



Utilice StorageGRID

StorageGRID

NetApp
October 03, 2025

Tabla de contenidos

Utilice StorageGRID	1
Usar una cuenta de inquilino	1
Uso del Administrador de arrendatarios	1
Gestión del acceso al sistema para usuarios de inquilinos	16
Gestión de cuentas de inquilinos de S3	38
Gestión de servicios de plataforma S3	67
Use S3	108
Compatibilidad con la API REST de S3	109
Configurar las conexiones y las cuentas de inquilino	113
Cómo StorageGRID implementa la API DE REST de S3	119
Operaciones y limitaciones compatibles con la API REST de S3	126
Operaciones de la API de REST de StorageGRID S3	180
Políticas de acceso a bloques y grupos	203
Configurar la seguridad para la API DE REST	229
Supervisión y auditoría de operaciones	232
Ventajas de las conexiones HTTP activas, inactivas y simultáneas	235
Use Swift	238
Compatibilidad con la API de OpenStack Swift en StorageGRID	238
Configurar las conexiones y las cuentas de inquilino	242
Operaciones compatibles con la API REST de Swift	247
Operaciones de la API de REST de StorageGRID Swift	259
Configurar la seguridad para la API DE REST	264
Supervisión y auditoría de operaciones	267

Utilice StorageGRID

Usar una cuenta de inquilino

Aprenda a usar una cuenta de inquilino de StorageGRID.

- "["Uso del Administrador de arrendatarios"](#)"
- "["Gestión del acceso al sistema para usuarios de inquilinos"](#)"
- "["Gestión de cuentas de inquilinos de S3"](#)"
- "["Gestión de servicios de plataforma S3"](#)"

Uso del Administrador de arrendatarios

El Administrador de inquilinos le permite gestionar todos los aspectos de una cuenta de inquilino de StorageGRID.

Puede usar el Administrador de inquilinos para supervisar el uso del almacenamiento de una cuenta de inquilino y para gestionar los usuarios con federación de identidades o creando grupos y usuarios locales. En las cuentas de inquilinos S3, también se pueden gestionar claves S3, gestionar bloques S3 y configurar servicios de plataforma.

Usar una cuenta de inquilino de StorageGRID

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.

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

Opcionalmente, las cuentas de arrendatarios 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 instrucciones para implementar aplicaciones cliente S3.

- **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.

Creación de cuentas de inquilino

Las cuentas de inquilino las crea un administrador de grid de StorageGRID mediante Grid Manager. Al crear una cuenta de inquilino, el administrador de grid especifica la siguiente información:

- Nombre para mostrar del arrendatario (el ID de cuenta del arrendatario se asigna automáticamente y no se puede modificar).
- Si la cuenta de inquilino usa S3 o Swift.
- Para las cuentas de inquilino de S3: Si la cuenta de inquilino está permitida para usar los servicios de la plataforma. Si se permite el uso de servicios de plataforma, la cuadrícula debe configurarse para que admita su uso.
- Opcionalmente, una 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 está habilitada la federación de identidades para el sistema StorageGRID, el grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.
- Si el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la contraseña inicial del usuario raíz local del inquilino.

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.

Configuración de inquilinos de S3

Después de crear una cuenta de inquilino de S3, puede 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) o crear grupos y usuarios locales
- Gestión de claves de acceso de S3
- Creación y gestión de bloques de S3, incluidos los bloques conformes a la normativa
- Uso de servicios de plataforma (si está activado)
- Supervisión del uso de almacenamiento



Aunque puede crear y gestionar bloques de S3 con el administrador de inquilinos, debe tener claves de acceso de S3 y usar la API REST de S3 para procesar y gestionar objetos.

Configurar inquilinos Swift

Después de crear una cuenta de inquilino de Swift, los usuarios con 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 tener el permiso acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso Root Access no permite que los usuarios se autentiquen 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.

Información relacionada

["Administre StorageGRID"](#)

["Use S3"](#)

["Use Swift"](#)

Requisitos del navegador web

Debe utilizar un navegador web compatible.

Navegador Web	Versión mínima admitida
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Debe establecer la ventana del navegador en un ancho recomendado.

Ancho del navegador	Píxeles
Mínimo	1024
Óptimo	1280

Iniciando sesión en el Administrador de arrendatarios

Para acceder al Administrador de inquilinos, introduzca la URL del inquilino en la barra de direcciones de un navegador web compatible.

Lo que necesitará

- Debe tener sus credenciales de inicio de sesión.
- Debe tener una dirección URL para acceder al Administrador de inquilinos, tal y como le ha suministrado 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 contiene el nombre de dominio completo (FQDN) o la dirección IP utilizada para acceder a un nodo de administrador, y también puede incluir, de manera opcional, un número de puerto, el ID de cuenta de inquilino de 20 dígitos o ambos.

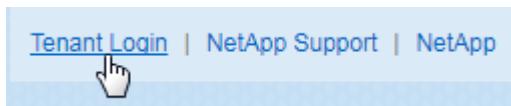
- Si la URL no incluye el ID de cuenta de 20 dígitos del inquilino, debe tener este ID de cuenta.
- Debe utilizar un navegador web compatible.
- Las cookies deben estar habilitadas en su navegador web.
- Debe tener permisos de acceso específicos.

Pasos

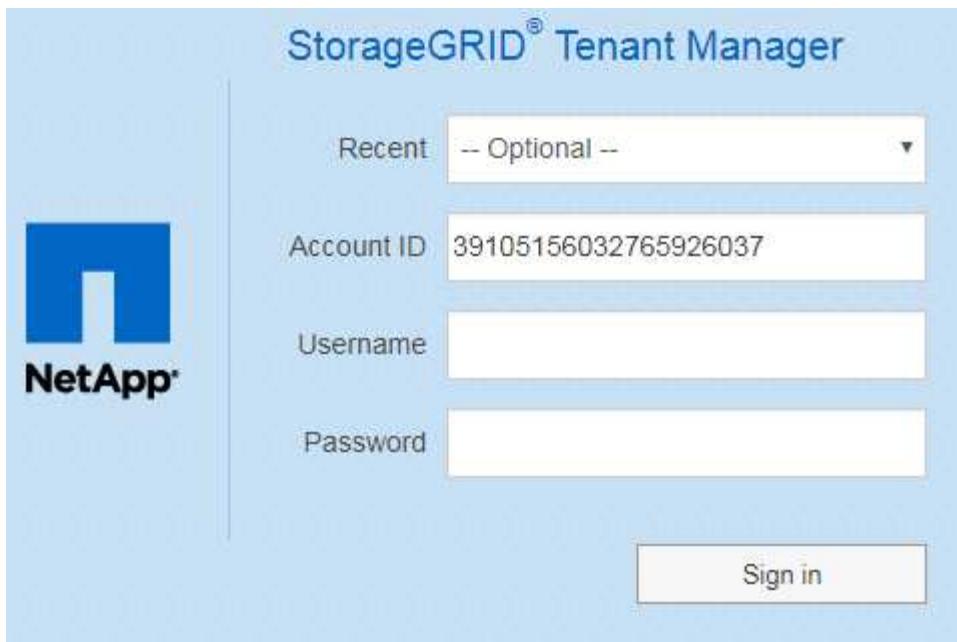
1. Inicie un explorador web compatible.
2. En la barra de dirección del navegador, introduzca la URL para acceder al Administrador de inquilinos.
3. Si se le solicita una alerta de seguridad, instale el certificado con el asistente de instalación del explorador.
4. Inicie sesión en el Administrador de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

La pantalla de inicio de sesión que ve depende de la dirección URL introducida y de si su empresa utiliza el inicio de sesión único (SSO). Verá una de las siguientes pantallas:

- La página de inicio de sesión de Grid Manager. Haga clic en el enlace **Ingreso de inquilino** de la parte superior derecha.



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



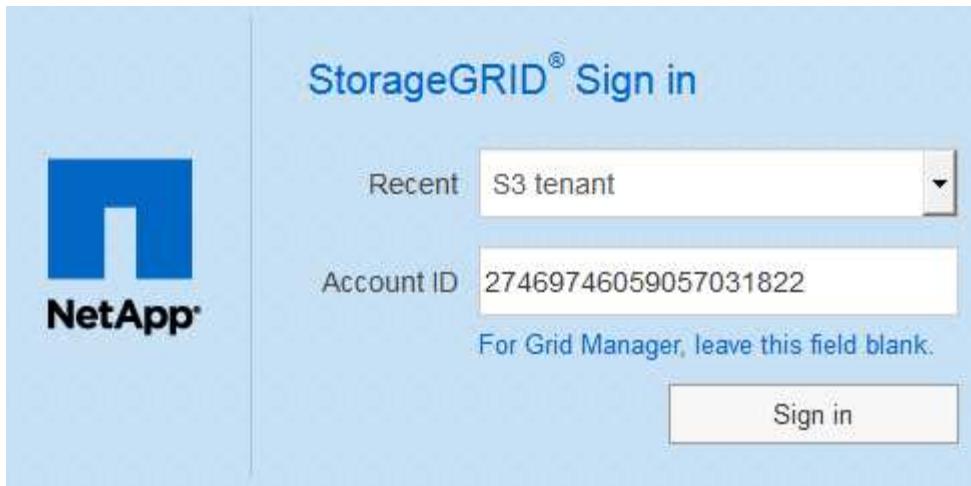
- i. Si no se muestra el ID de cuenta de 20 dígitos del arrendatario, seleccione el nombre de la cuenta de arrendatario si aparece en la lista de cuentas recientes o introduzca el ID de cuenta.
- ii. Introduzca su nombre de usuario y contraseña.
- iii. Haga clic en **Iniciar sesión**.

Aparecerá la consola del administrador de inquilinos.

- Si el inicio de sesión único de su organización está habilitado en el grid. Por ejemplo:

Introduzca sus credenciales de SSO estándar y haga clic en **Iniciar sesión**.

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



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

Aparecerá la consola del administrador de inquilinos.

5. Si ha recibido una contraseña inicial de otra persona, cambie la contraseña para proteger su cuenta. Seleccione **username > Change Password**.



Si SSO está habilitado para el sistema StorageGRID, no puede cambiar la contraseña del administrador de inquilinos.

