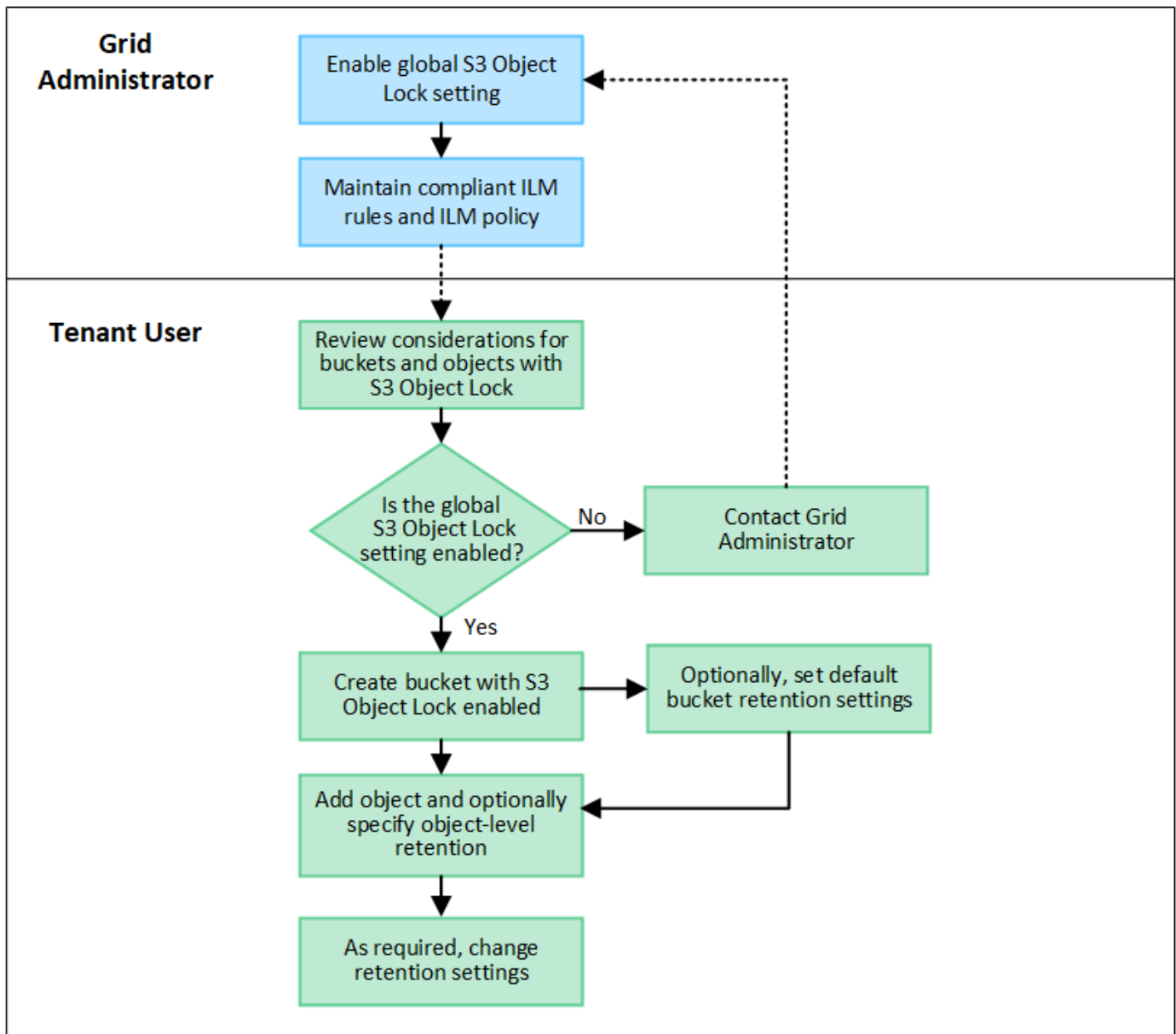
Consulte ["Cree un bloque de S3"](#) y.. ["Actualizar S3 Retención predeterminada de bloqueo de objetos"](#).

Flujo de trabajo de bloqueo de objetos de S3

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

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

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



Requisitos para bloques con bloqueo de objetos de S3 habilitado

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

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

Requisitos para objetos en bloques con S3 Object Lock habilitado

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

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

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

1. Procesamiento de objetos

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

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

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

2. Retención y eliminación de objetos

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

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

¿Puedo seguir gestionando los depósitos compatibles heredados?

La función de bloqueo de objetos S3 sustituye la función Compliance disponible en versiones anteriores de StorageGRID. Si ha creado cubos compatibles con una versión anterior de StorageGRID, puede seguir gestionando la configuración de estos bloques; sin embargo, ya no puede crear nuevos bloques compatibles. Para ver instrucciones, consulte https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5 [Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"].

Actualizar S3 Retención predeterminada de bloqueo de objetos

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

Antes de empezar

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

Pasos

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

Aparece la página de detalles bucket.

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

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

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

| Modo de retención predeterminado | Descripción |
|----------------------------------|--|
| Cumplimiento de normativas | <ul style="list-style-type: none">• El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta.• La fecha de retención del objeto se puede aumentar, pero no se puede reducir.• No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha. |
| Gobernanza | <ul style="list-style-type: none">• Usuarios con <code>s3:BypassGovernanceRetention</code> el permiso puede utilizar el <code>x-amz-bypass-governance-retention: true</code> solicitar cabecera para omitir la configuración de retención.• Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha.• Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto. |

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

para el depósito.

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

7. Seleccione **Guardar cambios**.

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

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

Antes de empezar

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

Acerca de esta tarea

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

Activar CORS para un cucharón

Pasos

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

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

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

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

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

Aparece la página de detalles bucket.

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

Modificar el ajuste de CORS

Pasos

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

Desactive el ajuste CORS

Pasos

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

Suprimir objetos del depósito

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

Consideraciones y requisitos

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

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



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

- Mientras los objetos se eliminan, el estado del depósito es **Eliminando objetos: Solo lectura**. En este estado, no puede agregar nuevos objetos al depósito.
- Cuando todos los objetos se han eliminado, el bloque permanece en su estado de solo lectura. Puede realizar una de las siguientes acciones:
 - Vuelva a colocar el depósito en modo de escritura y reutilícelo para objetos nuevos
 - Elimine el cucharón
 - Mantenga el bucket en modo de solo lectura para reservar su nombre para uso futuro
- Si un depósito tiene activado el control de versiones de objetos, la operación de supresión de objetos no eliminará los marcadores de supresión que estén en el depósito al iniciar estos pasos. Si desea suprimir un depósito con versiones después de suprimir todos los objetos, debe eliminar los marcadores de supresión preexistentes.
- Si utiliza "**replicación entre grid**", tenga en cuenta lo siguiente:
 - El uso de esta opción no elimina ningún objeto del depósito en la otra cuadrícula.
 - Si selecciona esta opción para el depósito de origen, se activará la alerta **Fallo de replicación entre redes** si agrega objetos al depósito de destino en la otra cuadrícula. Si no puede garantizar que nadie agregará objetos al depósito de la otra cuadrícula, "**desactive la replicación entre grid**" para ese depósito antes de eliminar todos los objetos de cubo.

Antes de empezar

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

Pasos

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

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

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

Menú Actions

- Seleccione la casilla de comprobación de cada bloque desde el que desea eliminar objetos.
- Selecciona **Acciones > Eliminar objetos en el cubo**.

Detalles

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

Buckets > my-bucket

my-bucket (read-only)

Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 3

[View bucket contents in Experimental S3 Console](#)

Delete bucket

⚠ All bucket objects are being deleted

StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select **Stop deleting objects**. You cannot restore objects that have already been deleted.

0% (0 of 3 objects deleted)

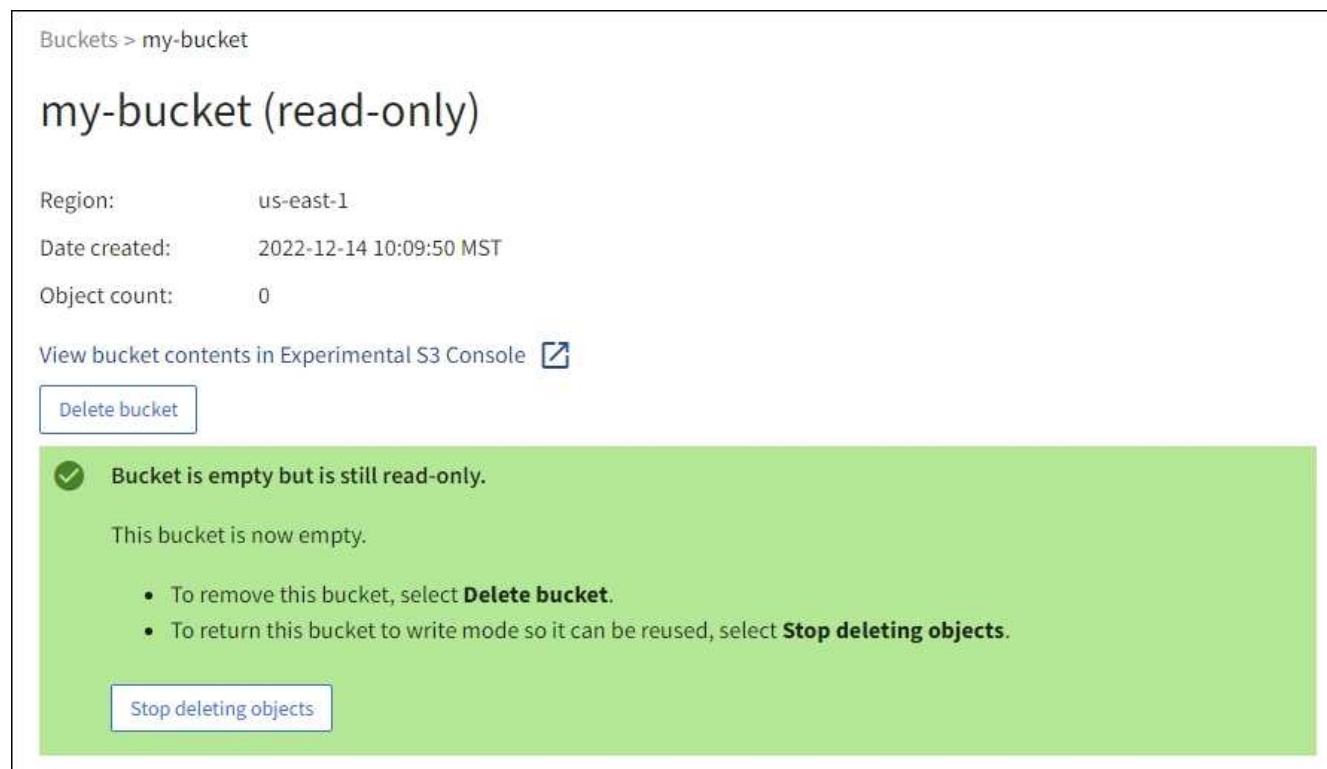
Stop deleting objects

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

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

6. Espere a que se complete la operación.

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



7. Debe realizar una de las siguientes acciones:

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



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

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

Eliminar bloque de S3

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

Antes de empezar

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

- Los cucharones que desea eliminar están vacíos.

Acerca de esta tarea

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

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

Pasos

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

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

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

Menú Actions

- a. Seleccione la casilla de verificación de cada bloque que desee eliminar.
- b. Seleccione **Acciones > Eliminar cubos**.

Detalles

- a. Seleccione un nombre de cubo para mostrar sus detalles.
- b. Seleccione **Eliminar cubo**.

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

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

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

Utilice la consola Experimental S3

Puede usar la consola de S3 para ver los objetos de un bloque de S3.

También puede usar la consola de S3 para hacer lo siguiente:

- Agregar y eliminar objetos, versiones de objetos y carpetas
- Cambie el nombre de los objetos
- Mueva y copie objetos entre bloques y carpetas
- Administrar etiquetas de objetos
- Ver los metadatos de objetos
- Descargar objetos



La consola S3 está marcada como “experimental” porque aún no está completa o aprobada para su uso en un entorno de producción. Los inquilinos solo deben usar S3 Console cuando se realicen funciones para un pequeño número de objetos, como cuando se cargan objetos para simular una nueva política de ILM, solución de problemas de ingesta, o bien mediante grids de prueba de concepto o no de producción.

Antes de empezar


- Ha iniciado sesión en el administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el permiso de acceso root o que tiene tanto los objetos Gestionar todos los buckets como Gestionar con la consola S3 ["permisos"](#).



Los usuarios que tienen el permiso Administrar objetos con S3 Console pero que no tienen el permiso Administrar todos los cubos pueden seguir navegando directamente a la Consola Experimental S3.

- Ha creado un bucket.
- Se ha configurado una política de grupo o bloque S3 para el usuario.
- Conoce el ID de clave de acceso del usuario y la clave de acceso secreta. Opcionalmente, usted tiene un `.csv` archivo que contiene esta información. Consulte ["instrucciones para crear claves de acceso"](#).

Pasos

1. Seleccione **Cuchos**.
2. Seleccione [Experimental S3 Console](#) . También puede acceder a este enlace desde la página de detalles de la cuchara.
3. En la página de inicio de sesión de Experimental S3 Console, pegue el ID de clave de acceso y la clave de acceso secreta en los campos. De lo contrario, seleccione **cargar teclas de acceso** y seleccione el `.csv` archivo.
4. Seleccione **Iniciar sesión**.
5. Gestione los objetos que sea necesario.

StorageGRID Experimental S3 Console
Tenant01

Buckets > bucket-01

↑
📁
bucket-01

Upload
New folder
Refresh
Actions
Search by prefix

| <input type="checkbox"/> | Name | Logical space used | Last modified on |
|--------------------------|--------------------------------|--------------------|-------------------------|
| <input type="checkbox"/> | 03_Grid_Primer_11.5.pdf | 2.73 MB | 2021-12-03 09:43:26 MST |
| <input type="checkbox"/> | 04_Tenant_Users_Guide_11.5.pdf | 1.07 MB | 2021-12-03 09:44:24 MST |
| <input type="checkbox"/> | 06_Tenant_Users_Guide_11.5.pdf | 1.25 MB | 2021-12-03 09:44:27 MST |
| <input type="checkbox"/> | 08_Tenant_Users_Guide_11.5.pdf | 1.25 MB | 2021-12-03 09:44:27 MST |
| <input type="checkbox"/> | 09_Tenant_Users_Guide_11.5.pdf | 1.25 MB | 2021-12-03 09:44:26 MST |
| <input type="checkbox"/> | 10_Grid_Primer_11.5.pdf | 2.8 MB | 2021-12-03 09:43:27 MST |

Select an object or folder to view its details.

Displaying 16 objects
Selected 0 objects

|<
<
Previous
1
Next
>
>|

Gestione servicios de plataformas S3

¿Qué son los servicios de 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.

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

- **Replicación de CloudMirror:** Uso ["Servicio de replicación CloudMirror de StorageGRID"](#) Para reflejar objetos específicos de un bloque de StorageGRID en un destino externo especificado.

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



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

- **Notificaciones:** Uso ["notificaciones de eventos por bloque"](#) Enviar notificaciones sobre acciones

específicas realizadas en objetos a un Amazon Simple Notification Service™ (SNS) externo especificado.

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



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

- **Servicio de integración de búsqueda:** Utilice el "[servicio de integración de búsqueda](#)" Para enviar metadatos de objetos S3 a un índice de Elasticsearch especificado donde se pueden buscar o analizar los metadatos mediante un servicio externo.

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



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

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

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



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

Cómo se configuran los servicios de plataforma

Los servicios de plataforma se comunican con los puntos finales externos que configure mediante "[Administrador de inquilinos](#)" o la "[API de gestión de inquilinos](#)". Cada extremo representa un destino externo, como un bloque de StorageGRID S3, un bloque de Amazon Web Services, un tema de servicio de notificación simple (SNS) o un clúster de Elasticsearch alojado localmente, en AWS u otros lugares.

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

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

- Si desea que todos los objetos con las claves comiencen `/images` Para replicarse en un bloque de Amazon S3, debe añadir una configuración de replicación al bloque de origen.

- Si también desea enviar notificaciones cuando estos objetos están almacenados en el bloque, debe añadir una configuración de notificaciones.
- Por último, si desea indexar los metadatos de estos objetos, debe agregar la configuración de notificación de metadatos que se utiliza para implementar la integración de búsquedas.

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

| Servicio de plataforma | API REST DE S3 |
|------------------------------|---|
| "Replicación de CloudMirror" | <ul style="list-style-type: none"> • OBTENGA la replicación de Bucket • PUT Bucket replication |
| "Notificaciones" | <ul style="list-style-type: none"> • OBTENGA la notificación DE BUCKET • NOTIFICACIÓN DE PUT Bucket |
| "Integración de búsqueda" | <ul style="list-style-type: none"> • OBTENGA la configuración de notificación de metadatos del bloque de datos • PUT bucket metadata notification Configuration <p>Estas operaciones están personalizadas en StorageGRID.</p> |

Información relacionada

["Consideraciones sobre los servicios de plataforma"](#)

["USE LA API DE REST DE S3"](#)

Servicio de replicación de CloudMirror

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

La replicación de CloudMirror opera con independencia de la política de ILM activa de la cuadrícula. El servicio CloudMirror replica los objetos cuando se almacenan en el bloque de origen y los envía al Lo antes posible. de bloque de destino. La entrega de objetos replicados se activa cuando la ingesta de objetos se realiza correctamente.



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

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



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

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

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

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

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



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

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

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

Comprender las notificaciones para bloques

Es posible habilitar la notificación de eventos para un bloque de S3 si desea que StorageGRID envíe notificaciones sobre eventos especificados a un servicio de notificación simple (SNS) de destino.

Puede hacerlo "[configurar las notificaciones de eventos](#)" Asociando XML de configuración de notificación a un bloque de origen. El XML de configuración de notificaciones sigue las convenciones de S3 para configurar las notificaciones de bloques, con el tema SNS de destino especificado como URN de un extremo.

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

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

Notificaciones y mensajes compatibles

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

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

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

Comprender el servicio de integración de búsquedas

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

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

Puede activar el servicio de integración de búsqueda para cualquier bloque con versiones o sin versiones. La

integración de búsqueda se configura asociando el XML de configuración de notificación de metadatos al bloque que especifica los objetos en los que actuar y el destino de los metadatos del objeto.

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



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

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

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

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

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

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

Información relacionada

["XML de configuración para la integración de búsqueda"](#)

["Metadatos de objetos incluidos en las notificaciones de metadatos"](#)

["JSON generado por el servicio de integración de búsqueda"](#)

["Configure el servicio de integración de búsqueda"](#)

Consideraciones sobre los servicios de plataforma

Antes de implementar los servicios de la plataforma, revise las recomendaciones y

consideraciones sobre el uso de estos servicios.

Para obtener más información sobre S3, consulte ["USE LA API DE REST DE S3"](#).

Consideraciones sobre el uso de servicios de plataforma

| Consideración | Detalles |
|--|---|
| Supervisión del extremo de destino | Debe supervisar la disponibilidad de cada extremo de destino. Si se pierde la conectividad con el extremo de destino durante un periodo de tiempo prolongado y existe una gran acumulación de solicitudes, se producirá un error en las solicitudes de cliente adicionales (como solicitudes PUT) a StorageGRID. Debe volver a intentar estas solicitudes con errores cuando se pueda acceder al extremo. |
| Limitación de punto final de destino | <p>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.</p> <p>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.</p> <p>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.</p> |
| Solicitud de garantías | <p>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.</p> <p>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.</p> |
| Eliminaciones de objetos condicionados por ILM | <p>Para coincidir con el comportamiento de eliminación de los servicios de AWS CRR y SNS, 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.</p> <p>Por el contrario, las solicitudes de integración de búsqueda se envían cuando los objetos se eliminan debido a ILM.</p> |

Consideraciones sobre el uso del servicio de replicación de CloudMirror

| Consideración | Detalles |
|---|--|
| Estado de replicación | StorageGRID no admite el <code>x-amz-replication-status</code> encabezado. |
| Tamaño del objeto | <p>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 <i>admitido</i>.</p> <p>Nota: El tamaño máximo <i>recomendado</i> para una operación PUT Object 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.</p> |
| Versiones de bloques e ID de versión | <p>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.</p> <p>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.</p> <p>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.</p> |
| Etiquetado para versiones de objetos | <p>El servicio CloudMirror no replica ninguna solicitud DE etiquetado de objetos PUT ni ELIMINA solicitudes de etiquetado de objetos que proporcionen un ID de versión, debido a las limitaciones en el protocolo S3. Debido a que los ID de versión para el origen y el destino no están relacionados, no hay forma de garantizar que se replique una actualización de etiqueta para un ID de versión específico.</p> <p>Por el contrario, el servicio CloudMirror replica las solicitudes de etiquetado de objetos PUT o ELIMINA las solicitudes de etiquetado de objetos que no especifican un identificador 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).</p> |
| Cargas en varias partes y ETag valores | Cuando se crea un mirroring de objetos cargados con una carga de varias partes, el servicio CloudMirror no conserva las piezas. Como resultado, el ETag el valor del objeto reflejado será diferente al ETag valor del objeto original. |
| Objetos cifrados con SSE-C (cifrado en el lado del servidor con claves proporcionadas por el cliente) | El servicio CloudMirror no admite objetos cifrados con SSE-C. Si intenta procesar un objeto en el bloque de origen para la replicación de CloudMirror y la solicitud incluye los encabezados de solicitud de SSE-C, se produce un error en la operación. |

| Consideración | Detalles |
|--------------------------------------|---|
| Bloque con S3 Object Lock habilitado | Si el bloque de destino S3 para la replicación de CloudMirror tiene la función S3 Object Lock habilitada, el intento de configurar la replicación de bucket (PUT Bucket replication) producirá un error ACCESSDENIED. |

Configure los extremos de servicios de la plataforma

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

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

¿Qué es un extremo de servicios de plataforma?

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

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

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

Puede utilizar el mismo extremo que el destino para más de un bloque de origen. Por ejemplo, se pueden configurar varios bloques de origen para que envíen metadatos de objetos al mismo extremo de integración de búsqueda, de modo que se puedan realizar búsquedas en varios bloques. También es posible configurar un bloque de origen para que use más de un extremo como destino, lo que permite hacer cosas como enviar notificaciones sobre la creación de objetos a un tema de SNS y notificaciones sobre la eliminación de objetos a un segundo tema 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 los extremos del servicio de notificación simple (SNS). No se admiten el servicio de cola simple (SQS) ni los extremos de AWS Lambda.

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 extremo cuando cree XML de configuración para el servicio de plataforma. El URN de cada extremo debe ser único.

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

URN elementos

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

- Si el servicio está alojado en Amazon Web Services (AWS), utilice `arn:aws`.
- Si el servicio está alojado en Google Cloud Platform (GCP), utilice `arn:aws`.
- Si el servicio se aloja localmente, utilice `urn:mystore`

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

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

| Servicio | Tipo |
|----------------------------|------|
| Replicación de CloudMirror | s3 |
| Notificaciones | sns |
| Integración de búsqueda | es |

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

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

| Servicio | Recurso específico |
|----------------------------|--------------------|
| Replicación de CloudMirror | nombre del bloque |

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

Urnas para servicios alojados en AWS y GCP

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

- Replicación de CloudMirror:

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

- Notificaciones:

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

- Integración de búsqueda:

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



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

Servicios alojados localmente

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

- Replicación de CloudMirror:

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

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

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

- Notificaciones:

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

- Integración de búsqueda:

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



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

Cree un extremo de servicios de plataforma

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

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un ["navegador web compatible"](#).
- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Pertenece a un grupo de usuarios que tiene el ["Gestionar puntos finales o permisos de acceso raíz"](#).
- Se ha creado el recurso al que hace referencia el punto final de servicios de plataforma:
 - Replicación de CloudMirror: Bloque de S3
 - Notificación de eventos: Tema SNS
 - 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):
 - Clave de acceso: ID de clave de acceso y clave de acceso secreta
 - Basic HTTP: Nombre de usuario y contraseña
 - CAP (C2S Access Portal): URL de credenciales temporales, certificados de servidor y de cliente,

claves de cliente y una contraseña de clave privada de cliente opcional.

- Certificado de seguridad (si se utiliza un certificado de CA personalizado)
- Si las funciones de seguridad de Elasticsearch están activadas, tiene el privilegio de clúster de supervisión para las pruebas de conectividad y el privilegio WRITE INDEX o los privilegios INDEX y DELETE INDEX para las actualizaciones de documentos.

Pasos

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

Aparece la página de extremos de servicios de plataforma.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

0 endpoints Create endpoint

Delete endpoint

| | Display name ? | Last error ? | Type ? | URI ? | URN ? |
|------------------------------|----------------|--------------|--------|-------|-------|
| No endpoints found | | | | | |
| Create endpoint | | | | | |

2. Seleccione **Crear punto final**.

Create endpoint

1 Enter details

2 Select authentication type
Optional

3 Verify server
Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name ?

URI ?

https://example.com

URN ?

arn:aws:s3::bucket_name

Cancel

Continue

- Introduzca un nombre para mostrar para describir brevemente el extremo y su propósito.

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

- 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, el puerto 443 se utiliza para URI HTTPS y el puerto 80 se utiliza para URI HTTP.

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** y, a continuación, introduzca o cargue las credenciales necesarias.

Create endpoint

✓ Enter details

2 Select authentication type
Optional

3 Verify server
Optional

Authentication type ?

Select the method used to authenticate connections to the endpoint.