Información relacionada

["Administre StorageGRID"](#)

["Requisitos del navegador web"](#)

Cierre de sesión en el Administrador de arrendatarios

Una vez que haya terminado de trabajar con el Administrador de inquilinos, debe cerrar sesión para garantizar 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, a continuación, seleccione **Cerrar sesión**.

Opción	Descripción
SSO no en uso	Ha cerrado sesión en el nodo de administrador. Se muestra la página de inicio de sesión del administrador de inquilinos. Nota: Si ha iniciado sesión en más de un nodo de administración, debe cerrar sesión en cada nodo.
SSO 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. Nota: Si está activado SSO y también ha iniciado sesión en Grid Manager, también debe cerrar sesión en Grid Manager para cerrar sesión en SSO.

Consola del administrador de inquilinos

La consola de tenant Manager proporciona una información general de la configuración de una cuenta de inquilino y la cantidad de espacio utilizado por los objetos en los bloques de inquilino (S3) o contenedores (Swift). Si el cliente tiene una cuota, en Dashboard se muestra cuánto de la cuota se usa y cuánto queda. Si hay algún error relacionado con la cuenta de inquilino, los errores se muestran en la consola.



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 cargan objetos, la consola se parece al siguiente ejemplo:

Dashboard

16 Buckets
[View buckets](#)

2 Platform services endpoints
[View endpoints](#)

0 Groups
[View groups](#)

1 User
[View users](#)

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Total objects

8,418,886
objects

Tenant details

Name	Human Resources
ID	4955 9096 9804 4285 4354

View the instructions for Tenant Manager.

[Go to documentation](#)

Resumen de la cuenta de inquilino

La parte superior de la consola 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 de la consola contiene la siguiente información:

- Número total de objetos para el arrendatario.

Para una cuenta de S3, si no se han ingerido objetos y tiene el permiso de acceso raíz, se muestran las directrices de introducción en lugar del número total de objetos.

- El nombre de la cuenta de inquilino y su ID.
- Un enlace a la documentación de StorageGRID.

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.



La utilización de cuotas 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, es posible que se impida temporalmente que un arrendatario cargue nuevos objetos hasta que se vuelva a calcular la utilización de cuota. El cálculo de la utilización de cuotas puede 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.

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**. Para obtener más información, consulte la referencia de alertas en las instrucciones para supervisar y solucionar problemas de StorageGRID.



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

Si supera la cuota, no podrá cargar nuevos objetos.



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



Para ver detalles adicionales y gestionar reglas y notificaciones para alertas, consulte las instrucciones para supervisar y solucionar problemas de StorageGRID.

Errores de punto final

Si ha utilizado Grid Manager para configurar uno o más extremos para utilizarlos con los servicios de la plataforma, el Panel de arrendatarios muestra una alerta si se han producido errores 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 detalles sobre un error de punto final, seleccione endpoints para mostrar la página endpoints.

Información relacionada

["Resolución de problemas de errores de extremos de servicios de plataforma"](#)

["Solución de problemas de monitor"](#)

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.

La 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.

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

Pasos

1. Inicie sesión en el Administrador de inquilinos.
2. Seleccione **Ayuda > Documentación de API** en el encabezado Administrador de inquilinos.

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 arrendatario actual, incluyendo 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").

Consulte «"Protección contra la falsificación de solicitudes entre sitios"» para obtener información sobre la mejora de la seguridad de la autenticación.



Si está habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, debe realizar diferentes pasos para la autenticación. Consulte «"autenticación en la API si está activado el inicio de sesión único"» en las instrucciones para administrar StorageGRID.

- **Config** — Operaciones relacionadas con la versión del producto y las versiones de la API de Gestión de arrendatarios. Puede mostrar la versión de la versión del producto y las versiones principales de la API que admite esa versión.
- **Containers** — Operaciones en bloques de S3 o contenedores Swift, como se indica a continuación:

Protocolo	Permito lo permite
S3	<ul style="list-style-type: none">• Creación de cucharones que cumplen las normativas y no cumplen las normativas• Modificación de la configuración de conformidad heredada• Configurar el control de coherencia para las operaciones realizadas en objetos• Creación, actualización y eliminación de la configuración de CORS de un bloque• Habilitar y deshabilitar las actualizaciones de la última hora de acceso para los objetos• Gestionar la configuración de los servicios de plataforma, incluida la replicación de CloudMirror, las notificaciones y la integración de búsqueda (metadatos-notification)• Eliminación de cucharones vacíos
Swift	Configurar el nivel de coherencia utilizado para contenedores

- **Características desactivadas** — Operaciones para ver las funciones que podrían haberse desactivado.

- **Endpoints** — Operaciones para administrar un punto final. Los extremos permiten que un bloque de S3 use un servicio externo para la replicación de CloudMirror de StorageGRID, notificaciones o integración de búsqueda.
- **Grupos** — Operaciones para administrar grupos de inquilinos locales y recuperar grupos de inquilinos federados de un origen de identidades externo.
- **Identity-source** — Operaciones para configurar un origen de identidad externo y sincronizar manualmente la información del grupo federado y del usuario.
- **Regiones** — Operaciones para determinar qué regiones se han configurado para el sistema StorageGRID.
- **s3** — Operaciones para administrar claves de acceso S3 para usuarios inquilinos.
- **s3-object-lock** — Operaciones para determinar cómo se configura el bloqueo global de objetos (cumplimiento) de S3 para el sistema StorageGRID.
- **Usuarios** — Operaciones para ver y administrar usuarios de arrendatarios.

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

Example Value Model

```
[{"responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.0"}]
```

Emitir 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. Haga clic en 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 hacer clic en **Modelo** para conocer los requisitos de cada campo.

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

Información relacionada

["Protección contra falsificación de solicitudes entre sitios \(CSRF\)"](#)

["Administre StorageGRID"](#)

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 arrendatarios se bONTAP cuando se realizan cambios que son **no compatibles** con versiones anteriores. La versión menor de la API de administración de arrendatarios se bONTAP cuando se hacen cambios que **are sea compatible** 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

Determinar qué versiones de API son compatibles con 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
  ]
}
```

Especificar una versión de API para una 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 "{\n    \"username\": \"MyUserName\",\\n    \"password\": \"MyPassword\",\\n    \"cookie\": true,\\n    \"csrfToken\": true\n}" "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.

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



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.

Gestión del acceso al sistema para usuarios de inquilinos

Permite a los usuarios acceder a una cuenta de inquilino mediante la importación de grupos desde un origen de identidad federado y la asignación de permisos de administración. También puede crear usuarios y grupos de inquilinos locales, a menos que el inicio de sesión único (SSO) esté vigente para todo el sistema StorageGRID.

- "[Mediante la federación de identidades](#)"
- "[Gestión de grupos](#)"
- "[Gestión de usuarios locales](#)"

Mediante 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 un origen de identidad federado](#)"
- "[Forzar la sincronización con el origen de identidades](#)"
- "[Desactivar la federación de identidades](#)"

Configurar un origen de identidad federado

Puede configurar la federación de identidades si desea que los grupos de arrendatarios y los usuarios se gestionen en otro sistema, como Active Directory, OpenLDAP u Oracle Directory Server.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener permisos de acceso específicos.
- Debe utilizar Active Directory, OpenLDAP o Oracle Directory Server como proveedor de identidades. Si desea utilizar un servicio LDAP v3 que no esté en la lista, debe ponerse en contacto con el soporte técnico.
- 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.

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 al acceder a la página Federación de identidades, no podrá 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.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > federación de identidades**.
2. Seleccione **Activar federación de identidades**.
3. En la sección Tipo de servicio LDAP, seleccione **Active Directory, OpenLDAP o otros**.

Si selecciona **OpenLDAP**, configure el servidor OpenLDAP. Consulte las directrices para configurar un servidor OpenLDAP.

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 .
 - **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. En la sección Configure LDAP Server, introduzca la información sobre el servidor LDAP y las conexiones de red necesarias.

- **Hostname:** El nombre de host del servidor 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
- **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.

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

- **Usar STARTTLS (recomendado):** Usar STARTTLS para asegurar las comunicaciones con el servidor LDAP. Esta es la opción recomendada.
- **Use LDAPS:** La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Esta opción es compatible por motivos de compatibilidad.
- **No utilice TLS:** El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido.

Esta opción 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 CA predeterminado 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.

8. Seleccione **probar conexión** para validar la configuración de conexión para el servidor LDAP.

Si la conexión es válida, aparecerá un mensaje de confirmación en la esquina superior derecha de la página.

9. Si la conexión es válida, seleccione **Guardar**.

La siguiente captura de pantalla muestra valores de configuración de ejemplo para un servidor LDAP que utiliza Active Directory.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory OpenLDAP Other

Configure LDAP server (All fields are required)

Hostname	Port
my-active-directory.example.com	389
Username	
MyDomain\Administrator	
Password	*****
Group Base DN	DC=storagegrid,DC=example,DC=com
User Base DN	DC=storagegrid,DC=example,DC=com

Información relacionada

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

["Instrucciones para configurar un servidor OpenLDAP"](#)

Instrucciones para configurar un servidor OpenLDAP

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

Revestimientos memberOf y refit

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

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 revertidos en la Guía del administrador para OpenLDAP.

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.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener permisos de acceso específicos.
- El origen de identidad guardado debe estar activado.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > federación de identidades**.

Aparece la página federación de identidades. El botón **servidor de sincronización** se encuentra en la parte superior derecha de la página.



Si el origen de identidad guardado no está activado, el botón **servidor de sincronización** no estará activo.

2. Seleccione **servidor de sincronización**.

Aparece un mensaje de confirmación que indica que la sincronización se ha iniciado correctamente.

Información relacionada

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

Desactivar la federación de identidades

Si ha configurado un servicio de federación de identidades para este inquilino, puede deshabilitar temporalmente o de forma permanente la federación de identidades para los grupos de inquilinos y usuarios. Cuando se deshabilita la federación de identidades, no hay comunicación entre el sistema 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.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

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

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que hayan iniciado sesión actualmente conservarán el acceso a la cuenta de inquilino hasta que caduque la sesión, pero no podrán iniciar sesión después de que caduque la sesión.
- La sincronización entre el sistema StorageGRID y el origen de identidad no se llevará a cabo.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > federación de identidades**.
2. Desactive la casilla de verificación **Activar federación de identidades**.
3. Seleccione **Guardar**.

Información relacionada

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

Gestión de grupos

Se asignan permisos a grupos de usuarios para controlar qué tareas pueden realizar los usuarios de inquilinos. Puede importar grupos federados desde un origen de identidades, como Active Directory u OpenLDAP, o bien crear grupos locales.



Si se habilitó el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan acceder a los recursos de S3 y Swift, según los permisos de grupo.

Permisos de gestión de inquilinos

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

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

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

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



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

Puede asignar los siguientes permisos a un grupo. Tenga en cuenta que los inquilinos de S3 y los inquilinos de Swift tienen diferentes permisos de grupo. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

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 acceso raíz para iniciar sesión en la cuenta de arrendatario.
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	Solo inquilinos 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
Administrar todos los depósitos	<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 Cuchos.</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: sólo puede asignar el permiso Administrar todos los cucharones a grupos Swift desde la API de gestión de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.</p>
Gestionar extremos	<p>Solo inquilinos de S3. Permite a los usuarios usar el administrador de inquilinos o la API de gestión de inquilinos crear o editar extremos que se usan como destino de los servicios de plataforma StorageGRID.</p> <p>Los usuarios que no tienen este permiso no ven la opción de menú terminales de servicios de plataforma.</p>

Información relacionada

["Use S3"](#)

["Use Swift"](#)

Creación de grupos para un inquilino de S3

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

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Pasos

- Seleccione **ADMINISTRACIÓN de ACCESO > grupos**.

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups

Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous 1 Next →

2. Seleccione **Crear grupo**.
3. 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.
4. 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.
5. Seleccione **continuar**.
6. Seleccione un modo de acceso. 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.
 - **Read-write** (valor predeterminado): Los usuarios pueden iniciar sesión en el Administrador de inquilinos y administrar la configuración de arrendatario.
 - **Sólo lectura:** Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en el Administrador de inquilinos ni en la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.
7. Seleccione los permisos de grupo para este grupo.

Consulte la información sobre los permisos de administración de inquilinos.

8. Seleccione **continuar**.
9. Seleccione una política de grupo para determinar qué permisos de acceso S3 tendrán los miembros de este grupo.

- **Sin acceso S3:** Predeterminado. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se conceda el acceso mediante una política de bloques. 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.
 - **Personalizado:** A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto. Consulte las instrucciones para implementar una aplicación cliente S3 para obtener información detallada acerca de las políticas de grupo, incluidos la sintaxis del idioma y ejemplos.