Anonymous

Anonymous

Access Key

Basic HTTP

CAP (C2S Access Portal)

Previous

Continue

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. | <ul style="list-style-type: none">• 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. | <ul style="list-style-type: none">• Nombre de usuario• Contraseña |
| CAP (Portal de acceso C2S) | Usa certificados y claves para autenticar las conexiones al destino. | <ul style="list-style-type: none">• 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) |

8. Seleccione **continuar**.

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

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

Información relacionada

["Especifique URN para el extremo de servicios de la plataforma"](#)

["Configure la replicación de CloudMirror"](#)

["Configure las notificaciones de eventos"](#)

["Configure el servicio de integración de búsqueda"](#)

Probar la conexión para el extremo de servicios de la plataforma

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

Antes de empezar

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

Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

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

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

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

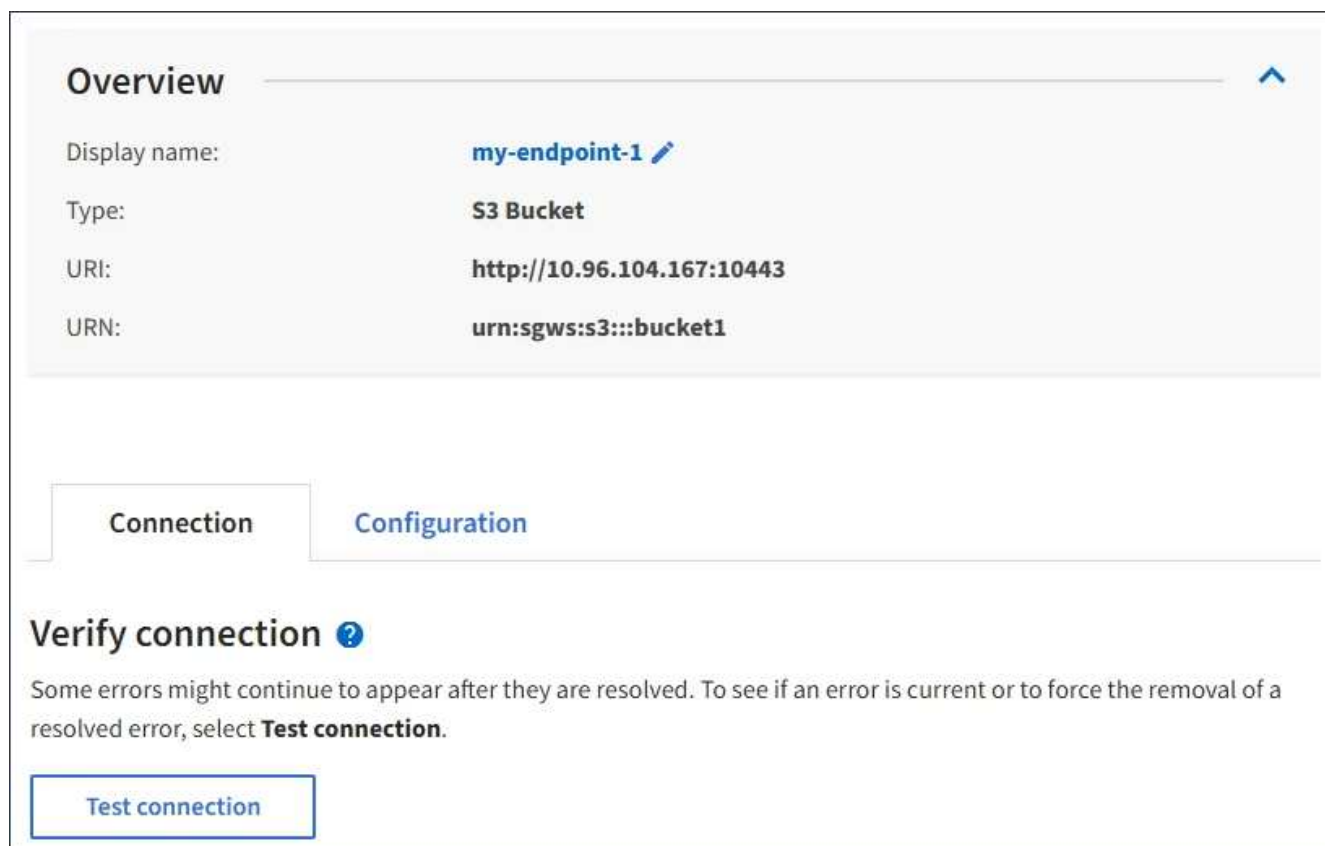
Create endpoint

Delete endpoint

| <input type="checkbox"/> | Display name | Last error | Type | URI | URN |
|--------------------------|---------------|-------------|---------------|----------------------------|-------------------------------------|
| <input type="checkbox"/> | my-endpoint-1 | | S3 Bucket | http://10.96.104.167:10443 | urn:sgws:s3:::bucket1 |
| <input type="checkbox"/> | my-endpoint-2 | 2 hours ago | Search | http://10.96.104.30:9200 | urn:sgws:es:::mydomain/sveloso/_doc |
| <input type="checkbox"/> | my-endpoint-3 | | Notifications | http://10.96.104.202:8080/ | arn:aws:sns:us-west-2::example1 |
| <input type="checkbox"/> | my-endpoint-4 | | S3 Bucket | http://10.96.104.167:10443 | urn:sgws:s3:::bucket2 |

2. Seleccione el extremo cuya conexión desea probar.

Aparece la página de detalles del extremo.



Overview

Display name: **my-endpoint-1**

Type: **S3 Bucket**

URI: **http://10.96.104.167:10443**

URN: **urn:sgws:s3:::bucket1**

Connection **Configuration**

Verify connection ?

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

3. Seleccione **probar conexión**.

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

Editar extremo de servicios de plataforma

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

Antes de empezar

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

Pasos

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

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

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

| <input type="checkbox"/> | Display name | Last error | Type | URI | URN |
|--------------------------|---------------|-------------|---------------|----------------------------|-------------------------------------|
| <input type="checkbox"/> | my-endpoint-1 | | S3 Bucket | http://10.96.104.167:10443 | urn:sgws:s3:::bucket1 |
| <input type="checkbox"/> | my-endpoint-2 | 2 hours ago | Search | http://10.96.104.30:9200 | urn:sgws:es:::mydomain/sveloso/_doc |
| <input type="checkbox"/> | my-endpoint-3 | | Notifications | http://10.96.104.202:8080/ | arn:aws:sns:us-west-2::example1 |
| <input type="checkbox"/> | my-endpoint-4 | | S3 Bucket | http://10.96.104.167:10443 | urn:sgws:s3:::bucket2 |

2. Seleccione el extremo que desea editar.

Aparece la página de detalles del extremo.

3. Seleccione **Configuración**.

Overview

Display name: **my-endpoint-3** 

Type: **Notifications**

URI: **http://10.96.104.202:8080/**

URN: **arn:aws:sns:us-west-2::example1**

Connection

Configuration

Edit configuration

Endpoint details

URI 

http://10.96.104.202:8080/

URN 

arn:aws:sns:us-west-2::example1

Authentication type

Basic HTTP 

Username 

testme

Password 

••••••••

Edit password

Verify server

- ☐ Use custom CA certificate
- ☒ Use operating system CA certificate
- ☐ Do not verify certificate

```
-----BEGIN CERTIFICATE-----  
abcdefghijklmnopqrstuvwxyz1234567890ABCDEFGHIJKL  
123456/7890ABCDEFabcdefghijkLABCD  
-----END CERTIFICATE-----
```

Test and save changes

4. Según sea necesario, cambie la configuración del extremo.



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

a. Para cambiar el nombre para mostrar del extremo, seleccione el icono de edición .

b. Según sea necesario, cambie el URI.

c. Según sea necesario, cambie el tipo de autenticación.

- Para la autenticación de la clave de acceso, cambie la clave según sea necesario seleccionando **Editar clave S3** y pegando un nuevo ID de clave de acceso y una clave de acceso secreta. Si necesita cancelar los cambios, seleccione **Revert S3 key EDIT**.
- Para la autenticación HTTP básica, cambie el nombre de usuario según sea necesario. Cambie la contraseña según sea necesario; para ello, seleccione **Editar contraseña** e introduzca la nueva contraseña. Si necesita cancelar los cambios, seleccione **Revert password EDIT**.
- Para la autenticación CAP (C2S Access Portal), cambie la URL de las credenciales temporales o la frase de contraseña de la clave privada del cliente opcional y cargue nuevos archivos de certificado y claves según sea necesario.



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

d. Según sea necesario, cambie el método para verificar el servidor.

5. Seleccione **probar y guardar los cambios**.

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

Eliminar extremo de servicios de plataforma

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

Antes de empezar

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

Pasos

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

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

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

| <input type="checkbox"/> | Display name ? | Last error ? | Type ? | URI ? | URN ? |
|--------------------------|----------------|---------------|---------------|----------------------------|-------------------------------------|
| <input type="checkbox"/> | my-endpoint-1 | | S3 Bucket | http://10.96.104.167:10443 | urn:sgws:s3:::bucket1 |
| <input type="checkbox"/> | my-endpoint-2 | ✖ 2 hours ago | Search | http://10.96.104.30:9200 | urn:sgws:es:::mydomain/sveloso/_doc |
| <input type="checkbox"/> | my-endpoint-3 | | Notifications | http://10.96.104.202:8080/ | arn:aws:sns:us-west-2::example1 |
| <input type="checkbox"/> | my-endpoint-4 | | S3 Bucket | http://10.96.104.167:10443 | urn:sgws:s3:::bucket2 |

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.

Delete endpoint



Are you sure you want to delete endpoint my-endpoint-10?

This might take a few minutes.

When you delete an endpoint, you can no longer use it to access external resources.

Cancel

Delete endpoint


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.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

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

Pasos

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

Overview

Display name:

my-endpoint-2

Type:

Search

URI:

http://10.96.104.30:9200

URN:

urn:sgws:es:::mydomain/sveloso/_doc

Connection

Configuration

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

Last error details

✖

2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

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 "es necesario actualizar las credenciales del punto final o el acceso al destino" 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 Prohibido"), compruebe los permisos asociados con las credenciales del punto final.

Información relacionada

- [Administrar los servicios de plataforma de StorageGRID](#) > [Solucionar problemas](#)
- ["Cree un extremo de servicios de plataforma"](#)
- ["Probar la conexión para el extremo de servicios de la plataforma"](#)
- ["Editar extremo de servicios de plataforma"](#)

Configure la replicación de CloudMirror

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

Antes de empezar

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

Acerca de esta tarea

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



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

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



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

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

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

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

Pasos

1. Habilite la replicación para su bloque de origen:

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

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

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

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

Aparece la página de detalles bucket.

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

Bucket options

Bucket access

Platform services

Replication

Disabled

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

☒ Enable replication

Clear

```

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

```

Save changes



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:

- 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".

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

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

Información relacionada

["Cree un extremo de servicios de plataforma"](#)

Configure las notificaciones de eventos

El servicio de notificaciones es uno de los tres servicios de la plataforma StorageGRID. Puede habilitar las notificaciones de un bloque para enviar información acerca de los eventos especificados a un servicio de destino que admita AWS simple Notification Service™ (SNS).

Antes de empezar

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

Acerca de esta tarea

Después de configurar las notificaciones de eventos, cada vez que se produce un evento especificado para un objeto del bloque de origen, se genera una notificación y se envía al tema Servicio de notificación simple (SNS) que se utiliza como extremo de destino. Para habilitar las notificaciones para un bloque, debe crear y aplicar un XML de configuración de notificación válido. El XML de configuración de notificaciones debe usar el URN de un extremo de notificaciones de eventos para cada destino.

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

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

Pasos

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


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

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3) > Cuchos**.

3. Seleccione el nombre del bloque de origen.

Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma > Notificaciones de eventos**.

5. Seleccione la casilla de verificación **Habilitar notificaciones de eventos**.

6. Pegue el XML de configuración de notificación en el cuadro de texto y seleccione **Guardar cambios**.

Bucket options

Bucket access

Platform services

Replication

Disabled

▼

Event notifications

Disabled

▲

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS).

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

☒ Enable event notifications

Clear

```

<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>
  </TopicConfiguration>
</NotificationConfiguration>

```

Save changes



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:

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

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

- b. Confirme que se ha entregado una notificación al tema SNS de destino.

Por ejemplo, si el tema de destino está alojado en el servicio de notificación simple (SNS) de AWS, puede configurar el servicio para que le envíe un correo electrónico cuando se entrega la notificación.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}
```

Si se recibe la notificación en el tema de destino, ha configurado correctamente el bloque de origen para

las notificaciones StorageGRID.

Información relacionada

["Comprender las notificaciones para bloques"](#)

["USE LA API DE REST DE S3"](#)

["Cree un extremo de servicios de plataforma"](#)

Utilice el servicio de integración de búsqueda

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

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



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

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

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

Información relacionada

["XML de configuración para la integración de búsqueda"](#)

["Metadatos de objetos incluidos en las notificaciones de metadatos"](#)

["JSON generado por el servicio de integración de búsqueda"](#)

["Configure el servicio de integración de búsqueda"](#)

["USE LA API DE REST DE S3"](#)

XML de configuración para la integración de búsqueda

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

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, puede enviar metadatos de

los objetos con el prefijo `images` en un destino y los metadatos de los objetos con el prefijo `videos` a otro. Las configuraciones que tienen prefijos superpuestos no son válidas y se rechazan cuando se envían. Por ejemplo, una configuración que incluye una regla para objetos con el prefijo `test` y una segunda regla para los objetos con el prefijo `test2` no está permitido.

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

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

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

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

| Nombre | Descripción | Obligatorio |
|---------|---|-------------|
| Estado | <p>El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas.</p> <p>Incluido en el elemento Regla.</p> | Sí |
| Prefijo | <p>Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado.</p> <p>Para hacer coincidir todos los objetos, especifique un prefijo vacío.</p> <p>Incluido en el elemento Regla.</p> | Sí |
| Destino | <p>Etiqueta de contenedor para el destino de una regla.</p> <p>Incluido en el elemento Regla.</p> | Sí |
| No | <p>URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades:</p> <ul style="list-style-type: none"> • es debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en el formulario <code>domain-name/myindex/mytype</code>. <p>Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mystore:es:::mydomain/myindex/mytype</code> <p>El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404.</p> <p>EL VALOR DE URN se incluye en el elemento Destination.</p> | Sí |

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

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

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

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:myes:es::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Configuración de notificaciones de metadatos con dos reglas

En este ejemplo, metadatos de objeto para objetos que coinciden con el prefijo `/images` se envía a un destino, mientras que los metadatos de objetos de los objetos que coinciden con el prefijo `/videos` se envía a un segundo destino.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Información relacionada

["USE LA API DE REST DE S3"](#)

["Metadatos de objetos incluidos en las notificaciones de metadatos"](#)

["JSON generado por el servicio de integración de búsqueda"](#)

["Configure el servicio de integración de búsqueda"](#)

Configure el servicio de integración de búsqueda

El servicio de integración de búsqueda envía metadatos de objetos a un índice de búsqueda de destino cada vez que se crea, se elimina o se actualizan sus metadatos o etiquetas.

Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket S3 cuyo contenido desea indexar.
- El punto final que pretende utilizar como destino para el servicio de integración de búsqueda ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el "[Gestione todos los bloques o permisos de acceso raíz](#)". Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar el servicio de integración de búsqueda para un bloque de origen, al crear un objeto o actualizar los metadatos o las etiquetas de un objeto se activan los metadatos de objeto que se enviarán al extremo de destino. Si habilita el servicio de integración de búsqueda para un depósito que ya contiene objetos, las notificaciones de metadatos no se envían automáticamente para los objetos existentes. Debe actualizar estos objetos existentes para asegurarse de que sus metadatos se agregan al índice de búsqueda de destino.

Pasos

1. Utilice un editor de texto para crear el XML de notificación de metadatos necesario para habilitar la integración de búsqueda.
 - Consulte la información sobre XML de configuración para la integración de búsquedas.
 - Al configurar XML, utilice URN de un extremo de integración de búsqueda como destino.

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:1111111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

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

Aparece la página de detalles bucket.
4. Seleccione **Servicios de plataforma > integración de búsqueda**
5. Seleccione la casilla de verificación **Habilitar integración de búsqueda**.

6. Pegue la configuración de notificación de metadatos en el cuadro de texto y seleccione **Guardar cambios**.

Platform services

Replication Disabled

Event notifications Disabled

Search integration Disabled

Enable the search integration service to send object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the search integration service.
- You must specify the URN of that endpoint in the search integration configuration XML for the bucket you want to index.

☒ Enable search integration

Clear

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Save changes



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

7. Compruebe que el servicio de integración de búsqueda está configurado correctamente:

- a. Añada un objeto al bloque de origen que cumpla los requisitos para activar una notificación de metadatos tal y como se especifica en el XML de configuración.

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

- b. Confirme que se ha agregado un documento JSON que contiene los metadatos y las etiquetas del objeto al índice de búsqueda especificado en el extremo.

Después de terminar

Según sea necesario, se puede deshabilitar la integración de búsqueda para un bloque con cualquiera de los siguientes métodos:

- Seleccione **STORAGE (S3) > Buckets** y desactive la casilla de verificación **Enable search integration**.
- Si utiliza la API de S3 directamente, utilice una solicitud de notificación DELETE Bucket. Consulte las instrucciones para implementar aplicaciones cliente de S3.

Información relacionada

["Comprender el servicio de integración de búsquedas"](#)

["XML de configuración para la integración de búsqueda"](#)

["USE LA API DE REST DE S3"](#)

["Cree un extremo de servicios de plataforma"](#)

JSON generado por el servicio de integración de búsqueda

Al habilitar el servicio de integración de búsqueda para un bloque, se genera un documento JSON y se envía al extremo de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas del objeto.

Este ejemplo muestra un ejemplo de JSON que se podría generar cuando un objeto con la clave SGWS/Tagging.txt se crea en un bloque llamado test. La test el bloque no tiene versiones, por lo que el versionId la etiqueta está vacía.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadatos de objetos incluidos en las notificaciones de metadatos

En la tabla se enumeran todos los campos que se incluyen en el documento JSON que se envían al extremo de destino cuando la integración de búsqueda está habilitada.

El nombre del documento incluye el nombre del bloque, el nombre del objeto y el ID de versión, si existe.

| Tipo | Nombre y descripción del artículo |
|---|--|
| Información sobre bloques y objetos | <code>bucket</code> : Nombre del cubo |
| <code>key</code> : Nombre de clave de objeto | <code>versionID</code> : Versión de objeto, para objetos en cubos con versiones |
| <code>region</code> : Región de cucharón, por ejemplo <code>us-east-1</code> | Metadatos del sistema |
| <code>size</code> : Tamaño del objeto (en bytes) visible para un cliente HTTP | <code>md5</code> : Hash de objeto |
| Metadatos del usuario | <code>metadata</code> : Todos los metadatos de usuario del objeto, como pares clave-valor <code>key:value</code> |
| Etiquetas | <code>tags</code> : Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor <code>key:value</code> |



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.

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 S3 y HTTP.

| Elemento | Versión |
|----------------------|--|
| Especificación de S3 | <i>Simple Storage Service referencia de API</i> 2006-03-01 |
| HTTP | 1.1 Para obtener más información acerca de HTTP, vea HTTP/1.1 (RFC 7230-35). Nota: StorageGRID no admite canalización HTTP/1.1. |

Información relacionada

["RFC de IETF 2616: Protocolo de transferencia de hipertexto \(HTTP/1.1\)"](#)

["Documentación de Amazon Web Services \(AWS\): Referencia de API de Amazon simple Storage Service"](#)

Actualizaciones del soporte de la API de REST DE S3

| Liberar | Comentarios |
|---------|--|
| 11.7 | <ul style="list-style-type: none">• Añadido "Referencia rápida: Solicitudes de API de S3 admitidas".• Se ha añadido soporte para el uso del modo de GOBIERNO con S3 Object Lock.• Se añadió compatibilidad con productos específicos de StorageGRID <code>x-ntap-sg-cgr-replication-status</code> Cabecera de respuesta para las solicitudes de objetos GET y HEAD. Este encabezado proporciona el estado de replicación de un objeto para la replicación entre grid.• Las solicitudes <code>SelectObjectContent</code> ahora admiten objetos de Parquet. |
| 11.6 | <ul style="list-style-type: none">• Se ha agregado soporte para utilizar <code>partNumber</code> Parámetro de solicitud en GET Object y HEAD Object peticiones.• 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 <code>s3:object-lock-remaining-retention-days</code> clave de condición de política para configurar el rango de períodos de retención permitidos para los objetos.• Se ha cambiado el tamaño máximo de <i>recommended</i> 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. |

| Liberar | Comentarios |
|---------|--|
| 11.5 | <ul style="list-style-type: none"> • 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. • La Content-MD5 el encabezado de la solicitud ahora es correctamente compatible. |
| 11.4 | <ul style="list-style-type: none"> • 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 agregado compatibilidad con las notificaciones de bloques en la <code>s3:ObjectRestore:Post</code> 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 |
| 11.3 | <ul style="list-style-type: none"> • 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 compatibilidad para operaciones DE ELIMINACIÓN, GET y PUT Bucket Lifecycle (solo acción de caducidad) y para el <code>x-amz-expiration</code> encabezado 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 | <p>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.</p> <p>Nota: los usos de ARN/URN en otra configuración JSON/XML, incluidos los utilizados en las características personalizadas de StorageGRID, no han cambiado.</p> |
| 11.1 | <p>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.</p> |

| Liberar | Comentarios |
|---------|---|
| 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 añadió compatibilidad con las restricciones de ubicación del etiquetado de objetos para bloques y la configuración de control de 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 DE REST de S3 por parte del sistema StorageGRID. la versión actualmente admitida de <i>simple Storage Service API Reference</i> 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 admite 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 admite todos [parámetros y cabeceras comunes](#) Para esta solicitud, además de este parámetro de consulta URI adicional:

- uploadId

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- CompleteMultipartUpload
- Part
- ETag
- PartNumber

Documentación de StorageGRID

["Completar carga de varias partes"](#)

"CopyObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [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

["PONER Objeto-Copia"](#)

"CreateBucket"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [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 todos [parámetros y cabeceras comunes](#) para esta solicitud, además de estos encabezados adicionales:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- 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

["Inicie la carga de varias partes"](#)

"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 todos [parámetros y cabeceras comunes](#) para esta solicitud, además de esta cabecera 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 todos [parámetros y cabeceras comunes](#) para esta solicitud, además de esta cabecera 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"](#) (ELIMINAR varios 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"](#) (OBTENER ciclo de vida del bloque)
- ["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"](#) (OBTENER notificación de bloque)

"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 admite todos [parámetros y cabeceras comunes](#) Para esta solicitud, además de estos parámetros de consulta URI adicionales:

- 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

["OBTENER objeto"](#)

"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 todos [parámetros y cabeceras comunes](#) para esta solicitud, además de estos encabezados adicionales:

- 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 HEAD"

"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](#) > [OBTENER servicio](#)

"ListCargas multipartitas"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud, además de estos parámetros adicionales:

- delimiter
- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Enumerar cargas de varias partes"](#)

"ListObjects"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud, además de estos parámetros adicionales:

- delimiter
- encoding-type
- marker
- max-keys
- prefix

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#) (OBTENER bloque)

"ListObjectsV2"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para 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"](#) (OBTENER bloque)

"ListObjectVersions"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para 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"](#) (OBTENER versiones de objeto de bloque)

"ListParts"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud, además de estos parámetros adicionales:

- max-parts
- part-number-marker
- uploadId

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Enumerar cargas de varias partes"](#)

"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:

- ServerSideEncryptionConfiguration
- Rule
- ApplyServerSideEncryptionByDefault
- 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:

- NewerNoncurrentVersions
- LifecycleConfiguration
- Rule
- Expiration
- Days
- Filter
- And
- Prefix
- Tag

- Key
- Value
- Prefix
- Tag
- Key
- Value
- ID
- NoncurrentVersionExpiration
- NoncurrentDays
- Prefix
- Status

Documentación de StorageGRID

- ["Operaciones en bloques"](#) (Ciclo de vida de PUT Bucket)
- ["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:

- Prefix
- Suffix
- NotificationConfiguration
- TopicConfiguration
- Event
- Filter
- S3Key
- FilterRule
- Name
- Value
- Id
- Topic

Documentación de StorageGRID

["Operaciones en bloques"](#) (NOTIFICACIÓN PUT Bucket)

"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 del 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

- ReplicationConfiguration
- Status
- Prefix
- Destination
- Bucket
- StorageClass
- Rule

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 todos [parámetros y cabeceras comunes](#) para esta solicitud, además de estos encabezados adicionales:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- 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 PUT"

"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 todos [parámetros y cabeceras comunes](#) para esta solicitud, además de esta cabecera 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"](#)

"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"](#)
- ["Seleccione Contenido de objeto"](#)

"UploadPart"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite 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-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

"Cargar artículo"

"UploadPartCopy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite 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

["Cargar pieza: Copiar"](#)

Configure las conexiones y las cuentas de inquilino

Para configurar StorageGRID para aceptar conexiones desde aplicaciones cliente, es necesario crear una o más cuentas de inquilino y configurar las conexiones.

Cree y configure cuentas de inquilino de S3

Se requiere una cuenta de inquilino de S3 para que los clientes de la API de S3 puedan almacenar y recuperar objetos en StorageGRID. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos, usuarios, bloques y objetos.

Las cuentas de inquilino S3 las crea un administrador de grid de StorageGRID mediante Grid Manager o la API de gestión de grid. Consulte ["Gestione inquilinos"](#) para obtener más detalles. Una vez creada una cuenta de inquilino de S3, los usuarios inquilinos pueden acceder al administrador de inquilinos para gestionar grupos, usuarios, claves de acceso y bloques. Consulte ["Usar una cuenta de inquilino"](#) para obtener más detalles.



Mientras que los usuarios inquilinos de S3 pueden crear y gestionar la clave de acceso y los depósitos S3 con el administrador de inquilinos, deben usar una aplicación cliente S3 para ingerir y gestionar objetos. Consulte ["USE LA API DE REST DE S3"](#) para obtener más detalles.

Cómo configurar las conexiones de cliente

Un administrador de grid toma opciones de configuración que afectan a la forma en que los clientes S3 se conectan a StorageGRID para almacenar y recuperar datos. Hay cuatro pasos básicos para conectar StorageGRID a cualquier aplicación S3:

- Realice tareas de requisitos previos en StorageGRID, según cómo se conectará la aplicación cliente a StorageGRID.
- Utilice StorageGRID para obtener los valores que la aplicación necesita para conectarse a la cuadrícula. Puede hacer lo siguiente ["Use el asistente de configuración de S3"](#) O configure cada entidad StorageGRID manualmente.
- Utilice la aplicación S3 para completar la conexión a StorageGRID. Cree entradas DNS para asociar direcciones IP a cualquier nombre de dominio que desee utilizar.
- Realice tareas continuas en la aplicación y en StorageGRID para gestionar y supervisar el almacenamiento de objetos a lo largo del tiempo.

Para obtener más información sobre estos pasos, consulte ["Configurar conexiones de cliente"](#).

Información necesaria para las conexiones del cliente

Para almacenar o recuperar objetos, las aplicaciones cliente S3 se conectan al servicio de equilibrio de carga, que se incluye en todos los nodos de administración y de puerta de enlace, o al servicio de enrutador de distribución local (LDR), que se incluye en todos los nodos de almacenamiento.

Las aplicaciones cliente se pueden conectar a StorageGRID mediante la dirección IP de un nodo de

cuadrícula y el número de puerto del servicio en ese nodo. Opcionalmente, puede crear grupos de alta disponibilidad (HA) de nodos de equilibrio de carga para proporcionar conexiones altamente disponibles que utilicen direcciones IP virtuales (VIP). Si desea conectarse a StorageGRID con un nombre de dominio completo (FQDN) en lugar de una dirección IP o VIP, puede configurar entradas de DNS.

Consulte "[Resumen: Direcciones IP y puertos para conexiones cliente](#)" si quiere más información.

Decidir usar conexiones HTTPS o HTTP

Cuando se realizan conexiones de cliente mediante un extremo de equilibrio de carga, es necesario realizar conexiones mediante el protocolo (HTTP o HTTPS) especificado para ese extremo. Para utilizar HTTP para conexiones de cliente a nodos de almacenamiento, debe habilitar el uso.

De forma predeterminada, cuando las aplicaciones cliente se conectan a nodos de almacenamiento, deben utilizar HTTPS cifrado para todas las conexiones. Opcionalmente, puede habilitar conexiones HTTP menos seguras seleccionando **CONFIGURACIÓN > CONFIGURACIÓN DE SEGURIDAD > Red y objetos > Habilitar HTTP para conexiones de nodos de almacenamiento** en Grid Manager. Por ejemplo, una aplicación cliente puede utilizar HTTP al probar la conexión a un nodo de almacenamiento en un entorno no de producción.



Tenga cuidado al habilitar HTTP para una cuadrícula de producción porque las solicitudes y respuestas se enviarán sin cifrar.

Información relacionada

["Administre StorageGRID"](#)

["Ventajas de las conexiones HTTP activas, inactivas y simultáneas"](#)

S3 nombres de dominio de punto final para solicitudes S3

Antes de poder utilizar los nombres de dominio de punto final S3 para las solicitudes de cliente, un administrador de StorageGRID debe configurar el sistema para que acepte conexiones que utilicen nombres de dominio de punto final S3 en solicitudes de estilo de ruta de acceso S3 y S3 de estilo hospedado virtual.

Acerca de esta tarea

Para permitir utilizar solicitudes de estilo alojadas virtuales de S3, un administrador de grid debe realizar las siguientes tareas:

- Use Grid Manager para añadir los nombres de dominio de extremo S3 al sistema StorageGRID.
- Asegúrese de que el certificado que utiliza el cliente para las conexiones HTTPS a StorageGRID esté firmado para todos los nombres de dominio que el cliente necesita.

Por ejemplo, si el punto final de dominio de punto final de servicio de API S3 es `s3.company.com`, El administrador de la cuadrícula debe asegurarse de que el certificado utilizado para las conexiones HTTPS tiene `s3.company.com` Como Nombre Común del Asunto y en Nombres Alternativos del Asunto, y `*.s3.company.com` En el campo Nombres alternativos del asunto.

- "[Configure el servidor DNS](#)" Utilizado por el cliente para incluir registros DNS que coincidan con los nombres de dominio de punto final S3, incluidos los registros comodín necesarios.

Si el cliente se conecta mediante el servicio Load Balancer, el certificado que el administrador de grid configura es el certificado para el extremo de equilibrio de carga que utiliza el cliente.



Cada extremo de equilibrio de carga tiene su propio certificado y cada extremo se puede configurar para que reconozca diferentes nombres de dominio de extremo S3.

Si el cliente se conecta a nodos de almacenamiento, el certificado que configura el administrador de grid es el certificado de servidor personalizado único que se utiliza para el grid.

Consulte las instrucciones para "[Administración de StorageGRID](#)" si quiere más información.

Una vez completados estos pasos, puede utilizar solicitudes virtuales de estilo alojado.

Probar configuración de la API DE REST de S3

Puede utilizar la interfaz de línea de comandos (CLI de AWS) de Amazon Web Services para probar la conexión al sistema y verificar que puede leer y escribir objetos en el sistema.

Antes de empezar

- Ha descargado e instalado la CLI de AWS desde "aws.amazon.com/cli".
- Creó una cuenta de inquilino de S3 en el sistema StorageGRID.
- Creó una clave de acceso en la cuenta de inquilino.

Pasos

1. Configure los ajustes de la CLI de AWS para usar la cuenta que creó en el sistema StorageGRID:
 - a. Entrar 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 predeterminada que desea 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
```

Soporte para servicios de plataforma StorageGRID

Los servicios de plataforma StorageGRID permiten que las cuentas de inquilinos StorageGRID aprovechen servicios externos, como un bloque de S3 remoto, un extremo de servicio de notificación simple (SNS) o un clúster de Elasticsearch para ampliar los servicios que ofrece un grid.

La tabla siguiente resume los servicios de plataforma disponibles y las API S3 que se utilizan para configurarlos.

| Servicio de plataforma | Específico | API de S3 que se utiliza para configurar el servicio |
|----------------------------|---|--|
| Replicación de CloudMirror | Replica objetos de un bloque StorageGRID de origen en el bloque S3 remoto configurado. | PUT Bucket Replication (consulte "Operaciones en bloques") |
| Notificaciones | Envía notificaciones acerca de eventos en un bloque de StorageGRID de origen a un extremo de servicio simple de notificación (SNS) configurado. | Notificación PUT Bucket (consulte "Operaciones en bloques") |

| Servicio de plataforma | Específico | API de S3 que se utiliza para configurar el servicio |
|-------------------------|---|--|
| Integración de búsqueda | Envía metadatos de objetos para los objetos almacenados en un bloque de StorageGRID a un índice de Elasticsearch configurado. | "PUT bucket metadata notification Configuration" Nota: se trata de una API StorageGRID S3 personalizada. |

Un administrador de grid debe habilitar el uso de los servicios de plataforma para una cuenta de inquilino antes de poder utilizarlos. Consulte ["Administre StorageGRID"](#). A continuación, un administrador de arrendatarios debe crear un extremo que represente el servicio remoto en la cuenta de arrendatario. Este paso es necesario para poder configurar un servicio. Consulte ["Usar una cuenta de inquilino"](#).

Recomendaciones para el uso de servicios de plataformas

Antes de utilizar los servicios de plataforma, debe tener en cuenta las siguientes recomendaciones:

- NetApp recomienda que no permita más de 100 inquilinos activos con solicitudes S3 que requieran la replicación, las notificaciones y la integración de búsqueda de CloudMirror. Tener más de 100 inquilinos activos puede dar como resultado un rendimiento del cliente S3 más lento.
- Si un bucket de S3 del sistema StorageGRID tiene habilitadas las versiones y la replicación de CloudMirror, NetApp recomienda que el extremo de destino también tenga habilitado el control de versiones de bucket de S3. Esto permite que la replicación de CloudMirror genere versiones de objetos similares en el extremo.
- La replicación de CloudMirror no es compatible si el bloque de origen tiene la función S3 Object Lock habilitada.
- La replicación de CloudMirror generará un error ACCESSDENIED si el bloque de destino tiene activada la conformidad heredada.

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.

Controles de consistencia

Los controles de consistencia proporcionan un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en diferentes nodos de almacenamiento y sitios, según lo requiera la aplicación.

De forma predeterminada, StorageGRID garantiza la coherencia de lectura tras escritura de los objetos recién creados. Cualquier OBTENER después de un PUESTO completado correctamente podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, actualizaciones de metadatos y eliminaciones son

coherentes en la actualidad. Por lo general, las sobrescrituras tardan segundos o minutos en propagarse, pero pueden tardar hasta 15 días.

Si desea realizar operaciones de objetos en un nivel de coherencia diferente, puede especificar un control de coherencia para cada bloque o para cada operación de API.

Controles de consistencia

El control de consistencia afecta a cómo los metadatos que utiliza StorageGRID para realizar un seguimiento de los objetos se distribuyen entre los nodos y, por lo tanto, la disponibilidad de los objetos para las solicitudes del cliente.

Puede establecer el control de coherencia de un bloque o una operación API en uno de los siguientes valores:

- **Todos:** Todos los nodos reciben los datos inmediatamente, o la solicitud fallará.
- **Strong-global:** Garantiza la coherencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.
- **Strong-site:** Garantiza la coherencia de lectura después de escritura para todas las solicitudes de cliente dentro de un sitio.
- **Read-after-new-write:** (Predeterminado) 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.

Utilizar controles de coherencia «reescritura tras escritura» y «disponibles»

Cuando una OPERACIÓN HEAD u GET utiliza el control de consistencia «relativamente una vez que una nueva escritura», StorageGRID realiza la búsqueda en varios pasos, como se indica a continuación:

- Primero busca el objeto con una baja consistencia.
- Si esa búsqueda falla, repite la búsqueda en el siguiente nivel de coherencia hasta que alcanza un nivel de coherencia equivalente al comportamiento de la búsqueda global.

Si una operación HEAD u GET utiliza el control de consistencia "READ-after-new-write", pero el objeto no existe, la búsqueda de objetos siempre alcanzará un nivel de consistencia equivalente al comportamiento de strong-global. Debido a que este nivel de coherencia requiere que haya varias copias de los metadatos del objeto disponibles en cada sitio, puede recibir un número elevado de errores del servidor interno 500 si no están disponibles dos o más nodos de almacenamiento en el mismo sitio.

A menos que necesite garantías de coherencia similares a las de Amazon S3, podrá evitar estos errores en LAS operaciones DE CABEZA y OBTENER al establecer el control de coherencia en "Available". Cuando un CABEZAL o UNA operación DE OBTENER utiliza el control de consistencia "disponible", StorageGRID sólo proporciona consistencia eventual. No vuelve a intentar una operación fallida en los niveles de coherencia crecientes, por lo que no es necesario que haya disponibles varias copias de los metadatos de objeto.

Especifique el control de coherencia para la operación de API

Para configurar el control de coherencia para una operación de API individual, deben ser compatibles los controles de coherencia para la operación y debe especificar el control de coherencia en el encabezado de la solicitud. En este ejemplo se establece el control de coherencia en «punto de referencia» para una operación

GET Object.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



Debe usar el mismo control de coherencia para las operaciones PUT Object y GET Object.

Especifique el control de coherencia para el bloque

Para establecer el control de consistencia para el bloque, puede utilizar StorageGRID la solicitud de consistencia PUT Bucket y LA solicitud DE consistencia GET Bucket. También puede usar el Administrador de inquilinos o la API de gestión de inquilinos.

Cuando configure los controles de coherencia para un cucharón, tenga en cuenta lo siguiente:

- La configuración del control de coherencia para un bloque determina el control de coherencia que se utiliza para las operaciones de S3 realizadas en los objetos del bloque o en la configuración de bloques. No afecta a las operaciones del propio cucharón.
- El control de coherencia de una operación API individual anula el control de coherencia del bloque.
- En general, los depósitos deben usar el control de consistencia predeterminado, «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 el control de consistencia de cada solicitud API. Establecer el control de consistencia a nivel de cucharón únicamente como último recurso.

Cómo interactúan los controles de coherencia y las reglas de ILM para afectar a la protección de datos

Tanto la elección del control de coherencia como la regla de ILM afectan a la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el control de consistencia usado cuando se almacena un objeto afecta a la colocación inicial de los metadatos de objetos, mientras que el comportamiento de procesamiento seleccionado para la regla de ILM afecta a la colocación inicial de las copias de objetos. Dado que StorageGRID requiere acceso tanto a los metadatos de un objeto como a sus datos para cumplir con las solicitudes de los clientes, seleccionar los niveles de protección correspondientes para el nivel de coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas más predecibles del sistema.

Para las reglas de ILM hay disponibles los siguientes comportamientos de consumo:

- **Confirmación doble:** StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve el éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.
- **Estricto:** Todas las copias especificadas en la regla ILM deben hacerse antes de que el éxito se devuelva al cliente.
- **Balanceado:** StorageGRID intenta hacer todas las copias especificadas en la regla ILM en la ingesta; si esto no es posible, se hacen copias provisionales y se devuelve éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.



Antes de seleccionar el comportamiento de procesamiento de una regla de ILM, lea la descripción completa de estos ajustes en las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

Ejemplo de cómo puede interactuar el control de consistencia y la regla de ILM

Suponga que tiene una cuadrícula de dos sitios con la siguiente regla de ILM y la siguiente configuración de nivel de coherencia:

- **Norma ILM:** Cree dos copias de objetos, una en el sitio local y otra en un sitio remoto. Se ha seleccionado el comportamiento de procesamiento estricto.
- **Nivel de coherencia:** "Strong-global" (los metadatos de objetos se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en el grid, StorageGRID realiza copias de objetos y distribuye los metadatos en ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra la pérdida en el momento del mensaje de procesamiento correcto. Por ejemplo, si el sitio local se pierde poco después del procesamiento, seguirán existiendo copias de los datos del objeto y los metadatos del objeto en el sitio remoto. El objeto se puede recuperar completamente.

Si en su lugar usa la misma regla de ILM y el nivel de consistencia de «otrong-site», es posible que el cliente reciba un mensaje de éxito después de replicar los datos del objeto en el sitio remoto, pero antes de que los metadatos del objeto se distribuyan allí. En este caso, el nivel de protección de los metadatos de objetos no coincide con el nivel de protección de los datos de objetos. Si el sitio local se pierde poco después del procesamiento, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre los niveles de coherencia y las reglas del ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Información relacionada

["Gestión de objetos con ILM"](#)

["OBTENGA coherencia de bloques"](#)

["PONGA la consistencia del cucharón"](#)

Cómo gestionan las reglas de ILM de StorageGRID los objetos

El administrador de grid crea reglas de gestión del ciclo de vida de la información (ILM) para gestionar los datos de los objetos que se ingieren en el sistema StorageGRID desde aplicaciones cliente de la API REST S3. A continuación, estas reglas se añaden a la política de ILM para determinar cómo y dónde se almacenan los datos de objetos con el tiempo.

La configuración de ILM determina los siguientes aspectos de un objeto:

- **Geografía**

La ubicación de los datos de un objeto, ya sea en el sistema StorageGRID (pool de almacenamiento) o en un pool de almacenamiento en el cloud.

- **Grado de almacenamiento**

El tipo de almacenamiento utilizado para almacenar datos de objetos, como la tecnología flash o el disco giratorio.

- **Protección contra pérdidas**

Cuántas copias se hacen y los tipos de copias que se crean: Replicación, codificación de borrado o ambos.

- **Retención**

Los cambios se producen a lo largo del tiempo en el modo en que se gestionan los datos de un objeto, dónde se almacenan y cómo se protegen de pérdidas.

- **Protección durante la ingesta**

El método utilizado para proteger los datos de objetos durante el procesamiento: Colocación síncrona (utilizando las opciones equilibradas o estrictas para el comportamiento de ingesta) o creación de copias provisionales (mediante la opción Dual Commit).

Las reglas de ILM pueden filtrar y seleccionar objetos. Para los objetos ingeridos mediante S3, las reglas de ILM pueden filtrar objetos en función de los siguientes metadatos:

- Cuenta de inquilino
- Nombre del bloque
- Tiempo de ingesta
- Clave
- Hora del último acceso



De forma predeterminada, las actualizaciones del último tiempo de acceso se deshabilitan para todos los bloques S3. Si su sistema StorageGRID incluye una regla de ILM que utiliza la opción de hora de último acceso, debe habilitar las actualizaciones a la hora del último acceso para los bloques S3 especificados en esa regla. Utilice la solicitud de hora de último acceso a PUT Bucket, el Gestor de inquilinos (consulte "[Activar o desactivar las actualizaciones de la hora del último acceso](#)") O la API de gestión de inquilinos. Al habilitar las actualizaciones del último tiempo de acceso, tenga en cuenta que el rendimiento de StorageGRID puede reducirse, especialmente en sistemas con objetos pequeños.

- Restricción de ubicación
- Tamaño del objeto
- Metadatos del usuario
- Etiqueta de objeto

Información relacionada

["Usar una cuenta de inquilino"](#)

["Gestión de objetos con ILM"](#)

["PUT Bucket última hora de acceso"](#)

Control de versiones de objetos

Puede utilizar el control de versiones para conservar varias versiones de un objeto, lo que protege contra la eliminación accidental de objetos y le 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 1,000 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 habilitar explícitamente el control de versiones para cada segmento a fin de activar esta funcionalidad para el bloque. A cada objeto de su 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 usen “Tiempo no corriente” como tiempo de referencia (seleccione **Sí** para la pregunta, “¿Aplicar esta regla solo a versiones de objetos anteriores?”) pulg ["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 reducen 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.

Consulte ["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 segmento mediante una solicitud PUT Bucket con el `x-amz-bucket-object-lock-enabled` solicite el encabezado. 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:
 - Usuarios con `s3:BypassGovernanceRetention` el permiso puede utilizar el `x-amz-bypass-governance-retention: true` solicitar cabecera para omitir la configuración de retención.
 - Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha.
 - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

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 de configuración de bloqueo de objeto PUT para que el depósito especifique el modo por defecto y el número por defecto de días o años.

PONER configuración de bloqueo de objeto

La solicitud de configuración PUT Object Lock 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 bloque, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` y `x-amz-object-lock-retain-until-date` no se han especificado. El período de retención predeterminado se utiliza para calcular el valor de retener hasta la fecha si `x-amz-object-lock-retain-until-date` no se ha especificado.

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 la `s3:PutBucketObjectLockConfiguration` permiso, o `be account root`, para completar esta operación.

La `Content-MD5` La cabecera de la solicitud se debe especificar en la solicitud PUT.

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"](#).
- Emita una solicitud de configuración OBTENER bloqueo de objeto.

OBTENER configuración de bloqueo de objeto

La solicitud OBTENER configuración de bloqueo de objeto le permite determinar si el bloqueo de objeto S3 está activado 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 bloque, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` no se ha especificado. El período de retención predeterminado se utiliza para calcular el valor de retener hasta la fecha if `x-amz-object-lock-retain-until-date` no se ha especificado.

Debe tener la `s3:GetBucketObjectLockConfiguration` permiso, o `be 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 un "OBJETO PUT", "PONER objeto: Copiar", o "Inicie la carga de varias partes" 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 retener hasta la fecha 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:

- La `Content-MD5` la cabecera de la solicitud es necesaria si la hay `x-amz-object-lock-*`. El encabezado de la solicitud está presente en LA solicitud `PUT Object`. `Content-MD5` No es necesario PARA PONER objeto: Copiar o iniciar carga de varias partes.
- Si el bloque no tiene habilitado el bloqueo de objetos S3 y un `x-amz-object-lock-*`. El encabezado de la solicitud está presente, se devuelve un error de solicitud incorrecta 400 (`InvalidRequest`).
- La solicitud `PUT Object` admite el uso de `x-amz-storage-class: REDUCED_REDUNDANCY` Para igualar 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 `HEAD Object` incluirá los encabezados `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, y `x-amz-object-lock-legal-hold`, si está configurado y si el remitente de la solicitud tiene el correcto `s3:Get*` permisos.

Puede utilizar el `s3:object-lock-remaining-retention-days` 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:

- `PUT Object legal-hold`

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.

- `PUT Object retention`
 - El valor de modo puede ser CUMPLIMIENTO o GOBIERNO (distingue entre mayúsculas y minúsculas).
 - El valor retener hasta la fecha 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` El permiso puede omitir la configuración de retención activa de un objeto que utiliza el modo de GOBIERNO. Todas las operaciones de retención `DELETE` o `PUT Object` deben incluir `x-amz-bypass-governance-retention:true` solicite el encabezado. Estos usuarios pueden realizar las siguientes operaciones adicionales:

- Realice operaciones de SUPRESIÓN DE objetos o SUPRESIÓN DE varios objetos para suprimir 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 de retención de objetos `PUT` 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 de retención de objetos PUT 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: Uso del bloqueo de objetos de S3"](#)

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 completa sobre la creación de configuraciones del ciclo de vida de S3, consulte ["Guía para desarrolladores 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

Si aplica una configuración del ciclo de vida a un bloque, la configuración del ciclo de vida del bloque siempre anula la configuración de ILM de StorageGRID. StorageGRID utiliza la configuración de caducidad del bloque, no de ILM, para determinar si se deben eliminar o conservar objetos específicos.

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:

- ELIMINAR ciclo de vida de bloque
- OBTENGA el ciclo de vida de la cuchara
- CICLO de vida DE la cuchara

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 sólo se aplica a los objetos que coinciden con el prefijo `category1/` y que tienen un `key2` valor de `tag2`. La `Expiration` Parámetro especifica que los objetos que coinciden con el filtro caducarán a medianoche el 22 de agosto de 2020.
2. La regla 2 sólo se aplica a los objetos que coinciden con el prefijo `category2/`. La `Expiration` el parámetro especifica que los objetos que coinciden con el filtro caducarán 100 días después de que se ingieran.



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 sólo se aplica a los objetos que coinciden con el prefijo `category3/`. La `Expiration` parámetro especifica que cualquier versión no actual de objetos coincidentes caducará 50 días después de que se conviertan en no actualizados.

```

{
  "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 del ciclo de vida, se aplica a un bloque emitiendo una solicitud PUT Bucket Lifecycle.

Esta solicitud aplica la configuración del ciclo de vida del archivo de ejemplo a los objetos de un bloque denominado `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que se ha aplicado correctamente una configuración del ciclo de vida al bloque, emita una solicitud GET Bucket Lifecycle. 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 PUT Object, HEAD Object o GET Object. Si se aplica una regla, la respuesta incluye una `Expiration` parámetro que indica cuándo caduca el objeto y qué regla de caducidad se ha coincido.



Dado que el ciclo de vida de los bloques anula la gestión del ciclo de vida de `expiry-date` se muestra la fecha real en la que se eliminará el objeto. Para obtener más información, consulte ["Cómo se determina la retención de objetos"](#).

Por ejemplo, esta solicitud PUT Object fue emitida el 22 de junio de 2020 y coloca un objeto en el `testbucket` cucharón.