10. 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 válido.

En este ejemplo, sólo se permite a los miembros del grupo enumerar y acceder a una carpeta que coincida con su nombre de usuario (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.

The screenshot shows the AWS Groups configuration page. On the left, there is a dropdown menu for selecting S3 access level. The options are: "No S3 Access" (radio button), "Read Only Access" (radio button), "Full Access" (radio button), and "Custom" (radio button, which is selected). Below the "Custom" option is a note: "(Must be a valid JSON formatted string.)". To the right of the dropdown is a large text area containing a JSON policy document. The JSON code is as follows:

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3>ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

11. Seleccione el botón que aparece, dependiendo de si está creando un grupo federado o un grupo local:

- Grupo federado: **Crear grupo**
- Grupo local: **Continuar**

Si está creando un grupo local, el paso 4 (Aregar usuarios) aparece después de seleccionar **continuar**.

Este paso no aparece para grupos federados.

12. Seleccione la casilla de verificación de cada usuario que desee agregar al grupo y, a continuación, seleccione **Crear grupo**.

Opcionalmente, puede guardar el grupo sin agregar usuarios. Puede agregar usuarios al grupo más tarde o seleccionar el grupo cuando agregue nuevos usuarios.

13. Seleccione **Finalizar**.

El grupo creado aparece en la lista de grupos. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

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

["Use S3"](#)

Creación de grupos para un inquilino 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.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Pasos

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

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups

Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous 1 Next →

2. Seleccione **Crear grupo**.
3. 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.
4. 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.
5. Seleccione **continuar**.
6. Seleccione un modo de acceso. 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.
 - **Read-write** (valor predeterminado): Los usuarios pueden iniciar sesión en el Administrador de inquilinos y administrar la configuración de arrendatario.
 - **Sólo lectura:** Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en el Administrador de inquilinos ni en la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

7. Establezca el permiso Grupo.
 - Active la casilla de verificación **acceso raíz** si los usuarios necesitan iniciar sesión en el Administrador de inquilinos o la API de administración de inquilinos. (Predeterminado)
 - Anule la selección de la casilla de verificación **acceso raíz** si los usuarios no necesitan acceso al Administrador de inquilinos o a la API de administración de inquilinos. Por ejemplo, anule la selección de la casilla de verificación de las aplicaciones que no necesitan acceder al arrendatario. A

continuación, asigne el permiso **Swift Administrator** para permitir que estos usuarios administren contenedores y objetos.

8. Seleccione **continuar**.
9. Active la casilla de verificación **Swift Administrator** si el usuario necesita poder utilizar la API de REST de Swift.

Los usuarios de Swift deben tener el permiso acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso Root Access no permite que los usuarios se autentiquen 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.

10. Seleccione el botón que aparece, dependiendo de si está creando un grupo federado o un grupo local:
 - Grupo federado: **Crear grupo**
 - Grupo local: **Continuar**

Si está creando un grupo local, el paso 4 (Agregar usuarios) aparece después de seleccionar **continuar**. Este paso no aparece para grupos federados.

11. Seleccione la casilla de verificación de cada usuario que desee agregar al grupo y, a continuación, seleccione **Crear grupo**.

Opcionalmente, puede guardar el grupo sin agregar usuarios. Puede agregar usuarios al grupo más tarde o seleccionar el grupo cuando cree nuevos usuarios.

12. Seleccione **Finalizar**.

El grupo creado aparece en la lista de grupos. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

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

["Use Swift"](#)

Ver y editar detalles del grupo

Al ver los detalles de un grupo, puede cambiar el nombre para mostrar del grupo, los permisos, las directivas y los usuarios que pertenecen al grupo.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > grupos**.
2. Seleccione el nombre del grupo cuyos detalles deseé ver o editar.

También puede seleccionar **acciones > Ver detalles del grupo**.

Aparece la página de detalles del grupo. En el siguiente ejemplo, se muestra la página de detalles del grupo S3.

Overview

Display name:	Applications
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

[Group permissions](#)[S3 group policy](#)[Users](#)

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode [?](#)

Select whether users can change settings and perform operations or whether they can only view settings and features.

 Read-write Read-only

Group permissions [?](#)

Select the tenant account permissions you want to assign to this group.

 Root Access

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

 Manage All Buckets

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

 Manage Endpoints

Allows users to configure endpoints for platform services.

 Manage Your Own S3 Credentials

Allows users to create and delete their own S3 access keys.

[Save changes](#)

3. Realice cambios en la configuración del grupo según sea necesario.



Para asegurarse de que se guardan los cambios, seleccione **Guardar cambios** después de realizar cambios en cada sección. Cuando se guarden los cambios, aparecerá un mensaje de confirmación en la esquina superior derecha de la página.

- a. De forma opcional, seleccione el nombre para mostrar o el ícono de edición para actualizar el nombre para mostrar.

No se puede cambiar el nombre exclusivo de un grupo. No se puede editar el nombre para mostrar de un grupo federado.

- b. Si lo desea, actualice los permisos.

- c. Para la política de grupo, realice los cambios adecuados para su inquilino S3 o Swift.

- Si va a editar un grupo para un inquilino de S3, seleccione de forma opcional una política de grupo S3 diferente. Si selecciona una política de S3 personalizada, actualice la cadena JSON según sea necesario.
- Si está editando un grupo para un inquilino Swift, también puede activar o desactivar la casilla de verificación **Swift Administrator**.

Para obtener más información sobre el permiso de administrador de Swift, consulte las instrucciones para crear grupos para un inquilino Swift.

- d. Opcionalmente, agregue o elimine usuarios.

4. Confirme que ha seleccionado **Guardar cambios** para cada sección que haya cambiado.

Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

["Creación de grupos para un inquilino de S3"](#)

["Creación de grupos para un inquilino Swift"](#)

Agregar usuarios a un grupo local

Puede agregar usuarios a un grupo local según sea necesario.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > grupos**.
2. Seleccione el nombre del grupo local al que desea añadir usuarios.

También puede seleccionar **acciones > Ver detalles del grupo**.

Aparece la página de detalles del grupo.

Overview

Display name:	Applications
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

[Group permissions](#)
[S3 group policy](#)
[Users](#)

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode [?](#)

Select whether users can change settings and perform operations or whether they can only view settings and features.

 Read-write Read-only

Group permissions [?](#)

Select the tenant account permissions you want to assign to this group.

Root Access

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

Manage All Buckets

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

Manage Endpoints

Allows users to configure endpoints for platform services.

Manage Your Own S3 Credentials

Allows users to create and delete their own S3 access keys.

[Save changes](#)

3. Seleccione **gestionar usuarios** y, a continuación, seleccione **Agregar usuarios**.

The screenshot shows a 'Manage users' interface. At the top, there are buttons for 'Add users' (blue) and 'Remove Users' (red). Below them is a search bar labeled 'Search Groups...' with a magnifying glass icon. To the right, it says 'Displaying 1 results'. The main area has three columns: 'Username', 'Full Name', and 'Denied'. A user named 'User_02' is listed with a full name of 'User_02_Managers' and a status of 'Denied'. The entire interface is contained within a light gray box.

4. Seleccione los usuarios que desea agregar al grupo y, a continuación, seleccione **Agregar usuarios**.

The screenshot shows an 'Add users' dialog box. It starts with the text 'Select local users to add to the group **Applications**'. Below this is a search bar labeled 'Search Groups...' with a magnifying glass icon. To the right, it says 'Displaying 1 results'. The main list has a checked checkbox next to 'User_01'. The columns are 'Username', 'Full Name', and 'Denied'. The user 'User_01' is listed with a full name of 'User_01_Applications' and a status of 'Denied'. At the bottom left is a 'Cancel' button, and at the bottom right is a blue 'Add users' button.

Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Edición de un nombre de grupo