```
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 DE OBJETO HEAD se utilizó para obtener metadatos para el mismo objeto en el bloque 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": {}
}
```

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 tu aplicación comprueba de forma rutinaria si existe un objeto en una ruta en la que no esperas que exista el objeto, debes usar el control de consistencia "disponible". Por ejemplo, debe utilizar el control de coherencia "disponible" si su aplicación dirige una ubicación antes DE PONERLA en práctica.

De lo contrario, si la operación HEAD no encuentra el objeto, es posible que reciba un número elevado de 500 errores internos de Server si uno o más nodos de almacenamiento no están disponibles.

Puede establecer el control de consistencia "Available" para cada bloque mediante LA solicitud DE consistencia PUT Bucket, o bien puede especificar el control de consistencia 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 la "[opción global para comprimir objetos almacenados](#)" está activado, las aplicaciones cliente S3 deben evitar realizar operaciones GET Object que especifiquen un rango de bytes devueltos. Estas operaciones de «lectura de rango» son ineficientes, ya que StorageGRID debe descomprimir de forma efectiva los objetos para acceder a los bytes solicitados. LAS operaciones GET Object que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, es ineficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden 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.

Información relacionada

- ["Controles de consistencia"](#)
- ["PONGA la consistencia del cucharón"](#)
- ["Administre StorageGRID"](#)

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 el `x-amz-date` Encabezado de la solicitud, anula cualquier valor especificado en el encabezado de solicitud de fecha. Al utilizar la versión 4 de la firma de AWS, el `x-amz-date` el 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: <ul style="list-style-type: none">• El valor SHA256 no se calcula para el cuerpo de la solicitud. El valor enviado por el usuario se acepta sin validación, como si fuera el valor <code>UNSIGNED-PAYLOAD</code> se había proporcionado para el <code>x-amz-content-sha256</code> encabezado. |
| x-amz-token de seguridad | No implementada. Retornos <code>XNotImplemented</code> . |

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 admite dos métodos de autenticación: HTTP `Authorization` encabezado y uso de parámetros de consulta.

Utilice el encabezado autorización HTTP

HTTP `Authorization` Todas las operaciones de la API de S3 utilizan el encabezado excepto las solicitudes anónimas, donde lo permite la directiva de bloques. La `Authorization` 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 |
|--|--|
| <div>OBTENER servicio</div> <div>(ListBuckets)</div> | 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 GET Storage Usage le indica la cantidad total de almacenamiento que está usando una cuenta y por cada bloque asociado con la cuenta. Se trata de una operación en el servicio con una ruta de / y un parámetro de consulta personalizado (?x-ntap-sg-usage) agregado. |
| OPCIONES / | Las aplicaciones cliente pueden emitir OPTIONS / Se solicita al puerto S3 en 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. |

Información relacionada

["Obtenga el uso del almacenamiento"](#)

Operaciones en bloques

El sistema StorageGRID admite un máximo de 1,000 bloques para cada cuenta de inquilino de S3.

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:

- ["Documentación de Amazon Web Services \(AWS\): Restricciones y limitaciones de buckets"](#)
- ["Configure los nombres de dominio de punto final S3"](#)

Las operaciones GET Bucket (List Objects) Y GET Bucket admiten los controles de coherencia de StorageGRID.

Puede comprobar si las actualizaciones a la hora del último acceso están habilitadas o deshabilitadas para grupos individuales.

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 |
|----------------------------------|--|
| ELIMINAR bloque | Esta operación elimina el cucharón. |
| ELIMINAR los cors de cucharón | Esta operación elimina la configuración de CORS para el cucharón. |
| DELETE Bucket Encryption | Esta operación elimina el cifrado predeterminado del bloque. Los objetos cifrados existentes permanecen cifrados, pero todos los objetos nuevos agregados al depósito no están cifrados. |
| ELIMINAR ciclo de vida de bloque | Esta operación elimina la configuración del ciclo de vida del bloque. Consulte "Cree una configuración del ciclo de vida de S3" . |
| ELIMINE la política de bloques | Esta operación elimina la política asociada al bloque. |
| DELETE Bucket replicación | Esta operación elimina la configuración de replicación conectada al bloque. |
| DELETE Bucket tagging | Esta operación utiliza <code>tagging</code> subrecurso para quitar todas las etiquetas de un bloque. |

| Funcionamiento | Implementación |
|---|---|
| OBTENER bloque (ListObjects) (ListObjectsV2) | <p>Esta operación devuelve algunos o todos (hasta 1,000) de los objetos de un bloque. La clase de almacenamiento para los objetos puede tener cualquiera de dos valores, incluso si el objeto se ingirió con la <code>REDUCED_REDUNDANCY</code> opción de clase de almacenamiento:</p> <ul style="list-style-type: none"> • <code>STANDARD</code>, Que indica que el objeto se almacena en una agrupación de almacenamiento que consta de nodos de almacenamiento. • <code>GLACIER</code>, Que indica que el objeto se ha movido al bloque externo especificado por el grupo de almacenamiento en la nube. <p>Si el bloque contiene un gran número de claves eliminadas que tienen el mismo prefijo, la respuesta podría incluir algunas <code>CommonPrefixes</code> que no contienen claves.</p> |
| OBTENGA las versiones DE objeto Bucket (Versiones de ListObjectVersions) | <p>Con el acceso DE LECTURA en un bloque, esta operación con el <code>versions</code> subrecurso enumera los metadatos de todas las versiones de objetos del bloque.</p> |
| GET Bucket acl | <p>Esta operación devuelve una respuesta positiva y el ID, DisplayName y permiso del propietario del bloque, lo que indica que el propietario tiene acceso completo al bloque.</p> |
| OBTENGA los cors del cucharón | <p>Esta operación devuelve el <code>cors</code> configuración del bloque.</p> |
| OBTENGA el cifrado de bloque | <p>Esta operación devuelve la configuración de cifrado predeterminada del bloque.</p> |
| OBTENGA el ciclo de vida de la cuchara (GetBucketLifecycleConfiguration) | <p>Esta operación devuelve la configuración del ciclo de vida del bloque. Consulte "Cree una configuración del ciclo de vida de S3".</p> |
| OBTENER ubicación de bloque | <p>Esta operación devuelve la región que se estableció mediante el <code>LocationConstraint</code> Elemento de la solicitud PUT Bucket. Si la región del cucharón es <code>us-east-1</code>, se devuelve una cadena vacía para la región.</p> |
| OBTENGA la notificación DE BUCKET (GetBucketNotificationConfiguration) | <p>Esta operación devuelve la configuración de notificación asociada al bloque.</p> |
| OBTENGA la política de bloques | <p>Esta operación devuelve la política asociada al bloque.</p> |

| Funcionamiento | Implementación |
|--|---|
| OBTENGA la replicación de Bucket | Esta operación devuelve la configuración de replicación asociada al bloque. |
| GET Bucket tagging | Esta operación utiliza <code>tagging</code> subrecurso para devolver todas las etiquetas de un bloque. |
| OBTENGA el control de versiones de Bucket | <p>Esta implementación usa la <code>versioning</code> subrecurso para devolver el estado de control de versiones de un bloque.</p> <ul style="list-style-type: none"> • <i>Blank</i>: Nunca se ha activado el control de versiones (el cucharón es <code>"unversioned"</code>) • Activado: El control de versiones está activado • Suspendido: El control de versiones se ha habilitado anteriormente y se ha suspendido |
| OBTENER configuración de bloqueo de objeto | <p>Esta operación devuelve el modo de retención predeterminado de bloque y el período de retención predeterminado, si está configurado.</p> <p>Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".</p> |
| Cubo DE CABEZA | <p>Esta operación determina si existe un bloque y tiene permiso para acceder a él.</p> <p>Esta operación devuelve:</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: El UUID del bloque en formato UUID. • <code>x-ntap-sg-trace-id</code>: El ID de traza único de la solicitud asociada. |

| Funcionamiento | Implementación |
|-------------------------------|--|
| COLOQUE el cucharón | <p>Esta operación crea un nuevo bloque. Al crear la cuchara, se convierte en el propietario de la cuchara.</p> <ul style="list-style-type: none"> • Los nombres de los bloques deben cumplir con las siguientes reglas: <ul style="list-style-type: none"> ◦ Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino). ◦ Debe ser compatible con DNS. ◦ Debe incluir al menos 3 y no más de 63 caracteres. ◦ 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 periodos provocarán problemas en la verificación del certificado comodín del servidor. • De forma predeterminada, los bloques se crean en la <code>us-east-1</code> región; sin embargo, puede utilizar la <code>LocationConstraint</code> elemento de solicitud en el cuerpo de solicitud para especificar una región diferente. Cuando utilice la <code>LocationConstraint</code> Elemento, debe especificar el nombre exacto de una región que se ha definido mediante el Administrador de grid 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. <p>Nota: Se producirá un error si la solicitud PUT Bucket utiliza una región que no se ha definido en StorageGRID.</p> <ul style="list-style-type: none"> • Puede incluir el <code>x-amz-bucket-object-lock-enabled</code> Solicite el encabezado para crear un bucket con el bloqueo de objetos S3 habilitado. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3". <p>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.</p> |
| COLOQUE los cors del cucharón | <p>Esta operación establece la configuración de CORS para un cucharón 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 se utiliza un bloque de S3 llamado <code>images</code> para almacenar gráficos. Mediante el ajuste de la configuración de CORS para <code>images</code> bloque, puede permitir que las imágenes de ese bloque se muestren en el sitio web <code>http://www.example.com</code>.</p> |

| Funcionamiento | Implementación |
|---|---|
| PUT Bucket Encryption | <p>Esta operación establece el estado de cifrado predeterminado de un bloque 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, defina la <code>SSEAlgorithm</code> parámetro a. <code>AES256</code>, y no utilice el <code>KMSMasterKeyID</code> parámetro.</p> <p>La configuración de cifrado predeterminada de bloque se omite si la solicitud de carga de objeto ya especifica cifrado (es decir, si la solicitud incluye la <code>x-amz-server-side-encryption-*</code> encabezado de solicitud).</p> |
| <p>CICLO de vida DE la cuchara</p> <p>(PutBucketLifecycleConfiguration)</p> | <p>Esta operación crea una nueva configuración del ciclo de vida para el bloque o reemplaza 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:</p> <ul style="list-style-type: none"> • Caducidad (días, fecha) • NoncurrentVersionExpiración (NoncurrentDays) • Filtro (prefijo, etiqueta) • Estado • ID <p>StorageGRID no admite estas acciones:</p> <ul style="list-style-type: none"> • AbortEncompleteMultipartUpload • ExpiredObjectDeleteMarker • Transición <p>Consulte "Cree una configuración del ciclo de vida de S3". Para comprender cómo la acción de caducidad en un ciclo de vida de bloques interactúa con las instrucciones de ubicación de ILM, consulte "Cómo funciona ILM a lo largo de la vida de un objeto".</p> <p>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.</p> |

| Funcionamiento | Implementación |
|---|---|
| <p>NOTIFICACIÓN DE PUT Bucket</p> <p>(PutBucketNotificationConfiguration)</p> | <p>Esta operación configura notificaciones para el bloque mediante el XML de configuración de notificación incluido en el cuerpo de la solicitud. Debe tener en cuenta los siguientes detalles de implementación:</p> <ul style="list-style-type: none"> StorageGRID admite temas como destinos el Servicio de notificación simple (SNS). No se admiten los puntos finales de Simple Queue Service (SQS) o Amazon 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. <p>El extremo debe existir para que la configuración de la notificación se realice correctamente. Si el extremo no existe, un <code>400 Bad Request</code> se devuelve un error con el código <code>InvalidArgument</code>.</p> <ul style="list-style-type: none"> No puede configurar una notificación para los siguientes tipos de evento. Estos tipos de evento no son compatibles. <ul style="list-style-type: none"> <code>s3:ReducedRedundancyLostObject</code> <code>s3:ObjectRestore:Completed</code> 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: <ul style="list-style-type: none"> EventSource <p><code>sgws:s3</code></p> *AwsRegion* <p>no incluido</p> x-amz-id-2 <p>no incluido</p> arn <p><code>urn:sgws:s3:::bucket_name</code></p> |
| <p>POLÍTICA DE PUT Bucket</p> | <p>Esta operación establece la política asociada al bloque.</p> |

| Funcionamiento | Implementación |
|------------------------|---|
| PUT Bucket replication | <p>Esta operación configura "Replicación de CloudMirror de StorageGRID" Para el depósito que utiliza 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:</p> <ul style="list-style-type: none"> • StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de <code>Filter</code> Elemento para reglas y sigue las convenciones V1 para eliminar versiones de objetos. Para obtener más detalles, consulte "Documentación de Amazon S3 en la configuración de la 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". <p>El extremo debe existir para que la configuración de replicación se complete correctamente. Si el extremo no existe, la solicitud falla como un 400 Bad Request. El mensaje de error indica: Unable to save the replication policy. The specified endpoint URN does not exist: <i>URN</i>.</p> <ul style="list-style-type: none"> • No es necesario especificar un <code>Role</code> En el XML de configuración. StorageGRID no utiliza este valor y se ignorará si se envía. • Si omite la clase de almacenamiento del XML de configuración, StorageGRID utiliza <code>STANDARD</code> clase de almacenamiento 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: <ul style="list-style-type: none"> ◦ 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 |
|--|--|
| PUT Bucket etiquetaje | <p>Esta operación utiliza <code>tagging</code> subrecurso para agregar o actualizar un conjunto de etiquetas para un bloque. Al añadir etiquetas de bloque, tenga en cuenta las siguientes limitaciones:</p> <ul style="list-style-type: none"> • 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. |
| PONER creación de versiones de bloques | <p>Esta implementación usa la <code>versioning</code> subrecurso para establecer el estado de control de versiones de un bloque existente. Puede establecer el estado de control de versiones con uno de los siguientes valores:</p> <ul style="list-style-type: none"> • 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 bloque reciben el ID de versión <code>null</code>. |
| PONER configuración de bloqueo de objeto | <p>Esta operación configura o elimina el modo de retención predeterminado de bloque y el período de retención predeterminado.</p> <p>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.</p> <p>Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" para obtener información detallada.</p> |

Información relacionada

["Controles de consistencia"](#)

["HORA de último acceso al bloque DE GET"](#)

["Utilice las políticas de acceso de bloques y grupos"](#)

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

Operaciones personalizadas en bloques

El sistema StorageGRID admite operaciones de bloques personalizadas que se añaden a la API DE REST de S3 y son específicas del sistema.

En la siguiente tabla, se enumeran las operaciones de bloque personalizadas que admite StorageGRID.

| Funcionamiento | Descripción | Si quiere más información |
|---|--|---|
| OBTENGA coherencia de bloques | Devuelve el nivel de coherencia que se aplica a un bloque determinado. | "OBTENGA coherencia de bloques" |
| PONGA la consistencia del cucharón | Establece el nivel de consistencia aplicado a un bloque determinado. | "PONGA la consistencia del cucharón" |
| HORA de último acceso al bloque DE GET | Devuelve si las actualizaciones del último tiempo de acceso están habilitadas o deshabilitadas para un bloque en particular. | "HORA de último acceso al bloque DE GET" |
| PUT Bucket última hora de acceso | Permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para un bloque en particular. | "PUT Bucket última hora de acceso" |
| DELETE bucket metadata notification Configuration | Elimina el XML de configuración de notificación de metadatos asociado a un bloque en particular. | "DELETE bucket metadata notification Configuration" |
| 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. | "OBTENGA la configuración de notificación de metadatos del bloque de datos" |
| PUT bucket metadata notification Configuration | Configura el servicio de notificación de metadatos para un bloque. | "PUT bucket metadata notification Configuration" |
| COLOQUE el cucharón con la configuración de cumplimiento | Obsoleto y no compatible: Ya no puede crear nuevos bloques con el cumplimiento de normativas habilitado. | "Obsoleto: COLOQUE el cucharón con la configuración de cumplimiento" |
| Obtenga el cumplimiento de normativas de Bucket | Obsoleto pero compatible: Devuelve la configuración de cumplimiento vigente para un bloque compatible existente. | "En desuso: OBTENGA el cumplimiento de normativas de bloques" |
| CUMPLIR con la normativa de los bloques | Obsoleto pero compatible: Permite modificar la configuración de cumplimiento de un bloque compatible heredado. | "Obsoleto: PUT Bucket Compliance" |

Información relacionada

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

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 "[controles de consistencia](#)" son compatibles con todas las operaciones de los objetos, con la excepción de lo siguiente:
 - OBTENER ACL de objeto
 - OPTIONS /
 - PONER objeto legal
 - PUT Object retention
 - SELECCIONE Contenido de objeto
- 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 «'últimos logros'» se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 inician 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.
- No se puede acceder a los objetos de datos procesados en el sistema de StorageGRID a través de Swift mediante S3.

En la siguiente tabla se describe cómo StorageGRID implementa operaciones de objetos API DE REST de S3.

| Funcionamiento | Implementación |
|--|--|
| ELIMINAR objeto | <p>Autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles.</p> <p>Al procesar una solicitud DE ELIMINACIÓN de objeto, 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.</p> <p>Creación de versiones</p> <p>Para eliminar una versión específica, el solicitante debe ser el propietario del bloque y utilizar el <code>versionId</code> subrecurso. El uso de este subrecurso elimina permanentemente la versión. Si la <code>versionId</code> corresponde a un marcador de borrado, el encabezado de respuesta <code>x-amz-delete-marker</code> se devuelve establecido en <code>true</code>.</p> <ul style="list-style-type: none"> • Si se elimina un objeto sin el <code>versionId</code> subrecurso en un bloque habilitado para la versión, da como resultado la generación de un marcador de borrado. La <code>versionId</code> para el marcador de borrado se devuelve mediante <code>x-amz-version-id</code> encabezado de respuesta, y el <code>x-amz-delete-marker</code> el encabezado de la respuesta se devuelve establecido en <code>true</code>. • Si se elimina un objeto sin el <code>versionId</code> subrecurso en un bloque suspendido de la versión, se produce la eliminación permanente de una versión "nula" ya existente o un marcador de borrado "nulo" y la generación de un nuevo marcador de borrado "nulo". La <code>x-amz-delete-marker</code> el encabezado de la respuesta se devuelve establecido en <code>true</code>. <p>Nota: En algunos casos, pueden existir varios marcadores de borrado para un objeto.</p> <p>Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" Para obtener información sobre cómo eliminar versiones de objetos en el modo de GOBIERNO.</p> |
| ELIMINAR varios objetos (ElieteObjects) | <p>Autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles.</p> <p>Se pueden eliminar varios objetos en el mismo mensaje de solicitud.</p> <p>Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" Para obtener información sobre cómo eliminar versiones de objetos en el modo de GOBIERNO.</p> |

| Funcionamiento | Implementación |
|------------------------------------|---|
| ELIMINAR etiquetado de objetos | <p>Utiliza la <code>tagging</code> subrecurso para quitar todas las etiquetas de un objeto.</p> <p>Creación de versiones</p> <p>Si la <code>versionId</code> el parámetro de consulta no se especifica en la solicitud, la operación elimina 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 borrado, se devuelve el estado "MetodNotAllowed" con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.</p> |
| OBTENER objeto | "OBTENER objeto" |
| OBTENER ACL de objeto | 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. |
| OBTENER retención legal de objetos | "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" |
| OBTENGA retención de objetos | "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" |
| GET Object tagging | <p>Utiliza la <code>tagging</code> subrecurso para devolver todas las etiquetas de un objeto.</p> <p>Creación de versiones</p> <p>Si la <code>versionId</code> el 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 borrado, se devuelve el estado "MetodNotAllowed" con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.</p> |
| OBJETO HEAD | "OBJETO HEAD" |
| Restauración DE objetos posterior | "Restauración DE objetos posterior" |
| OBJETO PUT | "OBJETO PUT" |
| PONER objeto: Copiar | "PONER objeto: Copiar" |
| PONER objeto legal | "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" |
| PUT Object retention | "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" |

| Funcionamiento | Implementación |
|---------------------|---|
| PUT Object tagging | <p>Utiliza la <code>tagging</code> subrecurso para agregar un conjunto de etiquetas a un objeto existente.</p> <p>Límites de etiqueta de objeto</p> <p>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.</p> <p>Comportamiento de ingesta y actualizaciones de etiquetas</p> <p>Cuando se utiliza PUT Object tagging para actualizar las etiquetas de un objeto, StorageGRID no vuelve a procesar 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.</p> <p>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.</p> <p>Resolución de conflictos</p> <p>Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en base a «las últimas victorias». El plazo para la evaluación de «últimos logros» se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 inician una operación.</p> <p>Creación de versiones</p> <p>Si la <code>versionId</code> el 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 borrado, se devuelve el estado "MethodNotAllowed" con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.</p> |
| SelectObjectContent | "SelectObjectContent" |

Información relacionada

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

Utilice S3 Select

StorageGRID admite las siguientes cláusulas, tipos de datos y operadores de Amazon S3 Select para ["SelectObjectContent"](#).



No se admiten los elementos que no aparecen en la lista.

Para obtener sintaxis, consulte ["SelectObjectContent"](#). Para obtener más información acerca de S3 Select, consulte ["Documentación de AWS para S3 Select"](#).

Solo las cuentas de inquilino con S3 Select habilitado pueden emitir consultas de SelectObjectContent. Consulte ["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 PUT"
- "PONER objeto: Copiar"
- "Inicie la carga de varias partes"

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 encabezado 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:

- "OBTENER objeto"
- "OBJETO HEAD"
- "OBJETO PUT"
- "PONER objeto: Copiar"
- "Inicie la carga de varias partes"
- "Cargar artículo"
- "Cargar pieza: Copiar"

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 todas las solicitudes realizadas sobre http cuando se utilice SSE-C. Por cuestiones de seguridad, debe tener en cuenta cualquier clave que envíe accidentalmente mediante http para que se vea 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 para desarrolladores de Amazon S3: Protección de datos mediante cifrado en el lado del servidor con claves de cifrado proporcionadas por el cliente \(SSE-C\)"](#)

OBTENER objeto

Puede usar la solicitud GET Object de S3 para recuperar un objeto de un bloque de S3.

OBJETOS GET y objetos de varias partes

Puede utilizar el `partNumber` parámetro de solicitud para recuperar una parte específica de un objeto de varias partes o segmentado. La `x-amz-mp-parts-count` el elemento de respuesta indica cuántas partes tiene el objeto.

Puede ajustar `partNumber` a 1 para objetos segmentados/multipartes y no segmentados/no multipartes; sin embargo, la `x-amz-mp-parts-count` el elemento de respuesta sólo se devuelve para objetos segmentados o multipartes.

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 el `x-amz-missing-meta` encabezado si el nombre o valor de clave incluye caracteres no imprimibles.

Encabezado de solicitud no compatible

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented`:

- `x-amz-website-redirect-location`

Creación de versiones

Si es un `versionId` no se especifica el subrecurso, la operación busca la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de borrado, se devuelve el estado "no encontrado" con la `x-amz-delete-marker` encabezado de respuesta establecido 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 la clave de cifrado del 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 que se deben tener en ["Usar cifrado del servidor"](#).

Comportamiento de OBTENER objeto para objetos de pool de almacenamiento en cloud

Si un objeto se ha almacenado en un ["Pool de almacenamiento en cloud"](#), El comportamiento de una solicitud GET Object depende del estado del objeto. Consulte ["OBJETO HEAD"](#) para obtener más detalles.



Si un objeto está almacenado en un Cloud Storage Pool y existen también una o varias copias del objeto en el grid, GET Object Requests intentará recuperar datos del grid, antes de recuperarlos del Cloud Storage Pool.

| Estado del objeto | Comportamiento DE GET Object |
|--|---|
| 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 un "Restauración DE objetos posterior" 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 se complete la solicitud DE restauración DE objeto POSTERIOR. |
| 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, es posible que UNA solicitud GET Object devuelva 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:

- La solicitud GET Object puede devolver algunos datos pero detenerse a mitad de camino a través de la transferencia.
- Una petición GET Object posterior podría devolver 403 Forbidden.

OBTENGA la replicación de objetos y entre grid

Si está utilizando ["federación de grid"](#) y.. ["replicación entre grid"](#) Está activado para un depósito, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud GET Object. La respuesta incluye los recursos específicos de StorageGRID `x-ntap-sg-cgr-replication-status` cabecera de respuesta, que tendrá uno de los siguientes valores:

| Cuadrícula | Estado de replicación |
|------------|--|
| Origen | <ul style="list-style-type: none">• ÉXITO: 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 el `x-amz-replication-status` encabezado.

Información relacionada

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

OBJETO HEAD

Puede usar la solicitud del ENCABEZADO Object de S3 para recuperar metadatos de un objeto sin devolver el objeto propiamente dicho. Si el objeto se almacena en un pool de almacenamiento en el cloud, puede usar HEAD Object para determinar el estado de transición del objeto.

OBJETO DE CABECERA y objetos de varias partes

Puede utilizar el `partNumber` parámetro de solicitud para recuperar metadatos de una parte específica de un objeto de varias partes o segmentado. La `x-amz-mp-parts-count` el elemento de respuesta indica cuántas partes tiene el objeto.

Puede ajustar `partNumber` a 1 para objetos segmentados/multipartes y no segmentados/no multipartes; sin embargo, la `x-amz-mp-parts-count` el elemento de respuesta sólo se devuelve para objetos segmentados o multipartes.

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 el `x-amz-missing-meta` encabezado si el nombre o valor de clave incluye caracteres no imprimibles.

Encabezado de solicitud no compatible

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented`:

- `x-amz-website-redirect-location`

Creación de versiones

Si es un `versionId` no se especifica el subrecurso, la operación busca la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de borrado, se devuelve el estado "no encontrado" con la `x-amz-delete-marker` encabezado de respuesta establecido 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 la clave de cifrado del 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 que se deben tener en "[Usar cifrado del servidor](#)".

PRINCIPALES respuestas de objetos 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 al OBJETO PRINCIPAL |
|--|--|
| 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 ningún encabezado de respuesta especial). |
| Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable | <p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Hasta que el objeto se realice la transición a un estado no recuperable, el valor de expiry-date se configura a una hora distante en el futuro. El sistema StorageGRID no controla la hora exacta de la transición.</p> |
| El objeto ha pasado a estar en estado no recuperable, pero también existe al menos una copia en la cuadrícula | <p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Valor para expiry-date se configura a una hora distante en el futuro.</p> <p>Nota: Si la copia en la cuadrícula no está disponible (por ejemplo, un nodo de almacenamiento está caído), debe emitir un "Restauración DE objetos posterior" Solicite restaurar la copia del Cloud Storage Pool antes de poder recuperar el objeto correctamente.</p> |
| El objeto ha pasado a un estado que no se puede recuperar y no existe ninguna copia en la cuadrícula | <p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> |
| Objeto en proceso de restauración a partir de un estado no recuperable | <p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p> |

| Estado del objeto | Respuesta al OBJETO PRINCIPAL |
|---|---|
| Objeto completamente restaurado en el pool de almacenamiento en cloud | <p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"</p> <p>La expiry-date Indica si el objeto del Cloud Storage Pool regresará a un estado no recuperable.</p> |

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, es posible que una solicitud HEAD Object devuelva 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.

HEAD Object y replicación entre grid

Si está utilizando ["federación de grid"](#) y.. ["replicación entre grid"](#) Está activado para un depósito, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud de objeto HEAD. La respuesta incluye los recursos específicos de StorageGRID `x-ntap-sg-cgr-replication-status` cabecera de respuesta, que tendrá uno de los siguientes valores:

| Cuadrícula | Estado de replicación |
|------------|--|
| Origen | <ul style="list-style-type: none"> • ÉXITO: 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 el `x-amz-replication-status` encabezado.

Información relacionada

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

Restauración DE objetos posterior

Puede usar la solicitud DE restauración DE objetos POST de S3 PARA restaurar un objeto almacenado en un pool de almacenamiento en cloud.

Tipo de solicitud admitido

StorageGRID solo admite solicitudes POSTERIORES a la restauración de objetos para restaurar un objeto. No admite la `SELECT` tipo de restauración. Seleccione solicitudes de devolución `XNotImplemented`.

Creación de versiones

Opcionalmente, especifique `versionId` para restaurar una versión específica de un objeto en un bloque con versiones. Si no especifica `versionId`, se restaura la versión más reciente del objeto

Comportamiento de la restauración POSTERIOR de objetos en objetos de Pool de almacenamiento en cloud

Si un objeto se ha almacenado en un Cloud Storage Pool (consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información), una solicitud POSTERIOR de restauración de objetos tiene el siguiente comportamiento, en función del estado del objeto. Consulte «'HEAD Object'» para obtener más información.



Si un objeto se almacena en un Cloud Storage Pool y existen también una o varias copias del objeto en la cuadrícula, no es necesario restaurar el objeto mediante la emisión de una solicitud DE restauración DE objetos POSTERIOR. En su lugar, la copia local se puede recuperar directamente, utilizando UNA solicitud GET Object.

| Estado del objeto | Comportamiento DE la restauración POSTERIOR de objetos |
|--|---|
| 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 han realizado cambios. Nota: Antes de que un objeto haya pasado a un estado no recuperable, no puedes cambiarlo <code>expiry-date</code> . |
| Objeto que ha pasado a un estado no recuperable | 202 Accepted Restaura una copia recuperable del objeto en el Pool de almacenamiento en la nube durante la cantidad de días especificada en el cuerpo de la solicitud. Al final de este período, el objeto se devuelve a un estado no recuperable. Opcionalmente, utilice la <code>Tier</code> solicitar elemento para determinar cuánto tiempo tardará el trabajo de restauración en finalizar (Expedited, Standard, o Bulk). Si no especifica <code>Tier</code> , la Standard se utiliza el nivel. Importante: Si un objeto ha sido trasladado a S3 Glacier Deep Archive o el Cloud Storage Pool utiliza almacenamiento de Azure Blob, no puede restaurarlo con el Expedited nivel. Se devuelve el siguiente error 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class. |

| Estado del objeto | Comportamiento DE la restauración POSTERIOR de objetos |
|--|--|
| 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, usted puede cambiar su <code>expiry-date</code> Volviendo a emitir la solicitud DE restauración DE objeto POSTERIOR con un nuevo valor para <code>Days</code> . La fecha de restauración se actualiza en relación con la hora de la solicitud. |

Información relacionada

["Gestión de objetos con ILM"](#)

["OBJETO HEAD"](#)

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

OBJETO PUT

Puede usar la solicitud PUT Object de S3 para añadir un objeto a un bloque.

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 *recomendado* para una única operación PUT Object 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.

El tamaño máximo de *soportado* para una única operación PUT Object es de 5 TiB (5.497.558.138.880 bytes). Sin embargo, la alerta * S3 PUT Object size demasiado grande* se activará si intenta cargar un objeto que supere los 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 PUT, PUT Object-Copy, GET y HEAD se realizan correctamente si los metadatos definidos por el usuario incluyen caracteres UTF-8 que se han escapado.
- StorageGRID no devuelve el `x-amz-missing-meta` encabezado si el valor interpretado del nombre o valor de 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`

Al especificar `aws-chunked` para `Content-Encoding` StorageGRID no verifica los siguientes elementos:

- StorageGRID no verifica el `chunk-signature` contra los datos del fragmento.
- StorageGRID no verifica el valor indicado para `x-amz-decoded-content-length` contra el objeto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

La codificación de transferencia con `chunked` es compatible si `aws-chunked` también se utiliza la firma de carga útil.

- `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
```

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 las opciones equilibradas o estrictas para el comportamiento de ingesta. 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:

- La `x-amz-acl` no se admite el encabezado de la solicitud.
- La `x-amz-website-redirect-location` el encabezado de la solicitud no es compatible y devuelve `XNotImplemented`.

Opciones para clase de almacenamiento

La `x-amz-storage-class` se admite el encabezado de la solicitud. El valor enviado para `x-amz-storage-class` Afecta la forma en que StorageGRID protege los datos de objetos durante el procesamiento

y no cuántas copias persistentes del objeto se almacenan en el sistema StorageGRID (determinado por ILM).

Si la regla de ILM que coincide con un objeto ingerido utiliza la opción estricta para el comportamiento de la ingesta, la `x-amz-storage-class` el 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 objeto especificadas en la regla de ILM (ubicación síncrona), la `x-amz-storage-class` el 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. La `REDUCED_REDUNDANCY` Se recomienda utilizar la opción cuando la regla de ILM que coincide con el objeto crea una única copia replicada. En este caso, utilizar `REDUCED_REDUNDANCY` elimina la creación y eliminación innecesarias de una copia de objetos adicional en cada operación de procesamiento.

Con el `REDUCED_REDUNDANCY` la opción no se recomienda en otras circunstancias.

`REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante el procesamiento. 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.

Especificando `REDUCED_REDUNDANCY` sólo afecta al número de copias que se crean cuando un objeto se ingiere por primera vez. No afecta al número de copias del objeto que se realizan cuando el objeto se evalúa mediante la política de ILM activa y no provoca que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID.



Si va a procesar un objeto en un bloque con el bloqueo de objetos S3 habilitado, el `REDUCED_REDUNDANCY` opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el `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`
- **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 la 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 el control de versiones está habilitado para un bloque, un valor único `versionId` se genera automáticamente para la versión del objeto almacenado. Este `versionId` también se devuelve en la respuesta mediante el `x-amz-version-id` encabezado 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

Cuando utilice la `Authorization` Encabezado Para autenticar solicitudes, StorageGRID difiere de AWS de las siguientes maneras:

- StorageGRID no requiere `host` cabeceras que se incluirán en `CanonicalHeaders`.
- StorageGRID no requiere `Content-Type` para ser incluido dentro de `CanonicalHeaders`.
- StorageGRID no requiere `x-amz-*` cabeceras que se incluirán en `CanonicalHeaders`.



Como práctica recomendada general, incluya siempre estos encabezados en él `CanonicalHeaders`. Para asegurarse de que se verifican; sin embargo, si excluye estas cabeceras, 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"](#)

["Operaciones en bloques"](#)

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

["Cómo se pueden configurar las conexiones de clientes"](#)

PONER objeto: Copiar

Puede usar la solicitud PUT Object - Copy de S3 para crear una copia de un objeto que ya está almacenado en S3. UNA operación PONER objeto - copia es la misma que realizar UNA GET y LUEGO UN PUT.

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 *recomendado* para una única operación PUT Object 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.

El tamaño máximo de *soportado* para una única operación PUT Object es de 5 TiB (5.497.558.138.880 bytes). Sin embargo, la alerta * S3 PUT Object size demasiado grande* se activará si intenta cargar un objeto que supere los 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 el `x-amz-missing-meta` encabezado si el valor interpretado del nombre o valor de 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 predeterminado es COPY, que permite copiar el objeto y los metadatos asociados.

Puede especificar REPLACE para sobrescribir los metadatos existentes al copiar el objeto o actualizar los metadatos del objeto.

- x-amz-storage-class
- x-amz-tagging-directive: El valor predeterminado es COPY, que le permite copiar el objeto y todas las etiquetas.

Puede especificar REPLACE para sobrescribir las etiquetas existentes al copiar el objeto o actualizar 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-website-redirect-location

Opciones para clase de almacenamiento

La `x-amz-storage-class` Se admite el encabezado de la solicitud y afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente especifica un comportamiento de ingesta de COMMIT doble o de equilibrado.

- 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 va a procesar un objeto en un bloque con el bloqueo de objetos S3 habilitado, el REDUCED_REDUNDANCY opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el 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 PUT Object - Copy

Si el bloque de origen y la clave, especificados en la `x-amz-copy-source` header, 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` el encabezado 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 se puede utilizar PUT Object - Copy 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` cabecera o la `x-amz-server-side-encryption-customer-algorithm` Encabezamiento, 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 utiliza cifrado del servidor, los encabezados de solicitud que proporcione dependerán de si el objeto de origen está cifrado y de si planea cifrar el objeto de destino.

- Si el objeto de origen se cifra utilizando una clave proporcionada por el cliente (SSE-C), debe incluir los tres encabezados siguientes en LA solicitud PUT Object - Copy, para que el objeto se pueda descifrar y copiar a continuación:
 - `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 cuando creó 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 DE PUT Object - Copy:
 - `x-amz-server-side-encryption`



La `server-side-encryption` no se puede actualizar el valor del objeto. En su lugar, haga una copia con un nuevo `server-side-encryption` valor con `x-amz-metadata-directive: REPLACE`.

Creación de versiones

Si se crea una versión del contenedor de origen, puede utilizar `x-amz-copy-source` encabezado para copiar la versión más reciente de un objeto. Para copiar una versión específica de un objeto, debe especificar explícitamente la versión que desea copiar mediante `versionId` subrecurso. Si se crea una versión del bloque de destino, la versión generada se devuelve en el `x-amz-version-id` encabezado de respuesta. Si se suspende el control de versiones para el bloque de destino, entonces `x-amz-version-id` devuelve un valor «null».

Información relacionada

["Gestión de objetos con ILM"](#)

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

["OBJETO PUT"](#)

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 ["Documentación de AWS para SelectObjectContent"](#).

Antes de empezar

- La cuenta de inquilino tiene el permiso de S3 Select.
- Ya tienes `s3:GetObject` permiso para el objeto al 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.



No se admite el uso de ScanRange.

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 a consultar, SUB-EST2020_ALL.csv, mire como esto:

```
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, mire como esto:

```
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
```

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

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 exceder 1,000 cargas simultáneas de varias partes en un solo bloque, ya que los resultados de List Multipart cargan consultas para ese bloque pueden 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 procesa, y para el objeto como un todo cuando se completa la carga de varias partes, si la regla de ILM utiliza el comportamiento de ingesta equilibrado o estricto. Debe saber cómo afecta esto a la ubicación de objetos y piezas:
 - Si ILM cambia mientras se carga varias partes de S3, es posible que cuando la carga de varias partes completa algunas partes del objeto no cumplan los requisitos actuales de ILM. Cualquier pieza que no se haya colocado correctamente se coloca en la cola de reevaluación de ILM y se mueve posteriormente 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 en DC1 mientras que todos los objetos más pequeños se almacenan en DC2, al ingerir cada parte de 1 GB de una carga multiparte de 10 partes se almacena en DC2. Cuando se evalúa ILM para el objeto como un todo, todas las partes del objeto se mueven a DC1.

- Todas las operaciones de carga de varias partes admiten controles de coherencia de StorageGRID.
- Según sea necesario, puede utilizar el cifrado del servidor con cargas en varias partes. Para usar SSE (cifrado en el servidor con claves gestionadas por StorageGRID), incluye el `x-amz-server-side-encryption`. Solicite el encabezado sólo en la solicitud Iniciar carga de varias partes. Para utilizar SSE-C (cifrado del servidor con claves proporcionadas por el cliente), debe especificar los mismos tres encabezados de solicitud de clave de cifrado en la solicitud de carga de varias partes iniciada y en cada solicitud de artículo de carga posterior.

| Funcionamiento | Implementación |
|----------------------------------|--|
| Enumerar cargas de varias partes | Consulte "Enumerar cargas de varias partes" |
| Inicie la carga de varias partes | Consulte "Inicie la carga de varias partes" |
| Cargar artículo | Consulte "Cargar artículo" |
| Cargar pieza: Copiar | Consulte "Cargar pieza: Copiar" |
| Completar carga de varias partes | Consulte "Completar carga de varias partes" |
| Cancelar carga de varias partes | Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones. |
| Enumerar piezas | Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones. |

Información relacionada

- ["Controles de consistencia"](#)
- ["Usar cifrado del servidor"](#)

Enumerar cargas de varias partes

La operación List Multipart carga enumera 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. Cuando se realiza la operación de carga de varias partes completa, ese es el punto en el que se crean objetos (y se crean versiones si procede).

Inicie la carga de varias partes

La operación Iniciar carga de varias partes (`CreateMultipartUpload`) inicia una carga de varias partes para un objeto y devuelve un ID de carga.

La `x-amz-storage-class` se admite el encabezado de la solicitud. El valor enviado para `x-amz-storage-class` Afecta la forma en que StorageGRID protege los datos de objetos durante el procesamiento y no cuántas copias persistentes del objeto se almacenan en el sistema StorageGRID (determinado por ILM).

Si la regla de ILM que coincide con un objeto ingerido utiliza la opción estricta para el comportamiento de la ingesta, la `x-amz-storage-class` el 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 objeto especificadas en la regla de ILM (ubicación síncrona), la `x-amz-storage-class` el 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. La `REDUCED_REDUNDANCY` Se recomienda utilizar la opción cuando la regla de ILM que coincide con el objeto crea una única copia replicada. En este caso, utilizar `REDUCED_REDUNDANCY` elimina la creación y eliminación innecesarias de una copia de objetos adicional en cada operación de

procesamiento.

Con el `REDUCED_REDUNDANCY` la opción no se recomienda en otras circunstancias.

`REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante el procesamiento. 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.

Especificando `REDUCED_REDUNDANCY` sólo afecta al número de copias que se crean cuando un objeto se ingiere por primera vez. No afecta al número de copias del objeto que se realizan cuando el objeto se evalúa mediante la política de ILM activa y no provoca que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID.



Si va a procesar un objeto en un bloque con el bloqueo de objetos S3 habilitado, el `REDUCED_REDUNDANCY` opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Se admiten los siguientes encabezados de solicitud:

- `Content-Type`
- `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
```

Valor para `creation-time` Se evalúa como segundos desde el 1 de enero de 1970.



Adición `creation-time` Como metadatos definidos por el usuario no se permite si va a agregar un objeto a un bloque que tiene la conformidad heredada habilitada. 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 información sobre cómo StorageGRID trata los caracteres UTF-8, consulte la documentación de PUT Object.

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 Iniciar carga de varias partes si desea cifrar el objeto con una clave única gestionada por StorageGRID. No especifique esta cabecera en ninguna de las solicitudes de carga de artículos.
 - x-amz-server-side-encryption
- **SSE-C:** Utilice los tres encabezados de la solicitud de carga de varias partes iniciada (y en cada solicitud de artículo de carga posterior) si desea cifrar el objeto con una clave única que proporciona y gestiona.
 - x-amz-server-side-encryption-customer-algorithm: Especificar AES256.
 - x-amz-server-side-encryption-customer-key: Especifique la 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

El siguiente encabezado de solicitud no es compatible y devuelve XNotImplemented

- x-amz-website-redirect-location

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 crean versiones si corresponde) cuando se realiza la operación de carga de varias partes completa.

Información relacionada

["Gestión de objetos con ILM"](#)

["OBJETO PUT"](#)

Cargar artículo

La operación cargar pieza carga una pieza en una carga de varias partes para un objeto.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- Content-Length
- Content-MD5

Solicitar encabezados para el cifrado del servidor

Si ha especificado el cifrado SSE-C para la solicitud de carga de varias partes iniciada, también debe incluir los siguientes encabezados de solicitud en cada solicitud de artículo de carga:

- 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 Iniciar carga de varias partes.
- x-amz-server-side-encryption-customer-key-MD5: Especifique el mismo resumen MD5 que ha proporcionado en la solicitud Iniciar carga de varias partes.



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 que se incluyen en el apartado «"usar cifrado en el 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 crean versiones si corresponde) cuando se realiza la operación de carga de varias partes completa.

Información relacionada

["Usar cifrado del servidor"](#)

Cargar pieza: Copiar

La operación cargar pieza - Copiar carga una parte de un objeto copiando datos de un objeto existente como origen de datos.

La operación cargar pieza - copia 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 del objeto especificados en `x-amz-copy-source-range` En 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 ha especificado el cifrado SSE-C para la solicitud de carga de varias partes iniciada, también debe incluir los siguientes encabezados de solicitud en cada parte de carga - solicitud de copia:

- `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 Iniciar carga de varias partes.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el mismo resumen MD5 que ha proporcionado en la solicitud Iniciar carga de varias partes.

Si el objeto de origen se cifra utilizando una clave proporcionada por el cliente (SSE-C), debe incluir los tres encabezados siguientes en la solicitud cargar pieza - Copiar, para que el objeto se pueda descifrar y copiar a continuación:

- `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 cuando creó 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 que se incluyen en el apartado «"usar cifrado en el 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 crean versiones si corresponde) cuando se realiza la operación de carga de varias partes completa.

Completar carga de varias partes

La operación de carga de varias partes completa completa finaliza una carga de varias partes de un objeto mediante el montaje de las piezas previamente cargadas.

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.

Solicitar encabezados

La `x-amz-storage-class` Se admite el encabezado de la solicitud y afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente especifica un comportamiento de ingesta de COMMIT doble o de equilibrado.

- 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 va a procesar un objeto en un bloque con el bloqueo de objetos S3 habilitado, el REDUCED_REDUNDANCY opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el 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.



La ETag El valor devuelto no es una suma MD5 de los datos, sino que sigue a la implementación de API de Amazon S3 de ETag valor para objetos de varias piezas.

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 el control de versiones está habilitado para un bloque, un valor único `versionId` se genera automáticamente para la versión del objeto almacenado. Este `versionId` también se devuelve en la respuesta mediante el `x-amz-version-id` encabezado 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.

Si esto ocurre, se genera una alarma en el administrador de grid en eventos totales (SMTT). El mensaje Last Event muestra "error al publicar notificaciones para la clave de objeto de nombre de bloque" del último objeto cuya notificación ha fallado. (Para ver este mensaje, seleccione **NODES > Storage Node > Events**. Ver último evento en la parte superior de la tabla). Los mensajes de eventos también se muestran en la `/var/local/log/bycast-err.log`.

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.

Información relacionada

["Gestión de objetos con ILM"](#)

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 |

| Nombre | Estado de HTTP |
|---------------------------------|------------------------------------|
| InvalidArgument | 400 solicitud incorrecta |
| InvalidBucketName | 400 solicitud incorrecta |
| InvalidBucketState | 409 conflicto |
| InvalidDigest | 400 solicitud incorrecta |
| InvalidEncryptionAlgorithmError | 400 solicitud incorrecta |
| InvalidPart | 400 solicitud incorrecta |
| 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 |

| Nombre | Estado de HTTP |
|---------------------------------|----------------------------|
| NotImplimed | 501 no implementada |
| NoSuchBucketPolicy | 404 no encontrado |
| ObjectLockConfigurationNotFound | 404 no encontrado |
| Error de preconditionError | Error de condición 412 |
| RequestTimeTooSowed | 403 Prohibido |
| ServiceUnavailable | 503 Servicio no disponible |
| 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 |

| Nombre | Descripción | Estado de HTTP |
|----------------|--|---------------------|
| 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 |

Solicitudes de StorageGRID S3

OBTENGA coherencia de bloques

La solicitud DE consistencia DE GET Bucket permite determinar el nivel de consistencia que se aplica a un bloque determinado.

Los controles de consistencia predeterminados se establecen para garantizar la lectura tras escritura de los objetos recién creados.

Tiene el permiso `s3:GetBucketConsistency`, o bien sea 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 la respuesta XML, `<Consistency>` devolverá uno de los siguientes valores:

| Control de consistencia | 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. |

| Control de consistencia | 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. |

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

["Controles de consistencia"](#)

PONGA la consistencia del cucharón

La solicitud PUT Bucket Consistency permite especificar el nivel de coherencia que se va a aplicar a las operaciones realizadas en un bloque.

Los controles de consistencia predeterminados se establecen para garantizar la lectura tras escritura de los objetos recién creados.

Antes de empezar

Tiene el permiso s3:PutBucketConsistency, o bien sea raíz de la cuenta, para completar esta operación.

Solicitud

La x-ntap-sg-consistency el parámetro debe contener uno de los siguientes valores:

| Control de consistencia | 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. |

| Control de consistencia | Descripción |
|---------------------------------|--|
| 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. |

Nota: en general, se debe utilizar el valor de control de la coherencia "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 el control de consistencia de cada solicitud API. Establecer el control de consistencia a nivel de cucharón únicamente 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

["Controles de consistencia"](#)

HORA de último acceso al bloque DE GET

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.

Tiene el permiso s3:GetBucketLastAccessTime, o sea la raíz de la cuenta, para completar esta operación.

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.

Tiene el permiso `s3:PutBucketLastAccessTime` para que un bloque, o sea la raíz de la cuenta, complete esta operación.



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 habilitar o deshabilitar las actualizaciones para la hora del último acceso mediante la solicitud de hora de último acceso PUT Bucket, la casilla de verificación **S3 > Buckets > Cambiar la configuración del último acceso** en el Administrador de inquilinos o la API de administración de inquilinos.

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 OBTENER objeto, OBTENER ACL de objeto, OBTENER etiquetado de objeto y Objeto de CABECERA no actualizan la última hora de acceso. El objeto no se agrega a las colas para la evaluación de la gestión del ciclo de vida de la información (ILM).
- PUT Object (PONER objeto): Copie y COLOQUE las solicitudes de etiquetado de objetos que sólo actualizan los metadatos. También actualice la hora del último acceso. El objeto se agrega a las colas para la evaluación de ILM.
- Si las actualizaciones de la hora de último acceso están desactivadas para el bloque de origen, las solicitudes de PUT Object - Copy 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, PONER objeto - Copiar solicitudes siempre actualizar la última hora de acceso.

La copia del objeto se agrega a las colas para la evaluación de ILM.

- Completar solicitudes de carga de varias partes actualizar la última hora de 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
```

Información relacionada

["Usar una cuenta de inquilino"](#)

DELETE bucket metadata notification Configuration

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.

Tiene el permiso `s3:DeleteBucketMetadataNotification` para un bucket, o sea root de la cuenta, para completar esta operación.

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.

Tiene el permiso `s3:GetBucketMetadataNotification` o ser raíz de la cuenta, para completar esta operación.

Ejemplo de solicitud

Esta solicitud recupera la configuración de notificación de metadatos del bloque 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 |
|---------------------------------------|---|-------------|
| MetadataNotificationConfi guration | 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 | <p>Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado.</p> <p>Se rechazan las reglas con prefijos superpuestos.</p> <p>Incluido en el elemento MetadataNotificationConfiguration.</p> | Sí |
| ID | <p>Identificador único de la regla.</p> <p>Incluido en el elemento Regla.</p> | No |
| Estado | <p>El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas.</p> <p>Incluido en el elemento Regla.</p> | Sí |
| Prefijo | <p>Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado.</p> <p>Para hacer coincidir todos los objetos, especifique un prefijo vacío.</p> <p>Incluido en el elemento Regla.</p> | Sí |
| Destino | <p>Etiqueta de contenedor para el destino de una regla.</p> <p>Incluido en el elemento Regla.</p> | Sí |

| Nombre | Descripción | Obligatorio |
|--------|--|-------------|
| No | <p>URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades:</p> <ul style="list-style-type: none"> • es debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en el formulario <code>domain-name/myindex/mytype</code>. <p>Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404.</p> <p>El valor de urn se incluye en el elemento Destination.</p> | Sí |

Ejemplo de respuesta

El XML incluido entre

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags muestra cómo se configura la integración con un extremo de integración de búsqueda para el bloque. En este ejemplo, los metadatos del objeto se envían a un índice de Elasticsearch llamado `current` y escriba `named 2017` Que se aloja en un dominio de AWS llamado `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"](#)

PUT bucket metadata notification Configuration

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.

Tiene el permiso `s3:PutBucketMetadataNotification` para un bloque o ser raíz de la cuenta, para completar esta operación.

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 de los objetos con el prefijo `/images` en un destino y objetos con el prefijo `/videos` a otro.

Las configuraciones que tienen prefijos superpuestos no son válidas y se rechazan cuando se envían. Por ejemplo, una configuración que incluía una regla para objetos con el prefijo `test` y una segunda regla para los objetos con el prefijo `test2` no se permitirá.

Los destinos se deben especificar con el URN de un extremo de StorageGRID. El extremo debe existir cuando

se envía la configuración de notificación de metadatos o la solicitud falla como un 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 |
|---------------------------------------|---|-------------|
| MetadataNotificationConfi guration | 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 | <p>El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas.</p> <p>Incluido en el elemento Regla.</p> | Sí |
| Prefijo | <p>Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado.</p> <p>Para hacer coincidir todos los objetos, especifique un prefijo vacío.</p> <p>Incluido en el elemento Regla.</p> | Sí |
| Destino | <p>Etiqueta de contenedor para el destino de una regla.</p> <p>Incluido en el elemento Regla.</p> | Sí |
| No | <p>URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades:</p> <ul style="list-style-type: none"> • es debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en el formulario <code>domain-name/myindex/mytype</code>. <p>Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404.</p> <p>El valor de urn se incluye en el elemento Destination.</p> | 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, metadatos de objeto para objetos que coinciden con el prefijo `/images` se envía a un destino, mientras que los metadatos de objetos de los objetos que coinciden con el prefijo `/videos` se envía a un segundo destino.

```
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-1:33333333: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 de JSON que se podría generar cuando un objeto con la clave `SGWS/Tagging.txt` se crea en un bloque llamado `test`. La `test` el bloque no tiene versiones, por lo que el `versionId` la etiqueta está vacía.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadatos de objetos incluidos en las notificaciones de metadatos

En la tabla se enumeran todos los campos que se incluyen en el documento JSON que se envían al extremo de destino cuando la integración de búsqueda está habilitada.

El nombre del documento incluye el nombre del bloque, el nombre del objeto y el ID de versión, si existe.

| Tipo | Nombre 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 <code>us-east-1</code> |
| 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 <i>key:value</i> | Todos los metadatos de usuario del objeto, como pares clave-valor |

| Tipo | Nombre del elemento | Descripción |
|-----------|----------------------------|--|
| Etiquetas | etiquetas <i>key:value</i> | 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 puede obtenerse mediante una solicitud DE SERVICIO GET 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.

Tiene 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 la `ObjectCount` y.. `DataBytes` valores en la respuesta. Los marcadores de eliminación no se agregan a la `ObjectCount` total.

Información relacionada

["Controles de consistencia"](#)

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 GET Bucket queda 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 PUT Bucket queda 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: 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.



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.

["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"](#)

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 la solicitud PUT Bucket para cumplir con las normativas a fin de crear un nuevo bloque compatible:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```


Obsoleto: GET Bucket Compliance Request

La solicitud DE cumplimiento GET Bucket queda 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.

["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"](#)

Tiene el permiso `s3:GetBucketCompliance` o ser la raíz de la cuenta para completar esta operación.

Ejemplo de solicitud

Esta solicitud de ejemplo le permite determinar la configuración de cumplimiento para el bloque denominado `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

En la respuesta XML, `<SGCompliance>` enumera 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 | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • 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 bloque no se creó para ser compatible, el código de estado HTTP para la respuesta es 404 Not Found, Con un código de error S3 de XNoSuchBucketCompliance.

Obsoleto: PUT Bucket Compliance Request

La solicitud DE cumplimiento PUT Bucket queda 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.

["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"](#)

Tiene 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 del bloque denominado `mybucket`. En este ejemplo, los objetos de `mybucket` ahora se conservará 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 | <p>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.</p> <p>Importante Al especificar un nuevo valor para <code>RetentionPeriodMinutes</code>, 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.</p> |

| Nombre | Descripción |
|------------------------|--|
| LegalHold | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • 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. |

Nivel de coherencia para la configuración de cumplimiento de normativas

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 el nivel de consistencia **strong-global** para garantizar que todos los sitios de centros de datos y todos los nodos de almacenamiento que contienen metadatos de bloques tengan coherencia de lectura tras escritura para la configuración de cumplimiento modificada.

Si StorageGRID no puede alcanzar el nivel de consistencia **strong-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 hacer que haya suficientes nodos de almacenamiento en cada sitio disponibles, el soporte técnico puede pedirle que vuelva a intentar la solicitud fallida forzando el nivel de consistencia de **sitio seguro**.



Nunca fuerce el nivel de consistencia de **sitio fuerte** para EL cumplimiento DE LA cuchara DE PUT a menos que usted haya sido dirigido a hacerlo por el soporte técnico y a menos que usted entienda las consecuencias potenciales de usar este nivel.

Cuando el nivel de consistencia se reduce a **sitio seguro**, StorageGRID garantiza que la configuración de cumplimiento actualizada tendrá coherencia de lectura tras escritura sólo para las solicitudes de cliente 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 coloca un bloque bajo una retención legal y fuerza un nivel de coherencia más bajo, la configuración de cumplimiento anterior del bloque (es decir, la retención legal) puede seguir vigente en algunos centros 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 del nivel de consistencia de **sitio fuerte**, vuelva a emitir la solicitud DE cumplimiento DE PUT Bucket e incluya el Consistency-Control 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 bloque no se creó 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 bloque, el código de estado HTTP es 400 Bad Request.

Información relacionada

"[Obsoleto: PONGA modificaciones de solicitud de cucharón para el cumplimiento](#)"

Políticas de acceso a bloques y grupos

Utilice las políticas de acceso de bloques y grupos

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

Existen dos tipos de políticas de acceso compatibles con StorageGRID.

- **Políticas de bloque**, que se configuran mediante las operaciones API Get Bucket, PUT Bucket y DELETE Bucket Policy S3. 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.



No hay ninguna diferencia de prioridad entre las políticas de grupo y de bloque.

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 | <p>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.</p> <p>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.</p> |
| 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": "*"

```

En el ejemplo siguiente, la instrucción utiliza los elementos Effect, Principal, Acción y recurso. En este ejemplo se muestra una sentencia de directiva de bloque completa que utiliza el efecto "permitir" para dar a los principales, el grupo admin `federated-group/admin` y el grupo financiero `federated-group/finance`, Permisos para realizar la acción `s3:ListBucket` en el bloque llamado `mybucket` Y la Acción `s3:GetObject` en todos los objetos dentro de ese cucharón.

```
{
  "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:iam:s3::mybucket",
        "arn:aws:iam: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.

Configuración de control de coherencia para políticas

De forma predeterminada, cualquier actualización que realice a las directivas de grupo será consistente. Una vez que la política de grupo sea coherente, los cambios pueden tardar 15 minutos más en aplicarse, debido al almacenamiento en caché de políticas. De forma predeterminada, las actualizaciones que realice en las políticas de bloques también serán coherentes.

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 se convierta en una Lo antes posible. efectiva por motivos de seguridad.

En este caso, puede ajustar la `Consistency-Control` En la solicitud DE política PUT Bucket, o puede utilizar la solicitud DE consistencia PUT Bucket. Al cambiar el control de coherencia para esta solicitud, debe utilizar el valor **all**, que ofrece la mayor garantía de coherencia de lectura tras escritura. Si especifica cualquier otro valor de control de consistencia en un encabezado para LA solicitud DE consistencia PUT Bucket, la solicitud será rechazada. Si especifica cualquier otro valor para una solicitud DE política PUT Bucket, el valor se ignorará. Una vez que una política de bloques se vuelve coherente, los cambios pueden tardar 8 segundos más en aplicarse, debido al almacenamiento en caché de la política.



Si establece el nivel de consistencia en **all** para forzar la aplicación de una nueva política de cucharón antes, asegúrese de volver a establecer el control de nivel de cucharón en su valor original cuando haya terminado. De lo contrario, todas las solicitudes de segmentos futuras utilizarán la configuración **all**.