Puede editar el nombre para mostrar de un grupo. No se puede editar el nombre único de un grupo.

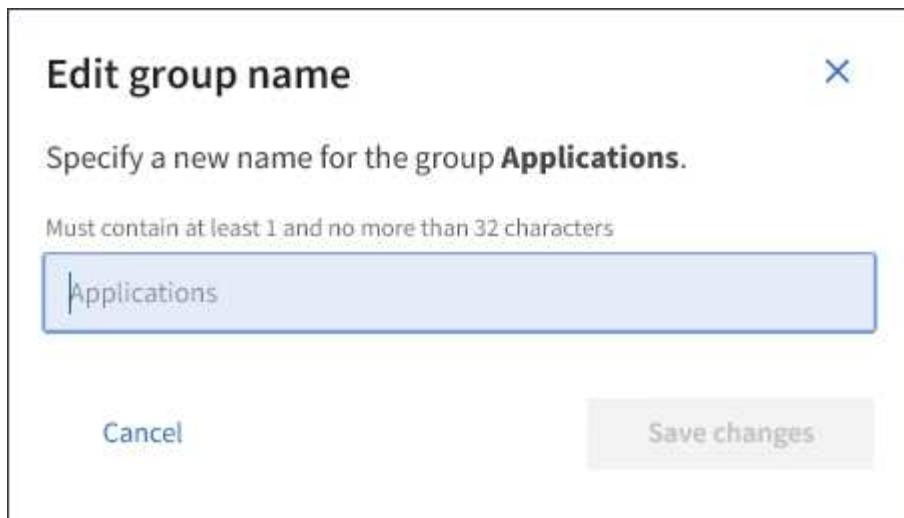
Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > grupos**.
2. Seleccione la casilla de verificación del grupo cuyo nombre para mostrar desee editar.
3. Seleccione **acciones > Editar nombre de grupo**.

Aparece el cuadro de diálogo Editar nombre del grupo.



4. Si está editando un grupo local, actualice el nombre para mostrar según sea necesario.

No se puede cambiar el nombre exclusivo de un grupo. No se puede editar el nombre para mostrar de un grupo federado.

5. Seleccione **Guardar cambios**.

Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

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

Duplicación de un grupo

Puede crear nuevos grupos más rápidamente duplicando un grupo existente.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO > grupos**.
2. Seleccione la casilla de verificación del grupo que desea duplicar.
3. Seleccione **Duplicar grupo**. Para obtener detalles adicionales sobre cómo crear un grupo, consulte las instrucciones para crear grupos para un inquilino S3 o para un inquilino Swift.
4. 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.

5. 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.

6. Seleccione **continuar**.

7. Según sea necesario, modifique los permisos para este grupo.

8. Seleccione **continuar**.

9. Según sea necesario, si va a duplicar un grupo para un inquilino S3, seleccione opcionalmente una directiva diferente de los botones de opción * Agregar directiva S3*. Si seleccionó una política personalizada, actualice la cadena JSON como sea necesario.

10. Seleccione **Crear grupo**.

Información relacionada

["Creación de grupos para un inquilino de S3"](#)

["Creación de grupos para un inquilino Swift"](#)

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

Eliminar un grupo

Puede eliminar un grupo del sistema. Cualquier usuario que sólo pertenezca a ese grupo ya no podrá iniciar sesión en el Administrador de inquilinos ni utilizar la cuenta de arrendatario.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

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

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups

Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous 1 Next →

2. Seleccione las casillas de verificación de los grupos que desea eliminar.

3. Seleccione **acciones > Eliminar grupo**.

Aparecerá un mensaje de confirmación.

4. Seleccione **Eliminar grupo** para confirmar que desea eliminar los grupos indicados en el mensaje de confirmación.

Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

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

Gestión de usuarios locales

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

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios de lectura y escritura que tenga el permiso acceso raíz.

 Si se habilitó el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el administrador de inquilinos o la API de gestión de inquilinos, aunque puedan usar las aplicaciones cliente S3 o Swift para acceder a los recursos del inquilino, en función de los permisos de grupo.

Acceso a la página usuarios

Seleccione **ADMINISTRACIÓN de ACCESO > usuarios**.

The screenshot shows the 'Users' page with the following interface elements:

- Title:** Users
- Description:** View local and federated users. Edit properties and group membership of local users.
- Count:** 3 users
- Create user:** A blue button in the top right corner.
- Actions dropdown:** A grey button labeled 'Actions ▾'.
- Table:** A list of users with columns: Username, Full Name, Denied, and Type.

	Username	Full Name	Denied	Type
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	User_01	User_01		Local
<input type="checkbox"/>	User_02	User_02		Local

Creación de usuarios locales

Es posible crear usuarios locales y asignarles 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 gestión ni políticas de grupo S3 aplicadas. 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 pertenecen a ningún grupo no tienen permisos de gestión ni acceso al contenedor de Swift.

Pasos

1. Seleccione **Crear usuario**.
2. Complete los siguientes campos.

- **Nombre completo:** El nombre completo de este usuario, por ejemplo, el nombre y apellido de una persona o el nombre de una aplicación.
- **Nombre de usuario:** El nombre que este usuario utilizará para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar.
- **Contraseña:** Contraseña que se utiliza cuando el usuario inicia sesión.
- **Confirmar contraseña:** Escriba la misma contraseña que escribió en el campo Contraseña.

- **Denegar acceso:** Si selecciona **Sí**, este usuario no puede iniciar sesión en la cuenta de arrendatario, aunque el usuario pueda seguir perteneciendo a uno o más grupos.

Por ejemplo, puede utilizar esta función para suspender temporalmente la capacidad de un usuario para iniciar sesión.

3. Seleccione **continuar**.

4. Asigne el usuario a uno o más grupos locales.

Los usuarios que no pertenecen a ningún grupo no tendrán permisos de administración. Los permisos son acumulativos. Los usuarios tendrán todos los permisos para todos los grupos a los que pertenezcan.

5. Seleccione **Crear usuario**.

Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Editar los detalles del usuario

Al editar los detalles de un usuario, puede cambiar el nombre completo y la contraseña del usuario, agregar el usuario a grupos diferentes e impedir que el usuario acceda al arrendatario.

Pasos

1. En la lista usuarios, seleccione el nombre del usuario cuyos detalles desee ver o editar.

Como alternativa, puede seleccionar la casilla de verificación para el usuario y, a continuación, seleccionar **acciones > Ver detalles del usuario**.

2. Realice los cambios necesarios en la configuración del usuario.

- Cambie el nombre completo del usuario según sea necesario seleccionando el nombre completo o el icono de edición En la sección Descripción general.

No puede cambiar el nombre de usuario.

- En la ficha **Contraseña**, cambie la contraseña del usuario según sea necesario.
- En la ficha **Access**, permita que el usuario inicie sesión (seleccione **no**) o impida que el usuario inicie sesión (seleccione **Sí**) según sea necesario.
- En la ficha **grupos**, agregue el usuario a grupos o elimine el usuario de los grupos según sea necesario.
- Según sea necesario para cada sección, seleccione **Guardar cambios**.

Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Duplicación de usuarios locales

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

Pasos

- En la lista usuarios, seleccione el usuario que desea duplicar.
- Seleccione **Duplicar usuario**.
- Modifique los campos siguientes para el nuevo usuario.

- **Nombre completo:** El nombre completo de este usuario, por ejemplo, el nombre y apellido de una persona o el nombre de una aplicación.
- **Nombre de usuario:** El nombre que este usuario utilizará para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar.
- **Contraseña:** Contraseña que se utiliza cuando el usuario inicia sesión.
- **Confirmar contraseña:** Escriba la misma contraseña que escribió en el campo Contraseña.
- **Denegar acceso:** Si selecciona **Sí**, este usuario no puede iniciar sesión en la cuenta de arrendatario, aunque el usuario pueda seguir perteneciendo a uno o más grupos.

Por ejemplo, puede utilizar esta función para suspender temporalmente la capacidad de un usuario para iniciar sesión.

4. Seleccione **continuar**.

5. Seleccione uno o más grupos locales.

Los usuarios que no pertenecen a ningún grupo no tendrán permisos de administración. Los permisos son acumulativos. Los usuarios tendrán todos los permisos para todos los grupos a los que pertenezcan.

6. Seleccione **Crear usuario**.

Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Eliminación de usuarios locales

Es posible eliminar de forma permanente usuarios locales que ya no necesiten acceder a la cuenta de inquilino de StorageGRID.

Con el Administrador de inquilinos, puede eliminar usuarios locales, pero no usuarios federados. Debe utilizar el origen de identidad federado para eliminar usuarios federados.

Pasos

1. En la lista usuarios, seleccione la casilla de verificación del usuario local que desea eliminar.
2. Seleccione **acciones > Eliminar usuario**.
3. En el cuadro de diálogo de confirmación, seleccione **Eliminar usuario** para confirmar que desea eliminar al usuario del sistema.

Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

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

Gestión de cuentas de inquilinos de S3

Puede usar el administrador de inquilinos para gestionar claves de acceso S3, así como para crear y gestionar bloques de S3.

- ["Gestión de claves de acceso de S3"](#)
- ["Gestión de bloques de S3"](#)

Gestión de claves de acceso de S3

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

Acerca de esta tarea

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

- Los usuarios que tengan el permiso **Administrar sus propias credenciales de S3** pueden crear o quitar sus propias claves de acceso S3.
- Los usuarios que tienen el permiso **acceso raíz** pueden administrar las claves de acceso para la cuenta raíz de S3 y el resto de usuarios. Las claves de acceso raíz proporcionan acceso completo a todos los bloques y objetos para el inquilino, a menos que se des habilite 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.

Crear 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 bloques y los objetos de la cuenta de inquilino de S3.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener el permiso gestionar sus propias credenciales de S3.