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 solicitud HTTP para la operación DE política PUT Bucket debe codificarse 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, el elemento denota los recursos Resource`o bien, `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 directores son denotados por el elemento «'Principal,'» o «'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 el nombre de usuario `Alex` se ha eliminado. Si un nuevo Alex se une a la organización y se le asigna la misma `Alex` nombre de usuario, es posible que el nuevo usuario herede sin querer los permisos concedidos 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 utiliza ahora el permiso `s3:PutReplicationConfiguration` para LAS acciones de replicación PUT y DELETE Bucket. StorageGRID utiliza permisos independientes para cada acción, que coinciden con la especificación original de Amazon S3.



SE realiza UNA ELIMINACIÓN cuando se utiliza UNA PUESTA para sobrescribir un valor existente.

Permisos que se aplican a los bloques

| Permisos | OPERACIONES DE LA API DE REST DE S3 | Personalizado para StorageGRID |
|---------------------------------|-------------------------------------|--------------------------------|
| <code>s3:CreateBucket</code> | COLOQUE el cucharón | |
| <code>s3>DeleteBucket</code> | ELIMINAR bloque | |

| Permisos | OPERACIONES DE LA API DE REST DE S3 | Personalizado para StorageGRID |
|-------------------------------------|---|--|
| s3:DeleteBucketMetadataNotification | DELETE bucket metadata notification Configuration | Sí |
| s3:DeleteBucketPolicy | ELIMINE la política de bloques | |
| s3:DeleteReplicationConfiguration | DELETE Bucket replicación | Sí, separe los permisos PARA PUT y DELETE* |
| s3:GetBucketAcl | GET Bucket ACL | |
| s3:GetBucketCompliance | CUMPLIMIENTO de LA normativa GET Bucket (obsoleto) | Sí |
| s3:GetBucketConsistency | OBTENGA coherencia de bloques | Sí |
| s3: GetBucketCORS | OBTENGA los cors del cucharón | |
| s3:GetEncryptionConfiguration | OBTENGA el cifrado de bloque | |
| s3:GetBucketLastAccessTime | HORA de último acceso al bloque DE GET | Sí |
| s3:GetBucketLocation | OBTENER ubicación de bloque | |
| s3:GetBucketMetadataNotification | OBTENGA la configuración de notificación de metadatos del bloque de datos | Sí |
| s3:GetBucketNotification | OBTENGA la notificación DE BUCKET | |
| s3:GetBucketObjectLockConfiguration | OBTENER configuración de bloqueo de objeto | |
| s3:GetBucketPolicy | OBTENGA la política de bloques | |
| s3:GetBucketTagging | GET Bucket tagging | |
| s3:GetBucketVersioning | OBTENGA el control de versiones de Bucket | |
| s3:GetLifecycleConfiguration | OBTENGA el ciclo de vida de la cuchara | |
| s3:GetReplicationConfiguration | OBTENGA la replicación de Bucket | |

| Permisos | OPERACIONES DE LA API DE REST DE S3 | Personalizado para StorageGRID |
|-------------------------------------|---|--|
| s3:ListAllMyBuckets | <ul style="list-style-type: none"> • OBTENER servicio • Obtenga el uso del almacenamiento | Sí, PARA OBTENER el uso del almacenamiento |
| s3:ListBucket | <ul style="list-style-type: none"> • GET Bucket (objetos de lista) • Cubo DE CABEZA • Restauración DE objetos posterior | |
| s3:ListBucketMultipartUploads | <ul style="list-style-type: none"> • Enumerar cargas de varias partes • Restauración DE objetos posterior | |
| 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 | <ul style="list-style-type: none"> • ELIMINAR los segmentos de cucharón† • COLOQUE los cors del cucharón | |
| s3:PutEncryptionConfiguration | <ul style="list-style-type: none"> • DELETE Bucket Encryption • PUT Bucket Encryption | |
| s3:PutBucketLastAccessTime | PUT Bucket última hora de acceso | Sí |
| s3:PutBucketMetadataNotification | PUT bucket metadata notification Configuration | Sí |
| s3:PutBucketNotification | NOTIFICACIÓN DE PUT Bucket | |
| s3:PutBucketObjectLockConfiguration | <ul style="list-style-type: none"> • COLOQUE el cucharón con el x-amz-bucket-object-lock-enabled: true Encabezado de solicitud (también requiere el permiso s3:CreateBucket) • PONER configuración de bloqueo de objeto | |
| s3:PutBucketPolicy | POLÍTICA DE PUT Bucket | |

| Permisos | OPERACIONES DE LA API DE REST DE S3 | Personalizado para StorageGRID |
|--------------------------------|---|--|
| s3:PutBucketEtiquetado | <ul style="list-style-type: none"> • ELIMINAR etiquetado de bloque† • PUT Bucket etiquetaje | |
| s3:PutBucketVersioning | PONER creación de versiones de bloques | |
| s3:PutLifecycleConfiguration | <ul style="list-style-type: none"> • ELIMINAR ciclo de vida del cucharón† • CICLO de vida DE la cuchara | |
| s3:PutReplicationConfiguration | PUT Bucket replication | 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 | <ul style="list-style-type: none"> • Cancelar carga de varias partes • Restauración DE objetos posterior | |
| s3:BypassGovernanceRetention | <ul style="list-style-type: none"> • ELIMINAR objeto • ELIMINAR varios objetos • PUT Object retention | |
| s3>DeleteObject | <ul style="list-style-type: none"> • ELIMINAR objeto • ELIMINAR varios objetos • Restauración DE objetos posterior | |
| s3>DeleteObjectTagging | ELIMINAR etiquetado de objetos | |
| s3>DeleteObjectVersionTagging | ELIMINAR etiquetado de objetos (una versión específica del objeto) | |
| s3>DeleteObjectVersion | ELIMINAR objeto (una versión específica del objeto) | |
| s3:GetObject | <ul style="list-style-type: none"> • OBTENER objeto • OBJETO HEAD • Restauración DE objetos posterior • SELECCIONE Contenido de objeto | |

| Permisos | OPERACIONES DE LA API DE REST DE S3 | Personalizado para StorageGRID |
|-------------------------------|--|--------------------------------|
| s3:GetObjectAcl | OBTENER ACL de objeto | |
| s3:GetObjectLegalHold | OBTENER retención legal de objetos | |
| s3:GetObjectRetention | OBTENGA retención de objetos | |
| s3:GetObjectTagging | OBTENER etiquetado de objetos | |
| s3:GetObjectVersionTagging | OBTENER etiquetado de objetos (una versión específica del objeto) | |
| s3:GetObjectVersion | GET Object (una versión específica del objeto) | |
| s3:ListMultipartUploadParts | Elementos de lista, restauración POSTERIOR al objeto | |
| s3:PutObject | <ul style="list-style-type: none"> • OBJETO PUT • PONER objeto: Copiar • Restauración DE objetos posterior • Inicie la carga de varias partes • Completar carga de varias partes • Cargar artículo • Cargar pieza: Copiar | |
| s3:PutObjectLegalHold | PONER objeto legal | |
| s3:PutObjectRetention | PUT Object retention | |
| s3:PutObjectEtiquetado | PONER etiquetado de objetos | |
| s3:PutObjectVersionEtiquetado | PONER etiquetado de objetos (una versión específica del objeto) | |
| s3:PutOverwriteObject | <ul style="list-style-type: none"> • OBJETO PUT • PONER objeto: Copiar • PUT Object tagging • ELIMINAR etiquetado de objetos • Completar carga de varias partes | Sí |
| s3:RestoreObject | Restauración DE objetos posterior | |

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 se habilita el control de versiones de S3, la configuración Denegar evita QUE LAS operaciones PUT Object tagging o DELETE Object tagging modifiquen el conjunto de etiquetas 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 directiva S3 actual permite la sobrescritura y el permiso PutOverwriteObject se establece en Deny, 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 **Evitar modificación de cliente** está seleccionada (**CONFIGURACIÓN > Ajustes 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 * y ? caracteres comodín. |
| StringNotLike | Compara una clave con un valor de cadena basado en la coincidencia negada (distingue entre mayúsculas y minúsculas). Puede incluir * y ? caracteres comodín. |
| 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. |

| Operadores de condición | Descripción |
|--------------------------|--|
| NumericGreaterthan | Compara una clave con un valor numérico basado en la coincidencia "mayor que". |
| NumericGreaterThanEquals | Compara una clave con un valor numérico basado en la coincidencia "mayor que o igual". |
| NumericLessThan | Compara una clave con un valor numérico basado en la coincidencia "less than". |
| NumericLessThanEquals | Compara una clave con un valor numérico basado en la coincidencia "menor que o igual". |
| 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. |

Teclas de condición compatibles

| Categoría | Teclas de condición aplicables | Descripción |
|-------------------|--------------------------------|---|
| Operadores IP | aws:SourceIp | <p>Comparará con la dirección IP desde la que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos.</p> <p>Nota: Si la solicitud S3 se envió a través del servicio Load Balancer en nodos Admin y nodos de Puertas de enlace, se comparará con la dirección IP anterior al servicio Load Balancer.</p> <p>Nota: Si se utiliza un equilibrador de carga no transparente de terceros, se comparará con la dirección IP de ese equilibrador de carga. Cualquiera X-Forwarded-For el encabezado se ignorará porque no se puede determinar su validez.</p> |
| Recurso/identidad | aws:nombre de usuario | Comparará con el nombre de usuario del remitente desde el que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos. |

| Categoría | Teclas de condición aplicables | Descripción |
|---|--|---|
| s3:ListBucket y. s3:ListBucketVersions permisos | s3:delimitador | Comparará con el parámetro delimitador especificado en una solicitud GET Bucket o GET Bucket Object Versions. |
| s3:ListBucket y. s3:ListBucketVersions permisos | s3:max-keys | Comparará con el parámetro max-keys especificado en una solicitud GET Bucket o GET Bucket Object Versions. |
| s3:ListBucket y. s3:ListBucketVersions permisos | s3:prefijo | Se comparará con el parámetro prefix especificado en una solicitud GET Bucket o GET Bucket Object Versions. |
| s3:PutObject | s3:retención-días restante del bloqueo de objetos | <p>Compara con la fecha de retención hasta especificada en x-amz-object-lock-retain-until-date cabecera de solicitud o calculada desde el período de retención predeterminado de bloque para asegurarse de que estos valores están dentro del intervalo permitido para las siguientes solicitudes:</p> <ul style="list-style-type: none"> • OBJETO PUT • PONER objeto: Copiar • Inicie la carga de varias partes |
| s3:PutObjectRetention | s3:retención-días restante del bloqueo de objetos | Compara con la fecha de retención especificada en la solicitud DE RETENCIÓN DE objeto PUT para garantizar que se encuentra dentro del intervalo permitido. |

Especifique las variables en una política

Las variables de las directivas se pueden utilizar para rellenar la información de directivas cuando esté disponible. Se pueden usar variables de política en la `Resource` comparaciones entre elementos y cadenas en la `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 |
|-------------------------------|--|
| <code>\${aws:SourceIp}</code> | Utiliza la clave SourceIp como la variable proporcionada. |
| <code>\${aws:username}</code> | Utiliza la clave de nombre de usuario como la variable proporcionada. |
| <code>\${s3:prefix}</code> | Utiliza la clave de prefijo específica del servicio como variable proporcionada. |
| <code>\${s3:max-keys}</code> | Utiliza la clave de max-keys específica del servicio como la variable proporcionada. |
| <code>\${*}</code> | Carácter especial. Utiliza el carácter como carácter literal *. |
| <code>\${?}</code> | Carácter especial. Utiliza el carácter como literal ? carácter. |
| <code>\${\$}</code> | 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 |

| Descripción de la política | Tipo de política | Comportamiento de Amazon | Comportamiento de StorageGRID |
|---|-------------------------|--|--|
| 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 |
| La directiva otorga a una cuenta que no es 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:

- En Grid Manager, vaya a **CONFIGURACIÓN > SEGURIDAD > CONFIGURACIÓN DE SEGURIDAD > RED AND OBJECTS** 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.
 - Añada una operación **PUT Object ALLOW** a la política de S3.



Al establecer **DeleteObject** en **DENEGAR** en una directiva S3, no se impide que ILM elimine objetos cuando existe una regla como "copias cero después de 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"](#)
- ["Gestión de objetos con ILM"](#)
- ["Usar una cuenta de inquilino"](#)

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. Las políticas de bloque se configuran mediante la API de S3 PutBucketPolicy. Consulte ["Operaciones en bloques"](#).

Se puede configurar una política de bloques mediante la CLI de AWS según el siguiente comando:

```
> 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, todos, incluido el anónimo, pueden enumerar objetos en el bloque y realizar operaciones Get Object en todos los objetos del bloque. 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, se permite a todos los integrantes de una cuenta especificada el acceso completo a un bloque, mientras que a todos los miembros de otra cuenta especificada sólo se les permite enumerar el bloque y realizar operaciones GetObject en los objetos del bloque 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 los usuarios, incluido el anónimo, pueden enumerar el bloque y realizar operaciones GET Object en todos los objetos del bloque, mientras que sólo los usuarios que pertenecen al grupo Marketing en la cuenta especificada se permite el 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, el usuario federado Alex tiene permiso de acceso completo al `examplebucket` cucharón 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, la `Deny Effect` para `PutOverwriteObject` y `DeleteObject` garantiza que nadie puede sobrescribir ni 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 existe `Principal` elemento de 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 el pleno acceso sólo a su «carpeta» en un cubo

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}/*"
    }
  ]
}

```

Configure la seguridad de la API DE REST

Debe revisar las medidas de seguridad implementadas para la API REST y entender cómo proteger el sistema.

Cómo proporciona StorageGRID seguridad para la API DE REST

Debe entender cómo el sistema StorageGRID implementa la seguridad, la autenticación y la autorización para la API DE REST.

StorageGRID usa las siguientes medidas de seguridad.

- Las comunicaciones de cliente con el servicio Load Balancer utilizan HTTPS si HTTPS está configurado para el extremo de equilibrio de carga.

Al configurar un extremo de equilibrio de carga, HTTP se puede habilitar opcionalmente. Por ejemplo, puede usar HTTP para pruebas u otros fines que no sean de producción. Consulte las instrucciones para administrar StorageGRID si desea obtener más información.

- De manera predeterminada, StorageGRID utiliza HTTPS para las comunicaciones cliente con los nodos de almacenamiento.

Opcionalmente, HTTP se puede habilitar para estas conexiones. Por ejemplo, puede usar HTTP para pruebas u otros fines que no sean de producción. Consulte las instrucciones para administrar StorageGRID si desea obtener más información.

- Las comunicaciones entre StorageGRID y el cliente se cifran mediante TLS.
- Las comunicaciones entre el servicio Load Balancer y los nodos de almacenamiento de la cuadrícula están cifradas si el extremo de equilibrio de carga está configurado para aceptar conexiones HTTP o HTTPS.
- Los clientes deben proporcionar encabezados de autenticación HTTP a StorageGRID para realizar operaciones de API DE REST.

Certificados de seguridad y aplicaciones cliente

Los clientes pueden conectarse al servicio Load Balancer en los nodos de gateway o de administración, directamente a los nodos de almacenamiento.

En todos los casos, las aplicaciones cliente pueden realizar conexiones TLS mediante un certificado de servidor personalizado cargado por el administrador de grid o un certificado generado por el sistema StorageGRID:

- Cuando las aplicaciones cliente se conectan al servicio Load Balancer, lo hacen utilizando el certificado que se configuró para el extremo de equilibrio de carga específico utilizado para realizar la conexión. Cada extremo tiene su propio certificado, que es un certificado de servidor personalizado cargado por el administrador de grid o un certificado que el administrador de grid generó en StorageGRID al configurar el extremo.
- Cuando las aplicaciones cliente se conectan directamente a un nodo de almacenamiento, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (que están firmados por la entidad de certificación del sistema), o bien, un único certificado de servidor personalizado proporcionado para la cuadrícula por un administrador de grid.

Los clientes deben configurarse para que confíen en la entidad emisora de certificados que firmó el certificado que utilicen para establecer conexiones TLS.

Consulte las instrucciones para administrar StorageGRID para obtener más información sobre la configuración de extremos del balanceador de carga y para obtener instrucciones sobre cómo añadir un único certificado de servidor personalizado para conexiones TLS directamente a nodos de almacenamiento.

Resumen

En la siguiente tabla, se muestra cómo se implementan los problemas de seguridad en las API DE REST de S3 y Swift:

| Problema de seguridad | Implementación de la API DE REST |
|----------------------------|---|
| Seguridad de la conexión | TLS |
| Autenticación del servidor | Certificado de servidor X.509 firmado por CA del sistema o certificado de servidor personalizado suministrado por el administrador |
| Autenticación de clientes | <ul style="list-style-type: none"> • S3: Cuenta de S3 (ID de clave de acceso y clave de acceso secreta) • Swift: Cuenta de Swift (nombre de usuario y contraseña) |

| Problema de seguridad | Implementación de la API DE REST |
|-------------------------|---|
| Autorización de cliente | <ul style="list-style-type: none"> • S3: Propiedad de bloque y todas las políticas de control de acceso aplicables • Swift: Acceso a roles de administrador |

Información relacionada

["Administre StorageGRID"](#)

Algoritmos de cifrado y hash compatibles para bibliotecas TLS

El sistema StorageGRID admite un conjunto limitado de conjuntos de cifrado que las aplicaciones cliente pueden utilizar al establecer una sesión de seguridad de la capa de transporte (TLS). Para configurar los cifrados, vaya a **CONFIGURACIÓN > SEGURIDAD > CONFIGURACIÓN DE SEGURIDAD** y seleccione **Políticas TLS y SSH**.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3.



SSLv3 y TLS 1.1 (o versiones anteriores) ya no son compatibles.

Información relacionada

["Configure las conexiones y las cuentas de inquilino"](#)

Supervisar y auditar operaciones

Supervise las tasas de procesamiento y recuperación de objetos

Es posible supervisar las tasas de procesamiento y recuperación de objetos, así como las métricas para el número de objetos, consultas y verificación. Puede ver el número de intentos fallidos y correctos por las aplicaciones cliente para leer, escribir y modificar objetos en el sistema StorageGRID.

Pasos

1. Inicie sesión en Grid Manager mediante una ["navegador web compatible"](#).
2. En el panel de control, seleccione **Rendimiento > S3 operaciones** o **Rendimiento > Operaciones Swift**.

En esta sección se resume el número de operaciones de cliente que realiza su sistema StorageGRID. La media de las tasas de protocolo se hace durante los últimos dos minutos.

3. Seleccione **NODES**.
4. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **Load Balancer**.

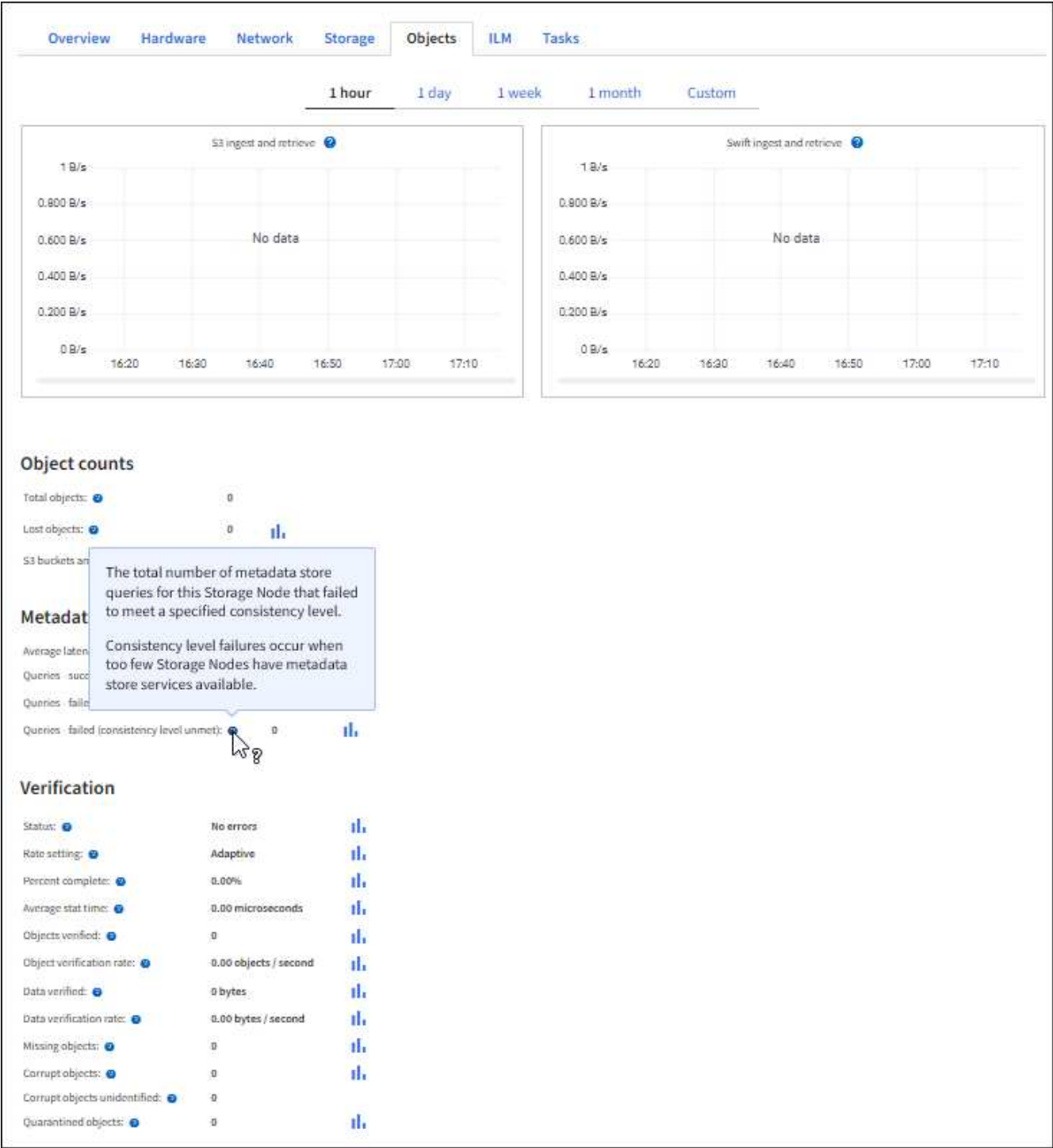
Los gráficos muestran tendencias para todo el tráfico de cliente dirigido a los extremos de equilibrador de carga dentro de la cuadrícula. Es posible seleccionar un intervalo de tiempo en horas, días, semanas, meses o años. también puede aplicar un intervalo personalizado.

5. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **objetos**.

El gráfico muestra las tasas de procesamiento y recuperación de todo el sistema StorageGRID en bytes por segundo y bytes totales. Es posible seleccionar un intervalo de tiempo en horas, días, semanas, meses o años. también puede aplicar un intervalo personalizado.

6. Para ver información sobre un nodo de almacenamiento en particular, seleccione el nodo en la lista de la izquierda y haga clic en la ficha **objetos**.

El gráfico muestra las tasas de procesamiento y recuperación de objetos de este nodo de almacenamiento. La pestaña también incluye métricas para el recuento de objetos, consultas y verificación. Puede hacer clic en las etiquetas para ver las definiciones de estas métricas.



7. Si desea aún más detalles:

- a. Seleccione **SUPPORT > Tools > Topología de cuadrícula**.
- b. Seleccione **síte > Descripción general > Principal**.

La sección API Operations muestra información resumida de la cuadrícula completa.

- c. Seleccione **Storage Node > LDR > Client Application > Overview > Main**

La sección Operaciones muestra información de resumen del nodo de almacenamiento seleccionado.

Acceder y revisar registros de auditoría

Los servicios de StorageGRID generan los mensajes de auditoría y se almacenan en archivos de registro de texto. Los mensajes de auditoría específicos de API de los registros de auditoría ofrecen datos críticos de seguridad, operación y supervisión del rendimiento que pueden ayudar a evaluar el estado del sistema.

Antes de empezar

- Tiene permisos de acceso específicos.
- Usted tiene la `Passwords.txt` archivo.
- Conoce la dirección IP de un nodo de administrador.

Acerca de esta tarea

Se denomina el archivo de registro de auditoría activo `audit.log`, Y se almacena en los nodos Admin.

Una vez al día, se guarda el archivo `audit.log` activo, y otro nuevo `audit.log` se ha iniciado el archivo. El nombre del archivo guardado indica cuándo se guardó, en el formato `yyyy-mm-dd.txt`.

Después de un día, el archivo guardado se comprime y cambia su nombre, en el formato `yyyy-mm-dd.txt.gz`, que conserva la fecha original.

En este ejemplo se muestra el activo `audit.log` archivo, el archivo del día anterior (`2018-04-15.txt`), y el archivo comprimido del día anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Pasos

1. Inicie sesión en un nodo de administrador:
 - a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
 - d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

2. Vaya al directorio que contiene los archivos del registro de auditoría:

```
cd /var/local/audit/export
```

3. Ver el archivo de registro de auditoría actual o guardado, según sea necesario.

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

Se realiza un seguimiento de varias operaciones de bloques y de objetos en los registros de auditoría de StorageGRID.

Se realizó un seguimiento de las operaciones de bloque en los registros de auditoría

- ELIMINAR bloque
- DELETE Bucket tagging
- ELIMINAR varios objetos
- GET Bucket (objetos de lista)
- OBTENGA las versiones DE objeto Bucket
- GET Bucket tagging
- Cubo DE CABEZA
- COLOQUE el cucharón
- CUMPLIR con la normativa de los bloques
- PUT Bucket etiquetaje
- PONER creación de versiones de bloques

Se realizó un seguimiento de las operaciones de objetos en los registros de auditoría

- Completar carga de varias partes
- Cargar parte (cuando la regla ILM utiliza los comportamientos de ingesta equilibrada o estricta)
- Cargar parte - Copiar (cuando la regla ILM utiliza los comportamientos de ingesta equilibrada o estricta)
- ELIMINAR objeto
- OBTENER objeto
- OBJETO HEAD
- Restauración DE objetos posterior
- OBJETO PUT
- PONER objeto: Copiar

Información relacionada

["Operaciones en bloques"](#)

["Operaciones en objetos"](#)

Ventajas de las conexiones HTTP activas, inactivas y simultáneas

La forma en que se configuran las conexiones HTTP puede afectar el rendimiento del

sistema StorageGRID. Las configuraciones varían en función de si la conexión HTTP está activa o inactiva o si tiene varias conexiones simultáneas.

Puede identificar las ventajas en el rendimiento de los siguientes tipos de conexiones HTTP:

- Conexiones HTTP inactivas
- Conexiones HTTP activas
- Conexiones HTTP simultáneas

Ventajas de mantener abiertas las conexiones HTTP inactivas

Debe mantener las conexiones HTTP abiertas incluso cuando las aplicaciones cliente están inactivas para permitir que las aplicaciones cliente realicen transacciones posteriores a través de la conexión abierta. Basándose en las mediciones del sistema y en la experiencia de integración, debe mantener abierta una conexión HTTP inactiva durante un máximo de 10 minutos. StorageGRID puede cerrar automáticamente una conexión HTTP que se mantenga abierta y inactiva durante más de 10 minutos.

Las conexiones HTTP abiertas y inactivas proporcionan las siguientes ventajas:

- Menor latencia desde el momento en que el sistema StorageGRID determina que debe realizar una transacción HTTP hasta el momento en que el sistema StorageGRID puede realizar la transacción

La latencia reducida es la ventaja principal, especialmente por la cantidad de tiempo necesario para establecer las conexiones TCP/IP y TLS.

- Aumento de la velocidad de transferencia de datos mediante la preparación del algoritmo de inicio lento TCP/IP con transferencias realizadas previamente
- Notificación instantánea de varias clases de condiciones de fallo que interrumpen la conectividad entre la aplicación cliente y el sistema StorageGRID

Determinar durante cuánto tiempo mantener abierta una conexión inactiva-es un intercambio entre las ventajas del inicio lento que se asocia a la conexión existente y la asignación ideal de la conexión a los recursos internos del sistema.

Ventajas de las conexiones HTTP activas

Para conexiones directas a nodos de almacenamiento, debe limitar la duración de una conexión HTTP activa a un máximo de 10 minutos, incluso si la conexión HTTP realiza transacciones continuamente.

La determinación de la duración máxima de la apertura de una conexión es un intercambio-entre los beneficios de la persistencia de la conexión y la asignación ideal de la conexión a los recursos internos del sistema.

Para las conexiones de cliente a los nodos de almacenamiento, la limitación de las conexiones HTTP activas proporciona las siguientes ventajas:

- Permite un balanceo de carga óptimo en el sistema StorageGRID.

Con el tiempo, es posible que una conexión HTTP ya no sea óptima a medida que cambian los requisitos de equilibrio de carga. El sistema realiza su mejor equilibrio de carga cuando las aplicaciones cliente establecen una conexión HTTP independiente para cada transacción, pero esto niega las ganancias mucho más valiosas asociadas con conexiones persistentes.

- Permite a las aplicaciones cliente dirigir transacciones HTTP a servicios LDR que tengan espacio

disponible.

- Permite iniciar los procedimientos de mantenimiento.

Algunos procedimientos de mantenimiento se inician solo después de que se completen todas las conexiones HTTP en curso.

En el caso de las conexiones cliente al servicio Load Balancer, limitar la duración de las conexiones abiertas puede ser útil para permitir que algunos procedimientos de mantenimiento se inicien con rapidez. Si la duración de las conexiones de cliente no es limitada, es posible que las conexiones activas tarden varios minutos en finalizarse automáticamente.

Ventajas de las conexiones HTTP simultáneas

Debe mantener abiertas varias conexiones TCP/IP al sistema StorageGRID para permitir el paralelismo, lo que aumenta el rendimiento. El número óptimo de conexiones paralelas depende de diversos factores.

Las conexiones HTTP simultáneas proporcionan las siguientes ventajas:

- Latencia reducida

Las transacciones pueden iniciarse inmediatamente en lugar de esperar a que se completen otras transacciones.

- Aumento de la productividad

El sistema StorageGRID puede realizar transacciones paralelas y aumentar el rendimiento global de las transacciones.

Las aplicaciones cliente deben establecer varias conexiones HTTP. Cuando una aplicación cliente tiene que realizar una transacción, puede seleccionar y utilizar inmediatamente cualquier conexión establecida que no esté procesando actualmente una transacción.

Antes de que el rendimiento empiece a degradarse, cada topología de los sistemas StorageGRID tiene un rendimiento máximo diferente para transacciones y conexiones simultáneas. El rendimiento máximo depende de factores como los recursos informáticos, los recursos de red, los recursos de almacenamiento y los enlaces WAN. También son factores que influyen en el número de servidores y servicios y el número de aplicaciones que admite el sistema StorageGRID.

A menudo, los sistemas StorageGRID admiten varias aplicaciones cliente. Debe tener esto en cuenta al determinar el número máximo de conexiones simultáneas que utiliza una aplicación cliente. Si la aplicación cliente consta de varias entidades de software que cada una establece conexiones al sistema StorageGRID, debe agregar todas las conexiones a través de las entidades. Es posible que tenga que ajustar el número máximo de conexiones simultáneas en las siguientes situaciones:

- La topología del sistema StorageGRID afecta al número máximo de transacciones y conexiones simultáneas que puede admitir el sistema.
- Las aplicaciones cliente que interactúan con el sistema StorageGRID a través de una red con ancho de banda limitado pueden tener que reducir el grado de concurrencia para garantizar que las transacciones individuales se completen en un tiempo razonable.
- Cuando muchas aplicaciones cliente comparten el sistema StorageGRID, puede que tenga que reducir el nivel de concurrencia para evitar superar los límites del sistema.

Separación de grupos de conexiones HTTP para operaciones de lectura y escritura

Puede utilizar pools independientes de conexiones HTTP para operaciones de lectura y escritura y controlar la cantidad de un pool que debe utilizar para cada uno. Los grupos separados de conexiones HTTP le permiten controlar mejor las transacciones y equilibrar las cargas.

Las aplicaciones cliente pueden crear cargas que sean dominantes de la recuperación (lectura) o del almacén (escritura). Con grupos separados de conexiones HTTP para transacciones de lectura y escritura, puede ajustar la cantidad de cada pool que se va a dedicar a transacciones de lectura o escritura.

Usar la API REST DE Swift (obsoleto)

Use la API de REST DE Swift: Información general

Las aplicaciones cliente pueden usar la API Swift de OpenStack para interactuar con el sistema StorageGRID.



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

StorageGRID admite las siguientes versiones específicas de Swift y HTTP.

| Elemento | Versión |
|----------------------|--|
| Especificación Swift | OpenStack Swift Object Storage API v1 a fecha de noviembre de 2015 |
| HTTP | 1.1 para obtener más información acerca de HTTP, consulte HTTP/1.1 (RFC 7230-35). Nota: StorageGRID no admite canalización HTTP/1.1. |

Información relacionada

["OpenStack: API de almacenamiento de objetos"](#)

Historial de soporte de la API de Swift en StorageGRID

Debe estar al tanto de los cambios en la compatibilidad del sistema StorageGRID con la API DE REST de Swift.

| Liberar | Comentarios |
|---------|--|
| 11.7 | Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras. |
| 11.6 | Cambios editoriales menores. |

| Liberar | Comentarios |
|----------------|---|
| 11.5 | Se ha eliminado el control de consistencia débil. En su lugar, se utilizará el nivel de consistencia disponible. |
| 11.4 | Añadido soporte para TLS 1.3. Se añadió la descripción de la relación entre ILM y la configuración de consistencia. |
| 11.3 | Las operaciones de PUT Object actualizadas para describir el impacto de las reglas de ILM que utilizan la colocación síncrona en el procesamiento (las opciones equilibradas y estrictas del comportamiento de procesamiento). Se ha agregado una descripción de las conexiones de cliente que utilizan extremos de equilibrador de carga o grupos de alta disponibilidad. Ya no se admiten los cifrados TLS 1.1. |
| 11.2 | Cambios editoriales menores en el documento. |
| 11.1 | Se añadió compatibilidad con el uso de HTTP para conexiones de clientes Swift a los nodos de grid. Se han actualizado las definiciones de controles de coherencia. |
| 11.0 | Se ha agregado soporte para 1,000 contenedores por cada cuenta de inquilino. |
| 10.3 | Actualizaciones administrativas y correcciones en el documento. Se han eliminado secciones para configurar certificados de servidor personalizados. |
| 10.2 | Soporte inicial de la API Swift por el sistema StorageGRID. La versión compatible actualmente es la API de almacenamiento de objetos Swift de OpenStack v1. |

Cómo StorageGRID implementa la API DE REST de Swift

Una aplicación cliente puede usar llamadas API DE REST de Swift para conectarse a nodos de almacenamiento y nodos de puerta de enlace para crear contenedores, así como para almacenar y recuperar objetos. De este modo, las aplicaciones orientadas a los servicios desarrolladas para OpenStack Swift pueden conectarse con el almacenamiento de objetos en las instalaciones que proporciona el sistema StorageGRID.

Gestión de objetos Swift

Una vez que se han ingerido objetos Swift en el sistema StorageGRID, se gestionan con las reglas de gestión de ciclo de vida de la información (ILM) de la política de ILM activa del sistema. La ["Reglas de ILM"](#) y. ["Política de ILM"](#) Determinar cómo crea y distribuye StorageGRID copias de datos de objetos y cómo administra esas copias con el tiempo. Por ejemplo, una regla de ILM puede aplicarse a los objetos en contenedores Swift específicos y puede especificar que se guarden varias copias de objetos en varios centros de datos durante un determinado número de años.

Póngase en contacto con su asesor de los servicios profesionales de NetApp o administrador de StorageGRID si tiene que comprender cómo las reglas y las políticas de ILM del grid afectan a los objetos de su cuenta de

inquilino Swift.

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 Swift inician una operación.

Garantías y controles de coherencia

De forma predeterminada, StorageGRID proporciona coherencia de lectura tras escritura para los objetos recién creados y coherencia eventual para las actualizaciones de objetos y operaciones DE CABECERA. Cualquiera "OBTENGA" después de un completado correctamente "PUESTO" podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, actualizaciones de metadatos y eliminaciones son coherentes en la actualidad. Por lo general, las sobrescrituras tardan segundos o minutos en propagarse, pero pueden tardar hasta 15 días.

StorageGRID también le permite controlar la coherencia de cada contenedor. Los controles de consistencia proporcionan un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en diferentes nodos de almacenamiento y sitios, según lo requiera la aplicación.

Recomendaciones para implementar la API DE REST de Swift

Debe seguir estas recomendaciones al implementar la API DE REST de Swift para usar con StorageGRID.

Recomendaciones para las cabezas a los objetos no existentes

Si tu aplicación comprueba de forma rutinaria si existe un objeto en una ruta en la que no esperas que exista el objeto, debes usar el control de consistencia "disponible". Por ejemplo, debe utilizar el control de coherencia "disponible" si la aplicación realiza una OPERACIÓN HEAD a una ubicación antes de realizar una operación PUT en esa ubicación.

De lo contrario, si la operación HEAD no encuentra el objeto, es posible que reciba un número elevado de 500 errores internos de Server si uno o más nodos de almacenamiento no están disponibles.

Puede establecer el control de consistencia "disponible" para cada contenedor utilizando el "PONGA la solicitud de consistencia del contenedor". Puede ver Establecer el control de consistencia "disponible" para cada contenedor mediante el "OBTENGA la solicitud de consistencia del contenedor".

Recomendaciones para los nombres de objetos

En el caso de los contenedores creados en StorageGRID 11.4 o posteriores, ya no es necesario restringir los nombres de objetos para cumplir con las prácticas recomendadas de rendimiento. Por ejemplo, ahora puede utilizar valores aleatorios para los primeros cuatro caracteres de nombres de objetos.

Para los contenedores que se crearon en las versiones anteriores a StorageGRID 11.4, siga estas recomendaciones para los nombres de objetos:

- No debe utilizar valores aleatorios como los primeros cuatro caracteres de nombres de objetos. Esto contrasta con la anterior recomendación de AWS para prefijos de nombres. En su lugar, debe utilizar prefijos no aleatorios y no únicos, como `image`.
- Si sigue la recomendación anterior de AWS de utilizar caracteres aleatorios y únicos en prefijos de

nombre, debe aplicar un prefijo a los nombres de objeto con un nombre de directorio. Es decir, utilice este formato:

```
mycontainer/mydir/f8e3-image3132.jpg
```

En lugar de este formato:

```
mycontainer/f8e3-image3132.jpg
```

Recomendaciones para «lecturas de rango»

Si la "[opción global para comprimir objetos almacenados](#)" Está habilitada, las aplicaciones cliente de Swift deben evitar la realización de OPERACIONES GET object que especifican un rango de bytes. Estas operaciones de «lectura de rango» son ineficientes, ya que StorageGRID debe descomprimir de forma efectiva los objetos para acceder a los bytes solicitados. LAS operaciones GET Object que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, es muy ineficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden 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.

Configure las conexiones y las cuentas de inquilino

Para configurar StorageGRID para aceptar conexiones desde aplicaciones cliente, es necesario crear una o más cuentas de inquilino y configurar las conexiones.

Cree y configure cuentas de inquilino de Swift

Se requiere una cuenta de inquilino de Swift para que los clientes de la API de Swift puedan almacenar y recuperar objetos en StorageGRID. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios, y contenedores y objetos.

Las cuentas de inquilino de Swift las crea un administrador de grid de StorageGRID mediante Grid Manager o la API de gestión de grid.

Cuando "[Crear una cuenta de inquilino de Swift](#)", el administrador de la cuadrícula especifica la siguiente información:

- "[Nombre mostrado para el arrendatario](#)" (El ID de cuenta del inquilino se asigna automáticamente y no se puede cambiar)
- Opcionalmente, a "[cuota de almacenamiento para la cuenta de inquilino](#)" — el número máximo de gigabytes, terabytes o petabytes disponibles para los objetos del inquilino. La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco).
- Si "[Inicio de sesión único \(SSO\)](#)" No está en uso para el sistema de StorageGRID, si la cuenta de inquilino utilizará su propio origen de identidades o compartirá el origen de identidad del grid y la contraseña inicial para el usuario raíz local del inquilino.

- Si SSO está habilitado, el grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.

Después de crear una cuenta de inquilino de Swift, los usuarios con el permiso de acceso raíz pueden acceder al administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) y crear grupos y usuarios locales
- Supervisión del uso de almacenamiento



Los usuarios de Swift deben contar con permiso de acceso raíz a ["Acceda al Gestor de inquilinos"](#). Sin embargo, el permiso de acceso raíz no permite que los usuarios se autenticuen en la API DE REST de Swift para crear contenedores y procesar objetos. Los usuarios deben tener el permiso de administrador de Swift para autenticarse en la API DE REST de Swift.

Cómo se pueden configurar las conexiones de clientes

Un administrador de grid toma opciones de configuración que afectan a la forma en que los clientes de Swift se conectan a StorageGRID para almacenar y recuperar los datos. La información específica que necesita para realizar una conexión depende de la configuración elegida.

Las aplicaciones cliente pueden almacenar o recuperar objetos conectándose al servicio de Equilibrador de Carga en los nodos de administración o de Gateway, u opcionalmente, la dirección IP virtual de un grupo de alta disponibilidad (HA) de nodos de administración o nodos de Gateway.



Todas las aplicaciones que dependen de StorageGRID para proporcionar balanceo de carga deben conectarse mediante el servicio Load Balancer.

- Nodos de almacenamiento, con o sin un equilibrador de carga externo

Al configurar StorageGRID, un administrador de grid puede utilizar Grid Manager o la API de gestión de grid para realizar los siguientes pasos, todos ellos opcionales:

1. Configure los extremos para el servicio Load Balancer.

Debe configurar los extremos para usar el servicio Load Balancer. El servicio Load Balancer en los nodos de administrador o de puerta de enlace distribuye conexiones de red entrantes desde aplicaciones cliente hasta los nodos de almacenamiento. Al crear un extremo de equilibrio de carga, el administrador de StorageGRID especifica un número de puerto, tanto si el extremo acepta conexiones HTTP o HTTPS, como el tipo de cliente (S3 o Swift) que utilizará el extremo y el certificado que se utilizará para las conexiones HTTPS (si procede). SWIFT es compatible con estos ["tipos de punto final"](#).

2. Configure redes de cliente no fiables.

Si un administrador de StorageGRID configura la red cliente de un nodo para que no sea de confianza, el nodo sólo acepta conexiones entrantes en la red cliente en puertos que se configuran explícitamente como extremos equilibradores de carga.

3. Configuración de grupos de alta disponibilidad.

Si un administrador crea un grupo de alta disponibilidad, las interfaces de red de varios nodos de administrador o nodos de puerta de enlace se colocan en una configuración de backup activo. Las conexiones de clientes se realizan mediante la dirección IP virtual del grupo de alta disponibilidad.

Consulte ["Opciones de configuración para grupos de alta disponibilidad"](#) si quiere más información.

Resumen: Direcciones IP y puertos para conexiones cliente

Las aplicaciones cliente se conectan a StorageGRID mediante la dirección IP de un nodo de grid y el número de puerto de un servicio en ese nodo. Si se configuran los grupos de alta disponibilidad, las aplicaciones cliente se pueden conectar mediante la dirección IP virtual del grupo de alta disponibilidad.

Información necesaria para realizar conexiones de cliente

La tabla resume las distintas maneras en que los clientes pueden conectarse a StorageGRID y las direcciones IP y los puertos que se utilizan para cada tipo de conexión. Consulte ["Puertos y direcciones IP para las conexiones de cliente"](#) También puede ponerse en contacto con el administrador de StorageGRID para obtener más información.

| Dónde se realiza la conexión | Servicio al que se conecta el cliente | Dirección IP | Puerto |
|------------------------------|---------------------------------------|--|--|
| Grupo de ALTA DISPONIBILIDAD | Equilibrador de carga | La dirección IP virtual de un grupo de alta disponibilidad | <ul style="list-style-type: none">• Puerto de punto final del equilibrador de carga |
| Nodo de administración | Equilibrador de carga | La dirección IP del nodo de administrador | <ul style="list-style-type: none">• Puerto de punto final del equilibrador de carga |
| Nodo de puerta de enlace | Equilibrador de carga | La dirección IP del nodo de puerta de enlace | <ul style="list-style-type: none">• Puerto de punto final del equilibrador de carga |
| Nodo de almacenamiento | LDR | La dirección IP del nodo de almacenamiento | <p>Puertos Swift predeterminados:</p> <ul style="list-style-type: none">• HTTPS: 18083• HTTP: 18085 |

Ejemplo

Para conectar un cliente Swift al extremo Load Balancer de un grupo de ha de nodos de Gateway, utilice una URL estructurada como se muestra a continuación:

- `https://VIP-of-HA-group:LB-endpoint-port`

Por ejemplo, si la dirección IP virtual del grupo de alta disponibilidad es 192.0.2.6 y el número de puerto de un extremo de equilibrio de carga de Swift es 10444, un cliente de Swift puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.6:10444`

Es posible configurar un nombre DNS para la dirección IP que utilizan los clientes para conectarse a StorageGRID. Póngase en contacto con el administrador de red local.

Decidir usar conexiones HTTPS o HTTP

Cuando se realizan conexiones de cliente mediante un extremo de equilibrio de carga, es necesario realizar conexiones mediante el protocolo (HTTP o HTTPS) especificado para ese extremo. Para utilizar HTTP para conexiones de cliente a nodos de almacenamiento, debe habilitar el uso.

De forma predeterminada, cuando las aplicaciones cliente se conectan a nodos de almacenamiento, deben utilizar HTTPS cifrado para todas las conexiones. Opcionalmente, puede activar conexiones HTTP menos seguras seleccionando el ["Active HTTP para las conexiones del nodo de almacenamiento"](#) Opción en Grid Manager. Por ejemplo, una aplicación cliente puede utilizar HTTP al probar la conexión a un nodo de almacenamiento en un entorno no de producción.



Tenga cuidado al habilitar HTTP para una cuadrícula de producción porque las solicitudes y respuestas se enviarán sin cifrar.

Si se selecciona la opción **Activar HTTP para conexiones de nodo de almacenamiento**, los clientes deben usar puertos para HTTP diferentes de los que usan para HTTPS.

Pruebe la conexión en la configuración de la API de Swift

Puede usar la interfaz de línea de comandos de Swift para probar la conexión con el sistema StorageGRID y verificar que puede leer y escribir objetos en el sistema.

Antes de empezar

- Debe haber descargado e instalado python-swiftclient, el cliente de línea de comandos de Swift.

["SwiftStack: python-swiftclient"](#)

- Debe tener una cuenta de inquilino de Swift en el sistema StorageGRID.

Acerca de esta tarea

Si no ha configurado la seguridad, debe añadir el `--insecure` marque cada uno de estos comandos.

Pasos

1. Consulte la URL de información para la implementación de Swift de StorageGRID:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

Esto es suficiente para probar que la implementación de Swift es funcional. Para seguir probando la configuración de la cuenta almacenando un objeto, continúe con los pasos adicionales.

2. Coloque un objeto en el contenedor:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Obtenga el contenedor para verificar el objeto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Elimine el objeto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Elimine el contenedor:

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0`
delete test_container
```

Información relacionada

["Cree y configure cuentas de inquilino de Swift"](#)

["Configure la seguridad de la API DE REST"](#)

Operaciones compatibles con la API REST de Swift

El sistema StorageGRID admite la mayoría de operaciones en la API Swift de OpenStack. Antes de integrar clientes API DE REST de Swift con StorageGRID, revise los detalles de la implementación para las operaciones de la cuenta, el contenedor y el

objeto.

Operaciones compatibles con StorageGRID

Se admiten las siguientes operaciones de API de Swift:

- ["Operaciones de cuentas"](#)
- ["Operaciones de contenedor"](#)
- ["Operaciones de objeto"](#)

Encabezados de respuesta comunes para todas las operaciones

El sistema StorageGRID implementa todos los encabezados comunes para las operaciones compatibles según lo definido por la API de almacenamiento de objetos Swift de OpenStack v1.

Información relacionada

["OpenStack: API de almacenamiento de objetos"](#)

Extremos de API de Swift compatibles

StorageGRID admite los siguientes extremos de la API de Swift: La URL de la información, la URL de autenticación y la URL de almacenamiento.

URL de información

Puede determinar las capacidades y las limitaciones de la implementación de Swift de StorageGRID emitiendo una solicitud GET a la URL de la base de Swift con la ruta /info.

```
https://FQDN | Node IP:Swift Port/info/
```

En la solicitud:

- *FQDN* es el nombre de dominio completo.
- *Node IP* Es la dirección IP del nodo de almacenamiento o del nodo de puerta de enlace en la red de StorageGRID.
- *Swift Port* Es el número de puerto que se usa para las conexiones API de Swift en el nodo de almacenamiento o la puerta de enlace.

Por ejemplo, la siguiente URL de información solicita información desde un nodo de almacenamiento con la dirección IP 10.99.106.103 y mediante el puerto 18083.

```
https://10.99.106.103:18083/info/
```

La respuesta incluye las capacidades de la implementación Swift como diccionario JSON. Una herramienta cliente puede analizar la respuesta JSON para determinar las capacidades de la implementación y usarlas como restricciones para operaciones de almacenamiento subsiguientes.

La implementación de StorageGRID de Swift permite un acceso sin autenticar a la URL de información.

URL de autenticación

Un cliente puede utilizar la URL de autenticación de Swift para autenticarse como usuario de cuenta de inquilino.

```
https://FQDN | Node_IP:Swift_Port/auth/v1.0/
```

Se deben proporcionar el ID de cuenta de inquilino, el nombre de usuario y la contraseña como parámetros en el X-Auth-User y. X-Auth-Key solicite los encabezados de la siguiente manera:

```
X-Auth-User: Tenant_Account_ID:Username
```

```
X-Auth-Key: Password
```

En los encabezados de la solicitud:

- *Tenant_Account_ID* Es el ID de cuenta que asigna StorageGRID cuando se creó el inquilino de Swift. Este es el mismo ID de cuenta de arrendatario que se utiliza en la página de inicio de sesión de Gestor de inquilinos.
- *Username* Es el nombre de un usuario arrendatario que se ha creado en el Administrador de arrendatarios. Este usuario debe pertenecer a un grupo con permiso de administrador de Swift. El usuario raíz del inquilino no puede configurarse para usar la API REST DE Swift.

Si la Federación de identidades está habilitada para la cuenta de inquilino, proporcione el nombre de usuario y la contraseña del usuario federado desde el servidor LDAP. Como alternativa, proporcione el nombre de dominio del usuario LDAP. Por ejemplo:

```
X-Auth-User: Tenant_Account_ID:Username@Domain_Name
```

- *Password* es la contraseña del usuario inquilino. Las contraseñas de usuario se crean y administran en el Administrador de inquilinos.

La respuesta a una solicitud de autenticación correcta devuelve una URL de almacenamiento y un token de autenticación, de la siguiente forma:

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID
```

```
X-Auth-Token: token
```

```
X-Storage-Token: token
```

De forma predeterminada, el token es válido durante 24 horas desde el tiempo de generación.

Se generan tokens para una cuenta de arrendatario específica. Un token válido para una cuenta no autoriza a un usuario a acceder a otra cuenta.

URL de almacenamiento

Una aplicación cliente puede emitir llamadas a la API DE REST de Swift para realizar operaciones de cuenta, contenedor y objeto admitidas contra un nodo de puerta de enlace o un nodo de almacenamiento. Las solicitudes de almacenamiento se dirigen a la URL de almacenamiento que se devuelve en la respuesta de autenticación. La solicitud también debe incluir el encabezado X-Auth-Token y el valor devuelto por la solicitud auth.

`https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID`

`[/container][/object]`

`X-Auth-Token: token`

Es posible que algunos encabezados de respuesta del almacenamiento que contienen estadísticas de uso no reflejen números precisos de los objetos modificados recientemente. Puede que en estos encabezados se deban utilizar unos minutos para que aparezcan números precisos.

Los siguientes encabezados de respuesta para las operaciones de cuentas y contenedores son ejemplos de los que contienen estadísticas de uso:

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

Información relacionada

["Configure las conexiones y las cuentas de inquilino"](#)

["Operaciones de cuentas"](#)

["Operaciones de contenedor"](#)

["Operaciones de objeto"](#)

Operaciones de cuentas

Las siguientes operaciones de la API de Swift se realizan en las cuentas.

OBTENGA la cuenta

Esta operación recupera la lista de contenedores asociada a las estadísticas de uso de la cuenta y la cuenta.

Se requiere el siguiente parámetro request:

- `Account`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Los siguientes parámetros de consulta de solicitud admitidos son opcionales:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`

- Prefix

Una ejecución satisfactoria devuelve los siguientes encabezados con una respuesta «'HTTP/1.1 204 sin contenido» si se encuentra la cuenta y no tiene contenedores o la lista de contenedores está vacía; o una respuesta «'HTTP/1.1 200 OK'» si se encuentra la cuenta y la lista de contenedores no está vacía:

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

CUENTA principal

Esta operación recupera información de la cuenta y estadísticas de una cuenta de Swift.

Se requiere el siguiente parámetro request:

- Account

Se requiere el siguiente encabezado de solicitud:

- X-Auth-Token

Una ejecución satisfactoria devuelve los encabezados siguientes con una respuesta «'HTTP/1.1 204 sin contenido»:

- Accept-Ranges
- Content-Length
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

Información relacionada

["Supervisar y auditar operaciones"](#)

Operaciones de contenedor

StorageGRID admite un máximo de 1,000 contenedores por cuenta de Swift. Las siguientes operaciones de la API de Swift se realizan en contenedores.