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 motivos de seguridad, no cree más claves de las necesarias y elimine las claves que no esté 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 para la seguridad en su entorno es bajo y no necesita crear nuevas claves periódicamente, no tendrá que establecer un tiempo de caducidad para sus 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.

The screenshot shows the 'Create access key' dialog box. At the top, there are two tabs: 'Choose expiration time' (selected) and 'Download access key'. Below the tabs, the heading 'Choose expiration time' is displayed. There are two radio button options: 'Do not set an expiration time' (unchecked) and 'Set an expiration time' (checked). A note below the first option says 'This access key will never expire.' To the right of the radio buttons are input fields for date ('MM/DD/YYYY'), calendar icon, time ('HH : MM'), and AM/PM ('AM'). At the bottom right of the dialog are 'Cancel' and 'Create access key' buttons.

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.

Create access key X

1 Choose expiration time 2 Download access key

Download access key
To save the keys for future reference, select **Download .csv**, or copy and paste the values to another location.

Info You will not be able to view the Access key ID or Secret access key after you close this dialog.

Access key ID
SHTBQKDRVHQ34YKKUAWX Copy

Secret access key
UGu9+XeACtnOWQYFdbzmgmgVXXDvCkSOzT1OsZ9K Copy

Download .csv Finish

6. Seleccione **Finalizar**.

La nueva clave aparece en la página Mis claves de acceso. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

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

Ver 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, puede crear nuevas claves o eliminar claves que ya no utilice.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener el permiso gestionar sus propias credenciales de S3.

i 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.

My access keys

Manage your personal S3 access keys. If a key will expire soon, you can create a new key and delete the one it is replacing.

4 keys

Create key

Delete key

<input type="checkbox"/>	Access key ID	Expiration time
<input type="checkbox"/>	*****OTLS	2020-11-23 12:00:00 MST
<input type="checkbox"/>	*****OM45	2020-12-01 19:00:00 MST
<input type="checkbox"/>	*****69QJ	None
<input type="checkbox"/>	*****3R8P	None

2. Ordene las teclas por tiempo de caducidad o ID de clave de acceso.

3. Según sea necesario, cree nuevas claves y elimine manualmente las claves que ya no utilice.

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.

Información relacionada

["Crear sus propias claves de acceso S3"](#)

["Eliminar sus propias claves de acceso de S3"](#)

[Eliminar 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.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener el permiso gestionar sus propias credenciales de S3.



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

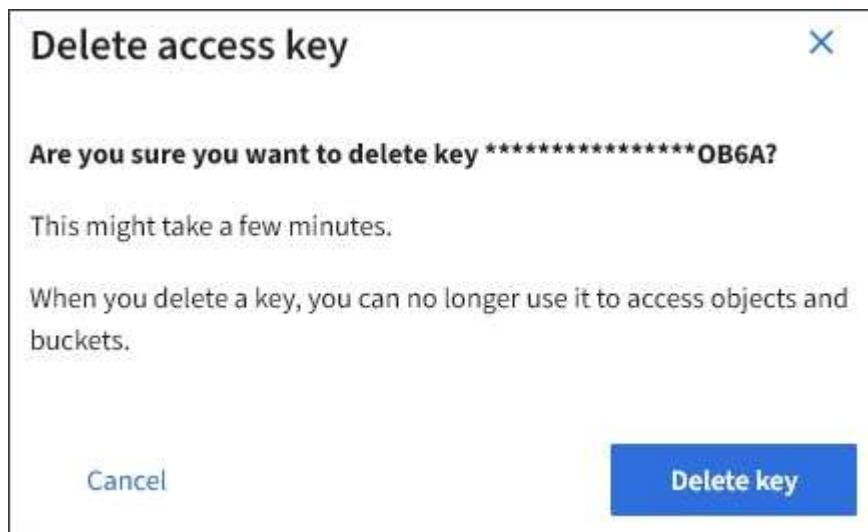
Pasos

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

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

2. Seleccione la casilla de comprobación de cada clave de acceso que desea quitar.
3. Seleccione tecla **Eliminar**.

Se muestra un cuadro de diálogo de confirmación.



4. Seleccione tecla **Eliminar**.

Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

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

Crear 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.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener el permiso 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 motivos de seguridad, no cree más claves de las que necesita el usuario y elimine las claves que no se estén 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.

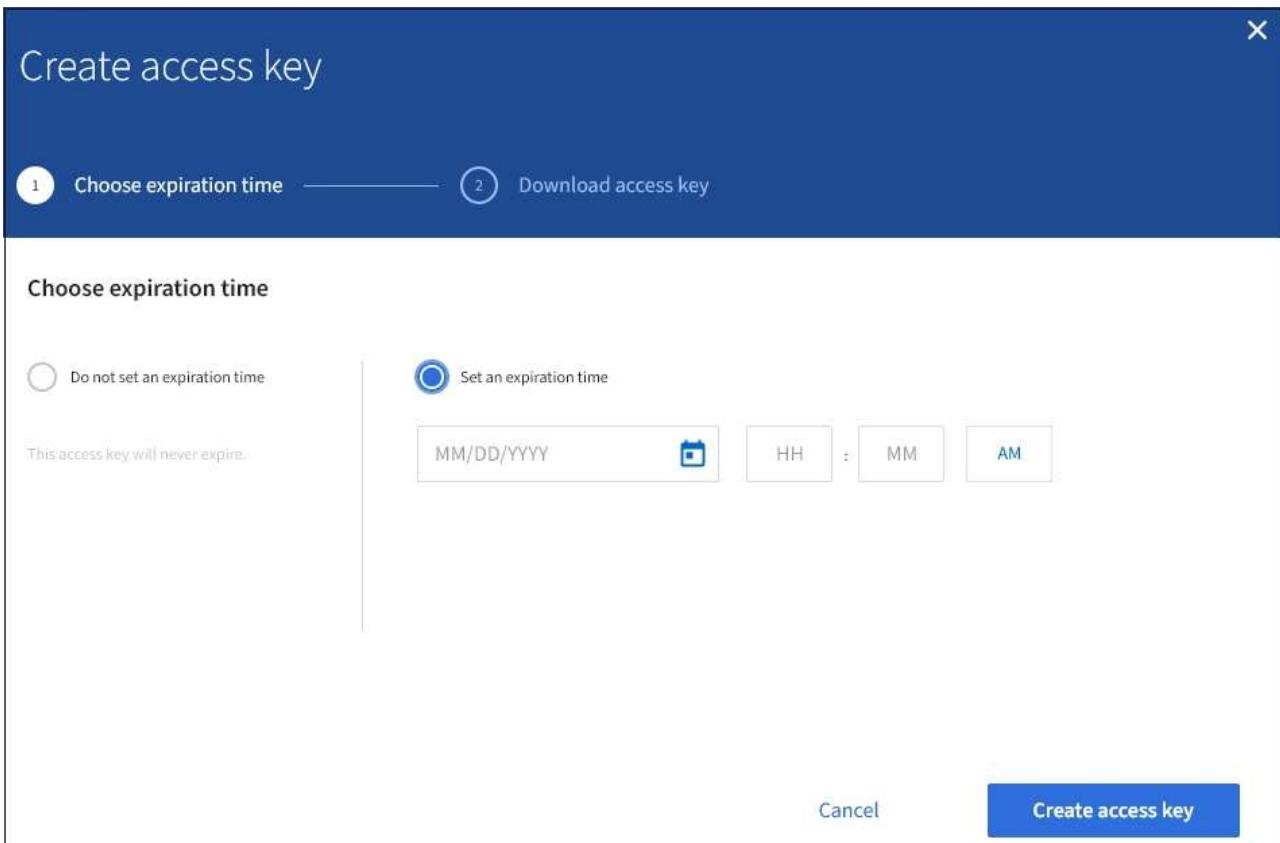
Cada clave puede tener un tiempo de caducidad específico o no puede caducar. Siga estas directrices para el tiempo de caducidad:

- 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 para la seguridad en su entorno es bajo y no necesita crear nuevas claves periódicamente, no tendrá que establecer un tiempo de caducidad para 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 establezca 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.



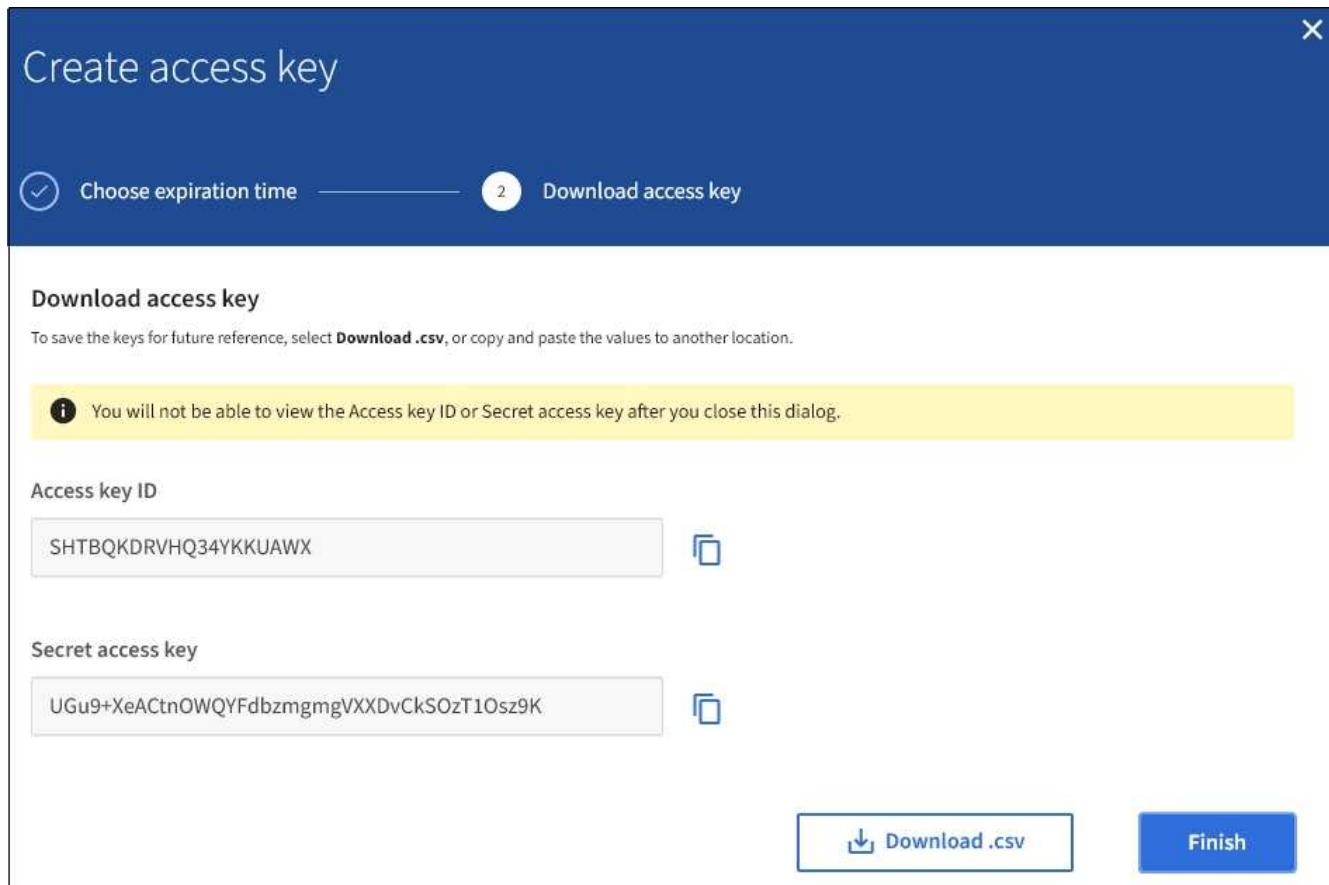
5. Seleccione **Crear clave de acceso**.

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.



7. Seleccione **Finalizar**.

La nueva clave aparece en la ficha teclas de acceso de la página de detalles del usuario. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

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

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.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener 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**.

Aparece la página Users (usuarios) y enumera los usuarios existentes.

2. Seleccione el usuario cuyas claves de acceso de S3 desee ver.

Aparece la página de detalles de usuario.

3. Seleccione **teclas de acceso**.

The screenshot shows the 'Access keys' tab selected in the top navigation bar. Below it, the heading 'Manage access keys' and the sub-instruction 'Add or delete access keys for this user.' are displayed. A 'Create key' button is visible. The table lists four access keys:

Access key ID	Expiration time
*****WX5J	2020-11-21 12:00:00 MST
*****6OHM	2020-11-23 13:00:00 MST
*****J505	None
*****4MTF	None

Text at the bottom right of the table area says 'Displaying 4 results'.

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

["Crear las claves de acceso S3 de otro usuario"](#)

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

Eliminación de 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.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe tener 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**.

Aparece la página Users (usuarios) y enumera los usuarios existentes.

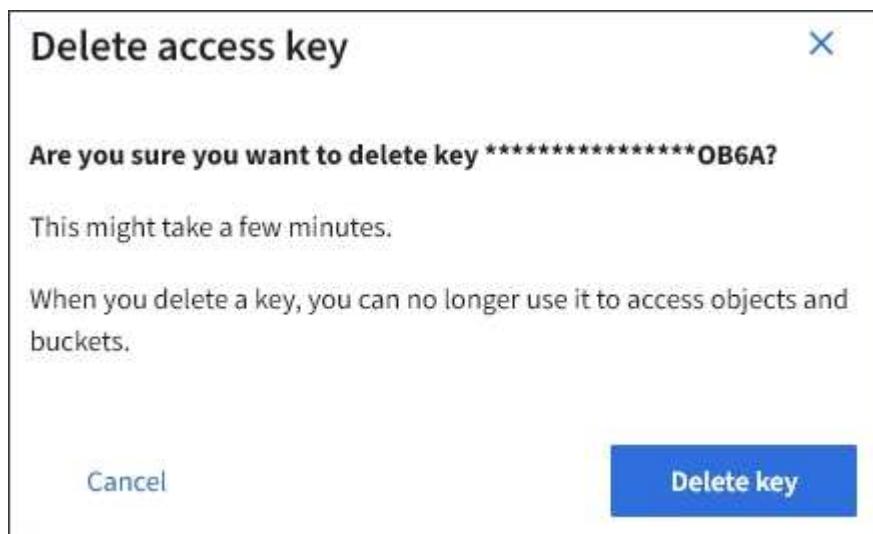
2. Seleccione el usuario cuyas claves de acceso de S3 desee gestionar.

Aparece la página de detalles de usuario.

3. Seleccione **teclas de acceso** y, a continuación, active la casilla de verificación de cada clave de acceso que desee eliminar.

4. Seleccione **acciones > Borrar clave seleccionada**.

Se muestra un cuadro de diálogo de confirmación.



5. Seleccione **tecla Eliminar**.

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

tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

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

Gestión de bloques de S3

Si usa un inquilino de S3 con los permisos adecuados, puede crear, ver y eliminar bloques de S3, actualizar la configuración de nivel de coherencia, configurar el uso compartido de recursos de origen cruzado (CORS), habilitar y deshabilitar las opciones de actualización del tiempo de acceso anterior y gestionar servicios de plataforma de S3.

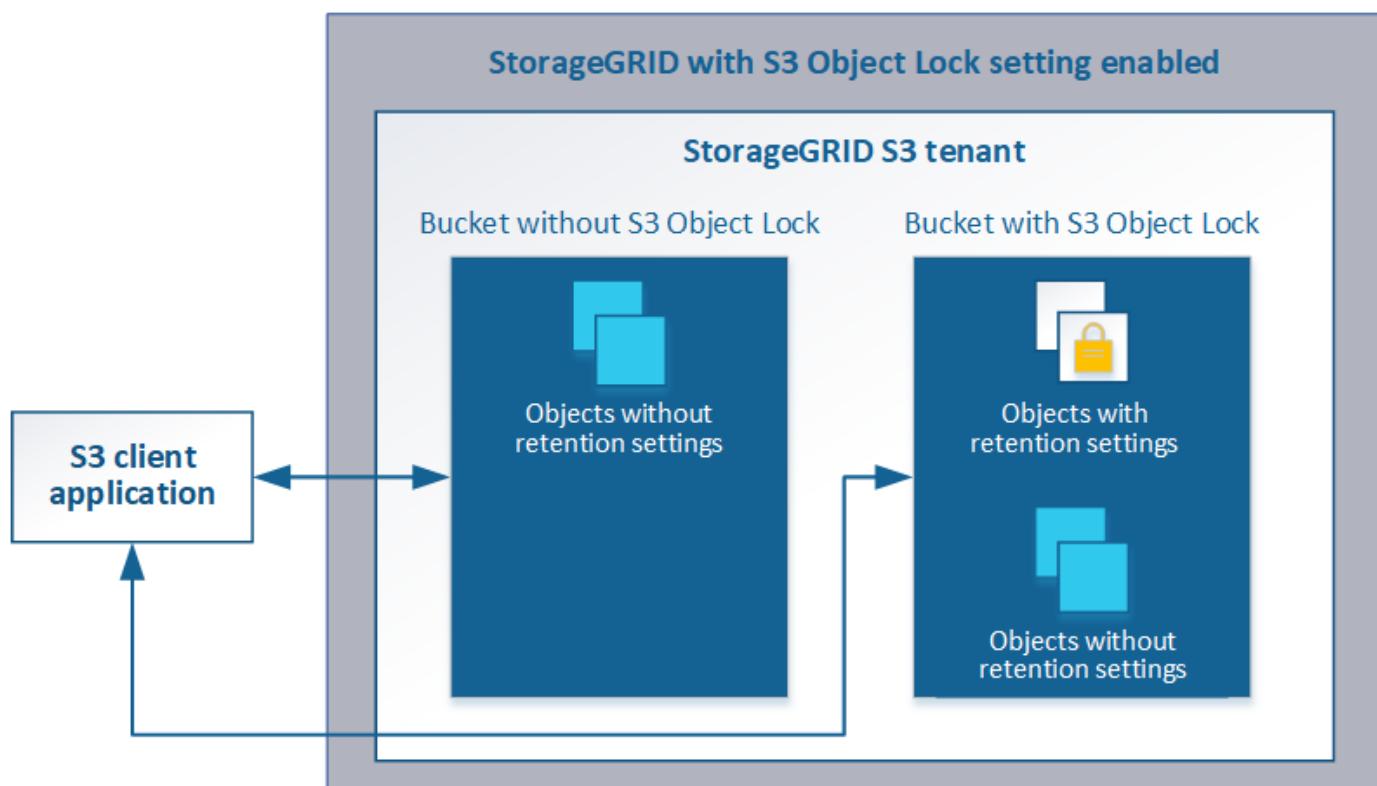
Uso del bloqueo de objetos de S3

Puede usar la función de bloqueo de objetos S3 en StorageGRID si los objetos deben cumplir 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 bloque tiene habilitada la función S3 Object Lock, las aplicaciones cliente S3 pueden especificar, opcionalmente, la configuración de retención para cualquier versión del objeto en ese bloque. Una versión de objeto debe tener la configuración de retención especificada para estar protegida por S3 Object Lock.



La función de bloqueo de objetos StorageGRID S3 ofrece un único modo de retención equivalente al modo de cumplimiento de normativas Amazon S3. De forma predeterminada, cualquier usuario no puede sobrescribir ni eliminar una versión de objeto protegido. La función de bloqueo de objetos StorageGRID S3 no es compatible con un modo de gobierno y no permite a los usuarios con permisos especiales omitir la configuración de retención o eliminar objetos protegidos.

Si un bloque tiene habilitado el bloqueo de objetos S3, la aplicación cliente S3 puede especificar, de manera opcional, la siguiente configuración de retención a nivel de objeto al crear o actualizar un objeto:

- **Retener-hasta-fecha:** Si la fecha retener-hasta-fecha de una versión de objeto es en el futuro, el objeto puede ser recuperado, pero no puede ser modificado o eliminado. Según sea necesario, se puede aumentar la fecha de retención hasta de un objeto, pero esta fecha no se puede disminuir.
- **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.

Para obtener información detallada sobre estos ajustes, vaya a "uso del bloqueo de objetos S3" en ["Operaciones y limitaciones compatibles con la API REST de S3"](#).

Gestión de bloques que cumplen con las normativas heredadas

La función de bloqueo de objetos S3 sustituye la función Compliance disponible en versiones anteriores de StorageGRID. Si ha creado cubos compatibles con una versión anterior de StorageGRID, puede seguir gestionando la configuración de estos bloques; sin embargo, ya no puede crear nuevos bloques compatibles. Para obtener instrucciones, consulte el artículo de la base de conocimientos de NetApp.

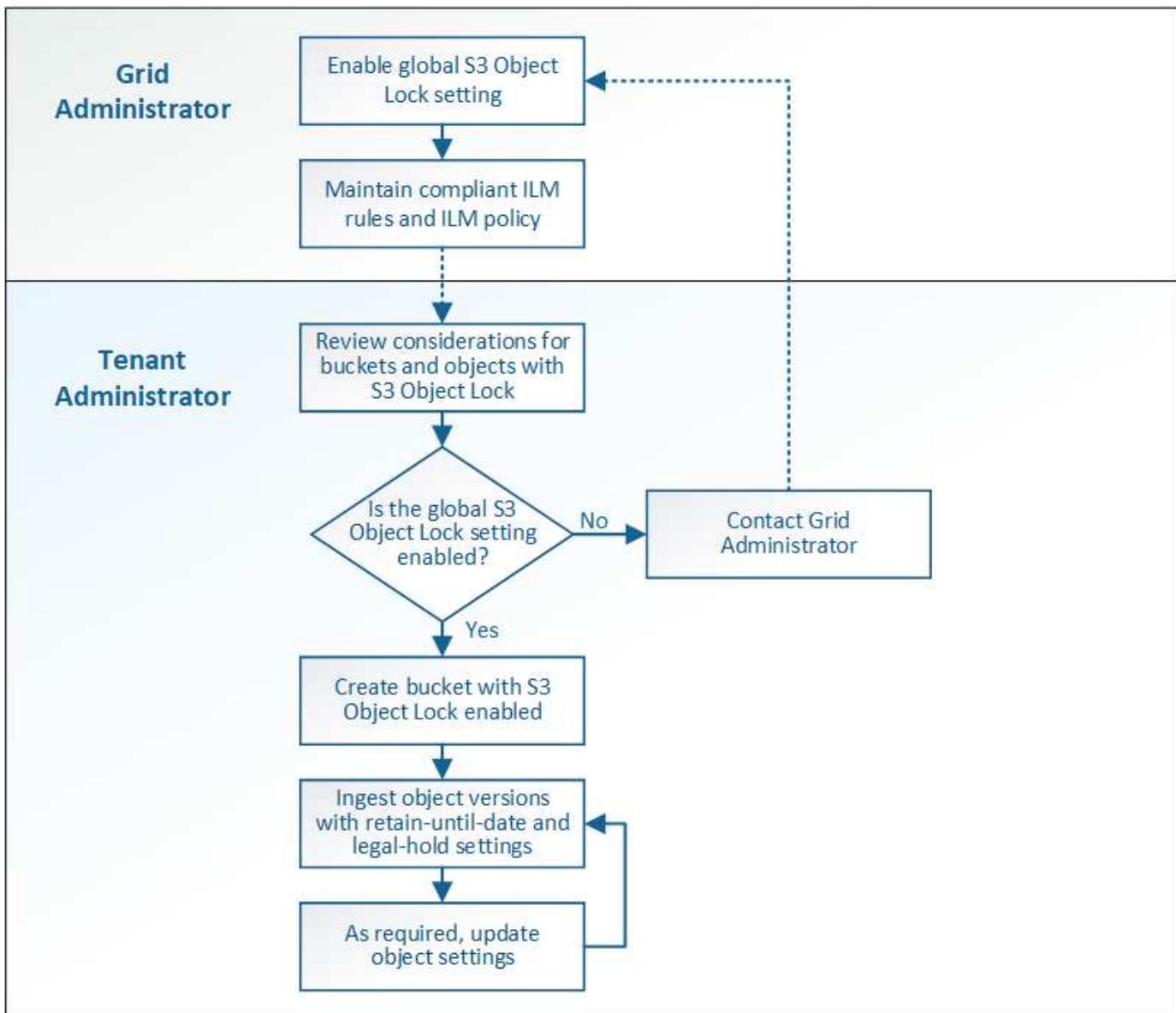
["Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"](#)

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 la gestión del ciclo de vida de la información.

Una vez que se habilita la opción global de bloqueo de objetos S3, se pueden crear bloques con el bloqueo de objetos S3 habilitado. Posteriormente, puede usar la aplicación cliente S3 para especificar opcionalmente la configuración de retención para cada versión del objeto.



Información relacionada

["Gestión de objetos con ILM"](#)

Requisitos para el bloqueo de objetos de S3

Antes de habilitar S3 Object Lock para un bloqueo, revise los requisitos para los bloques y objetos de S3 Object Lock y el ciclo de vida de los objetos en bloques con S3 Object Lock habilitado.

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.

Este ejemplo del Administrador de inquilinos muestra un bloque con el bloqueo de objetos S3 habilitado.

Buckets

Create buckets and manage bucket settings.

The screenshot shows the AWS S3 Buckets page. At the top, it says "1 bucket". On the right, there is a blue button labeled "Create bucket". Below the header is a table with the following columns: Actions, Name, S3 Object Lock, Region, Object Count, Space Used, and Date Created. The "Name" column lists "bank-records". The "S3 Object Lock" column for "bank-records" has a yellow border and contains a checkmark. The "Region" column shows "us-east-1", "Object Count" shows "0", "Space Used" shows "0 bytes", and "Date Created" shows "2021-01-06 16:53:19 MST". At the bottom of the table are navigation links: "Previous" and "Next" with a page number "1".

Actions	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

- Si planea utilizar el bloqueo de objetos S3, debe habilitar el bloqueo de objetos S3 al crear el bloque. No es posible habilitar el bloqueo de objetos de S3 para un bloque existente.
- Se requiere el versionado de bloques con S3 Object Lock. Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque.
- Después de crear un bloque con el bloqueo de objetos S3 habilitado, no se puede deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones de ese bloque.
- Un bloque StorageGRID con el bloqueo de objetos S3 habilitado no tiene un período de retención predeterminado. En su lugar, la aplicación cliente S3 puede especificar opcionalmente una fecha de retención y una configuración de conservación legal para cada versión del objeto que se agrega a ese bloque.
- Se admite la configuración del ciclo de vida de bloques para los bloques del ciclo de vida de objetos S3.
- 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

- La aplicación cliente S3 debe especificar la configuración de retención de cada objeto que tenga que protegerse mediante el bloqueo de objetos S3.
- Puede aumentar la fecha de retención hasta una versión de objeto, pero nunca puede disminuir este valor.
- Si recibe una notificación de una acción legal pendiente o una investigación normativa, puede conservar la información relevante colocando una retención legal en una versión del objeto. Cuando una versión de objeto se encuentra bajo una retención legal, ese objeto no se puede eliminar de StorageGRID, aunque haya alcanzado su fecha de retención. Tan pronto como se levante la retención legal, la versión del objeto se puede eliminar si se ha alcanzado la fecha de retención.
- El bloqueo de objetos de S3 requiere el uso de bloques con versiones. 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 bloque con el bloqueo de objetos S3 habilitado atraviesa tres etapas:

1. Procesamiento de objetos

- Al añadir una versión de objeto a un bloque con el bloqueo de objetos S3 habilitado, la aplicación cliente S3 puede especificar, de manera opcional, la configuración de retención del objeto (retener hasta la fecha, la conservación legal o ambos). A continuación, StorageGRID genera metadatos para ese objeto, que incluye un identificador de objeto (UUID) único y la fecha y la hora de procesamiento.
- Después de procesar una versión de objeto con configuración de retención, sus datos y los metadatos definidos por el usuario de S3 no se pueden modificar.
- StorageGRID almacena los metadatos del objeto de forma independiente de los datos del objeto. Mantiene tres copias de todos los metadatos de objetos en cada sitio.

2. Retención de objetos

- StorageGRID almacena varias copias del objeto. El número y el tipo exactos de copias y las ubicaciones del almacenamiento se determinan según las reglas conformes de la política de ILM activa.

3. Eliminación de objetos

- Un objeto se puede eliminar cuando se alcanza su fecha de retención.
- No se puede eliminar un objeto que se encuentra bajo una retención legal.

Crear un bloque de S3

Puede usar el administrador de inquilinos para crear bloques S3 para los datos de objetos. Al crear un bloque, debe especificar el nombre y la región del bloque. Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, de manera opcional, puede habilitar el bloqueo de objetos S3 para el bloque.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.
- Si planea crear un bloque con bloqueo de objetos S3, la configuración global de bloqueo de objetos S3 debe haber estado habilitada para el sistema StorageGRID y debe haber revisado los requisitos para los bloques y objetos de bloqueo de objetos S3.

["Uso del bloqueo de objetos de S3"](#)

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Cuchos**.

Aparece la página Cuchos y muestra todos los cestillos que ya se han creado.

Buckets

Create buckets and manage bucket settings.

0 buckets

Create bucket

Actions ▾

Name

S3 Object Lock

Region

Object Count

Space Used

Date Created

No buckets found

Create bucket

2. Seleccione Crear cucharón.

Se mostrará el asistente Create bucket.

Create bucket

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name

Region

us-east-1

Cancel

Create bucket



Si la opción de configuración global de bloqueo de objetos S3 está habilitada, Create bucket incluye un segundo paso para la gestión del bloqueo de objetos S3 para el bloque.

3. Introduzca un nombre único para el bloque.



No se puede cambiar el nombre del bloque después de crear el bloque.

Los nombres de los bloques deben cumplir con las siguientes reglas:

- Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino).
- Debe ser compatible con DNS.
- Debe 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 períodos en solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor.



Para obtener más información, consulte la documentación de Amazon Web Services (AWS).

4. Seleccione la región para este segmento.

El administrador de StorageGRID gestiona las regiones disponibles. La región de un bloque puede afectar la política de protección de datos aplicada a los objetos. De forma predeterminada, todos los bloques se crean en la us-east-1 región.



No se puede cambiar la región después de crear el bloque.

5. Seleccione **Crear cucharón o continuar**.

- Si el valor global de bloqueo de objetos S3 no está habilitado, seleccione **Crear bloque**. El cucharón se crea y se agrega a la tabla de la página Cuches.
- Si el valor global de bloqueo de objetos S3 está activado, seleccione **continuar**. Paso 2, se muestra Manage S3 Object Lock.

Create bucket

1 Enter details ————— 2 Manage S3 Object Lock Optional

Manage S3 Object Lock (This step is optional)

S3 Object Lock allows you to specify retention and legal hold settings for the objects ingested into a bucket. If you want to use S3 Object Lock, you must enable this setting when you create the bucket. You cannot add or disable S3 Object Lock after a bucket is created.

If S3 Object Lock is enabled, bucket versioning is required and will be enabled automatically.

Enable S3 Object Lock

[Previous](#) [Create bucket](#)

6. De manera opcional, seleccione la casilla de comprobación para habilitar S3 Object Lock para este bloque.

El bloqueo de objetos S3 debe estar habilitado para el bloque antes de que una aplicación cliente S3 pueda especificar la configuración de retención legal y hasta la fecha para los objetos agregados al bloque.



No se puede habilitar o deshabilitar S3 Object Lock después de crear el bloque.



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

7. Seleccione **Crear cucharón**.

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

Información relacionada

["Gestión de objetos con ILM"](#)

["API de gestión de inquilinos"](#)

["Use S3"](#)

Ver los detalles de bloques de S3

Puede ver una lista de las configuraciones de bloques y bloques en su cuenta de inquilino.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Cuchos**.

Aparece la página Cuchos y enumera todos los cucharones de la cuenta de arrendatario.

Buckets

Create buckets and manage bucket settings.

2 buckets

Create bucket

Actions ▾

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

← Previous 1 Next →

2. Revisar la información de cada bloque.

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

- Nombre: Nombre único del bloque, que no se puede cambiar.
- S3 Object Lock: Si está habilitado el bloqueo de objetos de S3 para este bloque.

Esta columna no se muestra si la configuración global de bloqueo de objetos S3 está deshabilitada.

Esta columna también muestra información para todos los segmentos compatibles anteriores.

- Región: La región del cucharón, que no se puede cambiar.
- Recuento de objetos: El número de objetos de este bloque.
- Espacio utilizado: Tamaño lógico de todos los objetos de este bloque. El tamaño lógico no incluye el espacio real necesario para las copias replicadas o con código de borrado o para los metadatos de objetos.
- Fecha de creación: La fecha y la hora en que se creó el segmento.



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

3. Para ver y gestionar la configuración de un bloque, seleccione el nombre del bloque.

Aparece la página de detalles bucket.

Esta página le permite ver y editar la configuración para las opciones de bloque, el acceso a bloque y los servicios de plataforma.

Consulte las instrucciones para configurar cada ajuste o servicio de plataforma.

Buckets > bucket-02

Overview

Name:	bucket-02
Region:	us-east-1
S3 Object Lock:	Disabled
Date created:	2020-11-04 14:51:59 MST