ELIMINAR contenedor

Esta operación elimina un contenedor vacío de una cuenta de Swift en un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- Account
- Container

Se requiere el siguiente encabezado de solicitud:

- X-Auth-Token

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 204 sin contenido":

- Content-Length
- Content-Type
- Date
- X-Trans-Id

OBTENGA el contenedor

Esta operación recupera la lista de objetos asociada con el contenedor junto con las estadísticas y los metadatos del contenedor en un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- Account
- Container

Se requiere el siguiente encabezado de solicitud:

- X-Auth-Token

Los siguientes parámetros de consulta de solicitud admitidos son opcionales:

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Path

- Prefix

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 200 Success" o "HTTP/1.1 204 sin contenido":

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

Contenedor DE LA CABEZA

Esta operación recupera las estadísticas y los metadatos del contenedor de un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- Account
- Container

Se requiere el siguiente encabezado de solicitud:

- X-Auth-Token

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 204 sin contenido":

- Accept-Ranges
- Content-Length
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

COLOQUE el contenedor

Esta operación crea un contenedor para una cuenta en un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- Account

- Container

Se requiere el siguiente encabezado de solicitud:

- X-Auth-Token

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 201 creado" o "HTTP/1.1 202 aceptado" (si el contenedor ya existe bajo esta cuenta):

- Content-Length
- Date
- X-Timestamp
- X-Trans-Id

Un nombre de contenedor debe ser único en el espacio de nombres de StorageGRID. Si el contenedor existe en otra cuenta, se devuelve el siguiente encabezado: "Conflicto HTTP/1.1 409".

Información relacionada

["Supervisar y auditar operaciones"](#)

Operaciones de objeto

Las siguientes operaciones de la API de Swift se realizan en objetos. Se puede realizar un seguimiento de estas operaciones en la ["Registro de auditoría de StorageGRID"](#).

ELIMINAR objeto

Esta operación elimina los metadatos y el contenido de un objeto del sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- Account
- Container
- Object

Se requiere el siguiente encabezado de solicitud:

- X-Auth-Token

Una ejecución correcta devuelve los encabezados de respuesta siguientes con un HTTP/1.1 204 No Content respuesta:

- Content-Length
- Content-Type
- Date
- X-Trans-Id

Al procesar una solicitud DE ELIMINACIÓN de objeto, 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.

Para obtener más información, consulte ["Cómo se eliminan los objetos"](#).

OBJETO GET

Esta operación recupera el contenido de objetos y obtiene los metadatos de objetos de un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- Account
- Container
- Object

Se requiere el siguiente encabezado de solicitud:

- X-Auth-Token

Los siguientes encabezados de solicitud son opcionales:

- Accept-Encoding
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Una ejecución correcta devuelve los encabezados siguientes con un HTTP/1.1 200 OK respuesta:

- Accept-Ranges
- Content-Disposition, devuelto sólo si Content-Disposition se establecieron los metadatos
- Content-Encoding, devuelto sólo si Content-Encoding se establecieron los metadatos
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

OBJETO HEAD

Esta operación recupera los metadatos y las propiedades de un objeto ingerido desde un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- Account
- Container
- Object

Se requiere el siguiente encabezado de solicitud:

- X-Auth-Token

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 200 OK":

- Accept-Ranges
- Content-Disposition, devuelto sólo si Content-Disposition se establecieron los metadatos
- Content-Encoding, devuelto sólo si Content-Encoding se establecieron los metadatos
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

PONER objeto

Esta operación crea un objeto nuevo con datos y metadatos, o reemplaza un objeto existente con datos y metadatos en un sistema StorageGRID.

La StorageGRID admite objetos de hasta 5 TiB (5,497,558,138,880 bytes) con un tamaño.



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 Swift inician una operación.

Se requieren los siguientes parámetros de solicitud:

- Account
- Container
- Object

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Los siguientes encabezados de solicitud son opcionales:

- `Content-Disposition`
- `Content-Encoding`

No utilice fragmentos `Content-Encoding` Si la regla de ILM que se aplica a un objeto filtra objetos según el tamaño y utiliza la ubicación síncrona durante el procesamiento (las opciones equilibradas o estrictas del comportamiento de ingesta).

- `Transfer-Encoding`

No utilice comprimidos ni fragmentados `Transfer-Encoding` Si la regla de ILM que se aplica a un objeto filtra objetos según el tamaño y utiliza la ubicación síncrona durante el procesamiento (las opciones equilibradas o estrictas del comportamiento de ingesta).

- `Content-Length`

Si una regla de ILM filtra objetos por tamaño y utiliza la ubicación síncrona durante el procesamiento, debe especificar `Content-Length`.



Si no sigue estas directrices para `Content-Encoding`, `Transfer-Encoding`, y `Content-Length`, StorageGRID debe guardar el objeto para poder determinar el tamaño del objeto y aplicar la regla ILM. En otras palabras, StorageGRID debe crear de forma predeterminada copias provisionales de un objeto durante el procesamiento. Es decir, StorageGRID debe utilizar la opción Dual COMMIT para el comportamiento de procesamiento.

Para obtener más información sobre la ubicación síncrona y las reglas de ILM, consulte ["Opciones de protección de datos para consumo"](#).

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` (metadatos relacionados con objetos)

Si desea utilizar la opción **Tiempo de creación definido por el usuario** como tiempo de referencia para una regla de ILM, debe almacenar el valor en un encabezado definido por el usuario llamado `X-Object-Meta-Creation-Time`. Por ejemplo:

```
X-Object-Meta-Creation-Time: 1443399726
```

Este campo se evalúa como segundos desde el 1 de enero de 1970.

- `X-Storage-Class: reduced_redundancy`

Este encabezado afecta al número de copias de objeto que crea StorageGRID si la regla de ILM que coincide con un objeto ingerido especifica un comportamiento de procesamiento de Doble COMMIT o

equilibrado.

- **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.

La `reduced_redundancy` El encabezado se utiliza mejor cuando la regla de ILM que coincide con el objeto crea una única copia replicada. En este caso, utilizar `reduced_redundancy` elimina la creación y eliminación innecesarias de una copia de objetos adicional en cada operación de procesamiento.

Con el `reduced_redundancy` la cabecera no se recomienda en otras circunstancias porque aumenta el riesgo de pérdida de datos de objetos durante el procesamiento. 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.

Tenga en cuenta que especificar `reduced_redundancy` sólo afecta al número de copias que se crean cuando un objeto se ingiere por primera vez. No afecta al número de copias del objeto que se realizan cuando el objeto se evalúa mediante la política de ILM activa y no provoca que los datos se almacenen en niveles más bajos de redundancia en el sistema StorageGRID.

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 201 creado":

- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Trans-Id

SOLICITUD DE OPCIONES

La solicitud DE OPCIONES comprueba la disponibilidad de un servicio Swift individual. El nodo de almacenamiento o el nodo de puerta de enlace especificado en la URL procesan la solicitud DE OPCIONES.

MÉTODO DE OPCIONES

Por ejemplo, las aplicaciones cliente pueden emitir una solicitud DE OPCIONES al puerto Swift en un nodo de almacenamiento sin proporcionar las credenciales de autenticación Swift 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.

Cuando se utiliza con la URL de información o la URL de almacenamiento, el método OPTIONS devuelve una lista de verbos admitidos para la URL dada (por ejemplo, HEAD, GET, OPTIONS y PUT). El método de OPCIONES no se puede utilizar con la URL de autenticación.

Se requiere el siguiente parámetro request:

- Account

Los siguientes parámetros de solicitud son opcionales:

- Container
- Object

Una ejecución satisfactoria devuelve los encabezados siguientes con una respuesta «'HTTP/1.1 204 sin contenido». La solicitud DE OPCIONES a la URL de almacenamiento no requiere que exista el destino.

- Allow (Una lista de verbos admitidos para la dirección URL dada, por ejemplo, CABEZA, OBTENER, OPCIONES, Y PUESTO)
- Content-Length
- Content-Type
- Date
- X-Trans-Id

Información relacionada
["Extremos de API de Swift compatibles"](#)

Respuesta de error a las operaciones de la API de Swift

Comprender las posibles respuestas de error puede ayudar a resolver las operaciones.

Pueden devolverse los siguientes códigos de estado HTTP cuando se produzcan errores durante una operación:

| Nombre de error de Swift | Estado de HTTP |
|--|--------------------------|
| AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadataValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataItems, TotalMetadataTooLarge | 400 solicitud incorrecta |
| ACCESSDENIED | 403 Prohibido |
| ContainerNotEmpty, ContainerAlreadyExists | 409 conflicto |

| Nombre de error de Swift | Estado de HTTP |
|----------------------------|------------------------------------|
| Internalerror | 500 error de servidor interno |
| InvalidRange | 416 rango solicitado no utilizable |
| MethodNotAllowed | 405 método no permitido |
| MissingContentLength | 411 longitud requerida |
| NOTFOUND | 404 no encontrado |
| NotImplied | 501 no implementada |
| Error de preconditionError | Error de condición 412 |
| ResourceNotFound | 404 no encontrado |
| No autorizado | 401 no autorizado |
| Entidad no procesable | 422 entidad no procesable |

Operaciones de la API de REST de StorageGRID Swift

Existen operaciones que se añaden a la API DE REST de Swift que son específicas del sistema StorageGRID.

OBTENGA la solicitud de consistencia del contenedor

"[Controles de consistencia](#)" Proporcionar un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios. La solicitud DE consistencia DEL contenedor le permite determinar el nivel de consistencia que se aplica a un contenedor en particular.

Solicitud

| Solicitar encabezado HTTP | Descripción |
|---------------------------|--|
| Token X-Auth | Especifica el token de autenticación Swift de la cuenta que se va a utilizar para la solicitud. |
| x-ntap-sg-consistency | Especifica el tipo de solicitud, donde <code>true</code> = OBTENER la consistencia del contenedor, y. <code>false</code> = OBTENER contenedor. |
| Host | El nombre de host al que se dirige la solicitud. |

Ejemplo de solicitud

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Respuesta

| Encabezado HTTP de respuesta | Descripción |
|------------------------------|---|
| Fecha | La fecha y la hora de la respuesta. |
| Conexión | Si la conexión con el servidor está abierta o cerrada. |
| X-Trans-ID | Identificador de transacción único para la solicitud. |
| Longitud de contenido | La longitud del cuerpo de respuesta. |
| x-ntap-sg-consistency | <p>El nivel de control de consistencia que se aplica al contenedor. Se admiten los siguientes valores:</p> <p>Todos: Todos los nodos reciben los datos inmediatamente o la solicitud falla.</p> <p>Strong-global: Garantiza la coherencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.</p> <p>Strong-site: Garantiza la coherencia de lectura después de escritura para todas las solicitudes de cliente dentro de un sitio.</p> <p>Read-after-new-write: (Predeterminado) 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.</p> <p>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.</p> |

Ejemplo de respuesta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

PONGA la solicitud de consistencia del contenedor

La solicitud DE PUT Container permite especificar el nivel de coherencia que se aplicará a las operaciones realizadas en un contenedor. De forma predeterminada, se crean nuevos contenedores utilizando el nivel de coherencia «entre una y otra escritura».

Solicitud

| Solicitar encabezado HTTP | Descripción |
|---------------------------|--|
| Token X-Auth | El token de autenticación Swift de la cuenta que se va a utilizar para la solicitud. |
| x-ntap-sg-consistency | <p>El nivel de control de coherencia que se va a aplicar a las operaciones en el contenedor. Se admiten los siguientes valores:</p> <p>Todos: Todos los nodos reciben los datos inmediatamente o la solicitud falla.</p> <p>Strong-global: Garantiza la coherencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.</p> <p>Strong-site: Garantiza la coherencia de lectura después de escritura para todas las solicitudes de cliente dentro de un sitio.</p> <p>Read-after-new-write: (Predeterminado) 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.</p> <p>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.</p> |
| Host | El nombre de host al que se dirige la solicitud. |

Cómo interactúan los controles de consistencia y las reglas de ILM para afectar a la protección de datos

Ambas opciones "[control de la coherencia](#)" Y la regla de ILM afectan a la forma en que se protegen los

objetos. Estos ajustes pueden interactuar.

Por ejemplo, el control de consistencia utilizado cuando se almacena un objeto afecta la ubicación inicial de los metadatos del objeto, mientras que el "[comportamiento de ingesta](#)" seleccionada para la regla de ILM afecta la ubicación inicial de las copias del objeto. Dado que StorageGRID requiere acceso tanto a los metadatos de un objeto como a sus datos para cumplir con las solicitudes de los clientes, seleccionar los niveles de protección correspondientes para el nivel de coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas más predecibles del sistema.

Ejemplo de cómo pueden interactuar el control de consistencia y la regla de ILM

Suponga que tiene una cuadrícula de dos sitios con la siguiente regla de ILM y la siguiente configuración de nivel de coherencia:

- **Norma ILM:** Cree dos copias de objetos, una en el sitio local y otra en un sitio remoto. Se ha seleccionado el comportamiento de procesamiento estricto.
- **Nivel de coherencia:** "Strong-global" (los metadatos de objetos se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en el grid, StorageGRID realiza copias de objetos y distribuye los metadatos en ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra la pérdida en el momento del mensaje de procesamiento correcto. Por ejemplo, si el sitio local se pierde poco después del procesamiento, seguirán existiendo copias de los datos del objeto y los metadatos del objeto en el sitio remoto. El objeto se puede recuperar completamente.

Si en su lugar usa la misma regla de ILM y el nivel de consistencia de «otrong-site», es posible que el cliente reciba un mensaje de éxito después de replicar los datos del objeto en el sitio remoto, pero antes de que los metadatos del objeto se distribuyan allí. En este caso, el nivel de protección de los metadatos de objetos no coincide con el nivel de protección de los datos de objetos. Si el sitio local se pierde poco después del procesamiento, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre los niveles de coherencia y las reglas del ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Ejemplo de solicitud

```
PUT /v1/28544923908243208806/_Swift container_  
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29  
x-ntap-sg-consistency: strong-site  
Host: test.com
```

Respuesta

| Encabezado HTTP de respuesta | Descripción |
|------------------------------|--|
| Date | La fecha y la hora de la respuesta. |
| Connection | Si la conexión con el servidor está abierta o cerrada. |

| Encabezado HTTP de respuesta | Descripción |
|------------------------------|---|
| X-Trans-Id | Identificador de transacción único para la solicitud. |
| Content-Length | La longitud del cuerpo de respuesta. |

Ejemplo de respuesta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

Configure la seguridad de la API DE REST

Debe revisar las medidas de seguridad implementadas para la API REST y entender cómo proteger el sistema.

Cómo proporciona StorageGRID seguridad para la API DE REST

Debe entender cómo el sistema StorageGRID implementa la seguridad, la autenticación y la autorización para la API DE REST.

StorageGRID usa las siguientes medidas de seguridad.

- Las comunicaciones de cliente con el servicio Load Balancer utilizan HTTPS si HTTPS está configurado para el extremo de equilibrio de carga.

Cuando usted ["configurar un punto final de equilibrio de carga"](#), HTTP se puede activar opcionalmente. Por ejemplo, puede usar HTTP para pruebas u otros fines que no sean de producción.

- De manera predeterminada, StorageGRID utiliza HTTPS para las comunicaciones cliente con los nodos de almacenamiento.

Opcionalmente, ["Active HTTP para estas conexiones"](#). Por ejemplo, puede usar HTTP para pruebas u otros fines que no sean de producción.

- Las comunicaciones entre StorageGRID y el cliente se cifran mediante TLS.
- Las comunicaciones entre el servicio Load Balancer y los nodos de almacenamiento de la cuadrícula están cifradas si el extremo de equilibrio de carga está configurado para aceptar conexiones HTTP o HTTPS.
- Los clientes deben proporcionar encabezados de autenticación HTTP a StorageGRID para realizar operaciones de API DE REST.

Certificados de seguridad y aplicaciones cliente

Los clientes pueden conectarse al servicio Load Balancer en los nodos de gateway o de administración, directamente a los nodos de almacenamiento.

En todos los casos, las aplicaciones cliente pueden realizar conexiones TLS mediante un certificado de servidor personalizado cargado por el administrador de grid o un certificado generado por el sistema StorageGRID:

- Cuando las aplicaciones cliente se conectan al servicio Load Balancer, lo hacen utilizando el certificado que se configuró para el extremo de equilibrio de carga específico utilizado para realizar la conexión. Cada extremo tiene su propio certificado, que es un certificado de servidor personalizado cargado por el administrador de grid o un certificado que el administrador de grid generó en StorageGRID al configurar el extremo.
- Cuando las aplicaciones cliente se conectan directamente a un nodo de almacenamiento, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (que están firmados por la entidad de certificación del sistema), o bien, un único certificado de servidor personalizado proporcionado para la cuadrícula por un administrador de grid.

Los clientes deben configurarse para que confíen en la entidad emisora de certificados que firmó el certificado que utilicen para establecer conexiones TLS.

Consulte ["configuración de puntos finales del equilibrador de carga"](#) y.. ["adición de un único certificado de servidor personalizado"](#) Para conexiones TLS directamente a nodos de almacenamiento.

Resumen

En la siguiente tabla, se muestra cómo se implementan los problemas de seguridad en las API DE REST de S3 y Swift:

| Problema de seguridad | Implementación de la API DE REST |
|----------------------------|--|
| Seguridad de la conexión | TLS |
| Autenticación del servidor | Certificado de servidor X.509 firmado por CA del sistema o certificado de servidor personalizado suministrado por el administrador |
| Autenticación de clientes | <ul style="list-style-type: none">• S3: Cuenta de S3 (ID de clave de acceso y clave de acceso secreta)• Swift: Cuenta de Swift (nombre de usuario y contraseña) |
| Autorización de cliente | <ul style="list-style-type: none">• S3: Propiedad de bloque y todas las políticas de control de acceso aplicables• Swift: Acceso a roles de administrador |

Algoritmos de cifrado y hash compatibles para bibliotecas TLS

El sistema StorageGRID admite un conjunto limitado de conjuntos de cifrado que las aplicaciones cliente pueden utilizar al establecer una sesión de seguridad de la capa de transporte (TLS). Para configurar los cifrados, vaya a **CONFIGURACIÓN > SEGURIDAD > CONFIGURACIÓN DE SEGURIDAD** y seleccione **Políticas TLS y SSH**.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3.



SSLv3 y TLS 1.1 (o versiones anteriores) ya no son compatibles.

Información relacionada

["Configure las conexiones y las cuentas de inquilino"](#)

Supervisar y auditar operaciones

Puede supervisar las cargas de trabajo y las eficiencias de las operaciones del cliente al ver las tendencias de las transacciones de todo el grid o de nodos específicos. Puede utilizar mensajes de auditoría para supervisar las operaciones y transacciones del cliente.

Supervise las tasas de procesamiento y recuperación de objetos

Es posible supervisar las tasas de procesamiento y recuperación de objetos, así como las métricas para el número de objetos, consultas y verificación. Puede ver el número de intentos fallidos y correctos por las aplicaciones cliente para leer, escribir y modificar objetos en el sistema StorageGRID.

Pasos

1. Inicie sesión en Grid Manager mediante una ["navegador web compatible"](#).
2. En el panel de control, seleccione **Rendimiento > S3 operaciones** o **Rendimiento > Operaciones Swift**.

En esta sección se resume el número de operaciones de cliente que realiza su sistema StorageGRID. La media de las tasas de protocolo se hace durante los últimos dos minutos.

3. Seleccione **NODES**.
4. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **Load Balancer**.

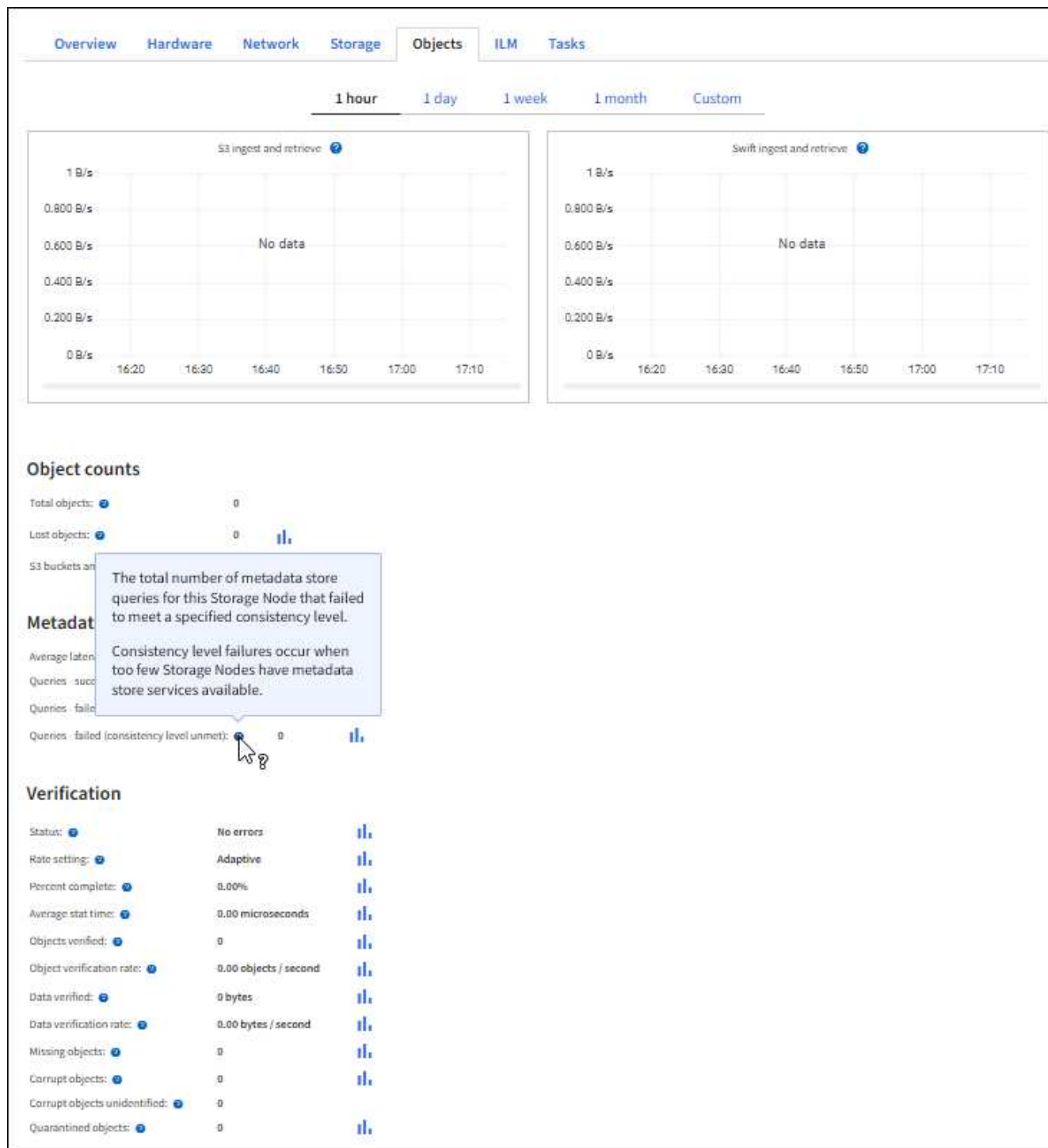
Los gráficos muestran tendencias para todo el tráfico de cliente dirigido a los extremos de equilibrador de carga dentro de la cuadrícula. Es posible seleccionar un intervalo de tiempo en horas, días, semanas, meses o años. también puede aplicar un intervalo personalizado.

5. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **objetos**.

El gráfico muestra las tasas de procesamiento y recuperación de todo el sistema StorageGRID en bytes por segundo y bytes totales. Es posible seleccionar un intervalo de tiempo en horas, días, semanas, meses o años. también puede aplicar un intervalo personalizado.

6. Para ver información sobre un nodo de almacenamiento en particular, seleccione el nodo en la lista de la izquierda y haga clic en la ficha **objetos**.

El gráfico muestra las tasas de procesamiento y recuperación de objetos de este nodo de almacenamiento. La pestaña también incluye métricas para el recuento de objetos, consultas y verificación. Puede hacer clic en las etiquetas para ver las definiciones de estas métricas.



7. Si desea aún más detalles:

- Seleccione **SUPPORT > Tools > Topología de cuadrícula**.
- Seleccione **síte > Descripción general > Principal**.

La sección API Operations muestra información resumida de la cuadrícula completa.

- Seleccione **Storage Node > LDR > Client Application > Overview > Main**

La sección Operaciones muestra información de resumen del nodo de almacenamiento seleccionado.

Acceder y revisar registros de auditoría

Los servicios de StorageGRID generan los mensajes de auditoría y se almacenan en archivos de registro de texto. Los mensajes de auditoría específicos de API de los registros de auditoría ofrecen datos críticos de seguridad, operación y supervisión del rendimiento que pueden ayudar a evaluar el estado del sistema.

Antes de empezar

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP de un nodo de administrador.

Acerca de esta tarea

La "[archivo de registro de auditoría activo](#)" se nombra `audit.log`, Y se almacena en los nodos Admin.

Una vez al día, se guarda el archivo `audit.log` activo y se inicia un nuevo archivo `audit.log`. El nombre del archivo guardado indica cuándo se guardó, en el formato `yyyy-mm-dd.txt`.

Después de un día, el archivo guardado se comprime y cambia su nombre, en el formato `yyyy-mm-dd.txt.gz`, que conserva la fecha original.

En este ejemplo, se muestra el archivo `audit.log` activo, el archivo del día anterior (`2018-04-15.txt`) y el archivo comprimido del día anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Pasos

1. Inicie sesión en un nodo de administrador:
 - a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
 - d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

2. Vaya al directorio que contiene los archivos del registro de auditoría: `cd /var/local/audit/export`
3. Ver el archivo de registro de auditoría actual o guardado, según sea necesario.

Se realizó un seguimiento de las operaciones de Swift en los registros de auditoría

Se realiza un seguimiento de todas las operaciones correctas DE ELIMINACIÓN, OBTENCIÓN, ENCABEZADO, PUBLICACIÓN y PUESTA DE almacenamiento en la "[Registro de auditoría de StorageGRID](#)". Los fallos no se registran, ni las solicitudes INFO, AUTH ni OPTIONS.

Se realiza un seguimiento de la información para las siguientes operaciones de Swift.

Operaciones de cuentas

- "OBTENGA la cuenta"
- "CUENTA principal"

Operaciones de contenedor

- "ELIMINAR contenedor"
- "OBTENGA el contenedor"
- "Contenedor DE LA CABEZA"
- "COLOQUE el contenedor"

Operaciones de objeto

- "ELIMINAR objeto"
- "OBJETO GET"
- "OBJETO HEAD"
- "PONER objeto"

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.