Bucket options **Bucket access** **Platform services**

Consistency level	Read-after-new-write	▼
Last access time updates	Disabled	▼

Información relacionada

["Cambiar el nivel de coherencia"](#)

["Habilitar o deshabilitar las actualizaciones de la hora del último acceso"](#)

["Configuración de uso compartido de recursos de origen cruzado \(CORS\)"](#)

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

["Configuración de notificaciones de eventos"](#)

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

Cambiar el nivel de coherencia

Si usa un inquilino de S3, puede usar el administrador de inquilinos o la API de gestión de inquilinos para cambiar el control de coherencia para las operaciones realizadas en los objetos en los bloques S3.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

El nivel de coherencia establece una compensación entre la disponibilidad de los objetos y la coherencia de dichos objetos en los diferentes nodos y sitios de almacenamiento. 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 **ALMACENAMIENTO (S3) > Cuchos**.

2. Seleccione el nombre del bloque de la lista.

Aparece la página de detalles bucket.

3. Seleccione **Opciones de bloque > nivel de coherencia**.

Bucket options **Bucket access** **Platform services**

Consistency level Read-after-new-write (default) ^

Change the consistency control for operations performed on the objects in the bucket. Consistency level makes a trade-off between the availability of the objects and the consistency of those objects across different Storage Nodes and sites.

In general, use the **Read-after-new-write** consistency level for your buckets. Then, if objects do not meet availability or consistency requirements, change the client application's behavior, or set the **Consistency-Control** header for an individual API request, which overrides the bucket setting.

- All
Provides the highest guarantee of consistency. All nodes receive the data immediately, or the request will fail.
- Strong-global
Guarantees read-after-write consistency for all client requests across all sites.
- Strong-site
Guarantees read-after-write consistency for all client requests within a site.
- Read-after-new-write (default)
Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability, and data protection guarantees.

Note: If your application attempts HEAD operations on keys that do not exist, set the Consistency Level to **Available**, unless you require AWS S3 consistency guarantees. Otherwise, a high number of 500 Internal Server errors can result if one or more Storage Nodes are unavailable.
- Available
Behaves the same as the **Read-after-new-write** consistency level, but only provides eventual consistency for HEAD operations. Offers higher availability for HEAD operations than **Read-after-new-write** if Storage Nodes are unavailable. Differs from AWS S3 consistency guarantees for HEAD operations only.

Save changes

4. Seleccione un nivel de coherencia para las operaciones realizadas en los objetos de este bloque.

Nivel de coherencia	Descripción
Todo	Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.

Nivel de coherencia	Descripción
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.
Read-after-new-write (predeterminado)	<p>Proporciona coherencia de lectura tras escritura para los objetos nuevos y consistencia final para las actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Coincide con las garantías de coherencia de Amazon S3.</p> <p>Nota: Si su aplicación intenta realizar operaciones HEAD en claves que no existen, establezca el nivel de consistencia en disponible, a menos que necesite garantías de consistencia de Amazon S3. De lo contrario, un número elevado de 500 errores internos del servidor pueden producirse si uno o más nodos de almacenamiento no están disponibles.</p>
Disponible (coherencia eventual para operaciones DE CABEZAL)	<p>Se comporta del mismo modo que el nivel de consistencia de lectura tras escritura nueva, pero sólo proporciona consistencia eventual para las operaciones DE CABEZAL. Ofrece una mayor disponibilidad para operaciones CON CABEZAL que lectura tras escritura nueva si los nodos de almacenamiento no están disponibles. Se diferencia de las garantías de coherencia de Amazon S3 solo para operaciones HEAD.</p>

5. Seleccione Guardar cambios.

Información relacionada

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

Habilitar o deshabilitar 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 sólo se aplican a los sistemas StorageGRID que incluyen al menos una regla de ILM que utiliza la opción **última hora de acceso** en sus instrucciones de colocación. Puede ignorar estas instrucciones si el sistema StorageGRID no incluye dicha regla.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Last Access Time es una de las opciones disponibles para la instrucción de colocación **Reference Time** para una regla de ILM. Si se establece el tiempo de referencia de una regla en tiempo de último acceso, los administradores de la cuadrícula pueden especificar que los objetos se coloquen en determinadas ubicaciones

de almacenamiento en función de cuándo se recuperaron por última vez esos objetos (se leen o se visualizan).

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.



Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

De forma predeterminada, las actualizaciones de la hora del último acceso están desactivadas. Si el sistema StorageGRID incluye una regla de ILM que utiliza la opción **Hora de último acceso** y desea que esta opción se aplique a los objetos de este bloque, debe habilitar las actualizaciones para el último tiempo de acceso para los bloques S3 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			

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Cuchos**.

2. Seleccione el nombre del bloque de la lista.

Aparece la página de detalles bucket.

3. Seleccione **Opciones de bloque > actualizaciones del último tiempo de acceso**.

4. Seleccione el botón de opción adecuado para activar o desactivar las actualizaciones de la hora del último acceso.

The screenshot shows the 'Bucket options' tab selected in the top navigation bar. Below it, the 'Bucket access' tab is active. The main content area displays the 'Consistency level' set to 'Read-after-new-write'. Under the 'Last access time updates' section, the status is 'Disabled'. A note below explains that this setting enables or disables last access time updates for objects in the bucket. It also specifies what happens when updates are disabled. A yellow callout box highlights the note: 'Updating the last access time when an object is retrieved can reduce performance, especially for small objects.' At the bottom, there are two radio button options: 'Enable last access time updates when retrieving an object' (unchecked) and 'Disable last access time updates when retrieving an object' (checked). A 'Save changes' button is located at the bottom right.

5. Seleccione **Guardar cambios**.

Información relacionada

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

"Gestión de objetos con ILM"

Configuración de uso compartido de recursos de origen cruzado (CORS)

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

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o 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 que las aplicaciones web de cliente de un dominio accedan 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>.

Pasos

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

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

3. Seleccione el nombre del bloque de la lista.

Aparece la página de detalles bucket.

4. Seleccione **acceso a bloque > 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 y seleccione **Guardar cambios**.

The screenshot shows the 'Bucket access' tab selected in the AWS S3 console. Under the 'Cross-Origin Resource Sharing (CORS)' section, the status is 'Disabled'. A descriptive text explains that CORS allows an S3 bucket and its objects to be accessible from web applications in other domains. Below this, there is a text input field containing XML code for CORS configuration. The XML code defines two CORS rules. Each rule specifies '*' as the allowed origin, allowing all methods (GET, POST, DELETE) and all headers. A 'Clear' button is available to remove the XML. At the bottom right is a 'Save changes' button.

```
<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>
  </CORSRule>
</CORSConfiguration>
```

7. Para modificar la configuración de CORS para el bloque, actualice el XML de configuración de CORS en el cuadro de texto o seleccione **Borrar** para volver a empezar. A continuación, seleccione **Guardar cambios**.

8. Para desactivar CORS para el cucharón, desactive la casilla de verificación **Activar CORS** y, a continuación, seleccione **Guardar cambios**.

Eliminar un bloque de S3

Puede usar el administrador de inquilinos para eliminar un bloque de S3 que esté vacío.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.

- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

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

No puede eliminar un bloque de S3 si contiene objetos o versiones de objetos no actuales. Para obtener información sobre cómo se eliminan los objetos con versiones S3, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Cuchos**.

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

Buckets

Create buckets and manage bucket settings.

2 buckets

Create bucket

Actions ▾

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

← Previous 1 Next →

2. Seleccione la casilla de verificación para el segmento vacío que desea eliminar.

El menú acciones está activado.

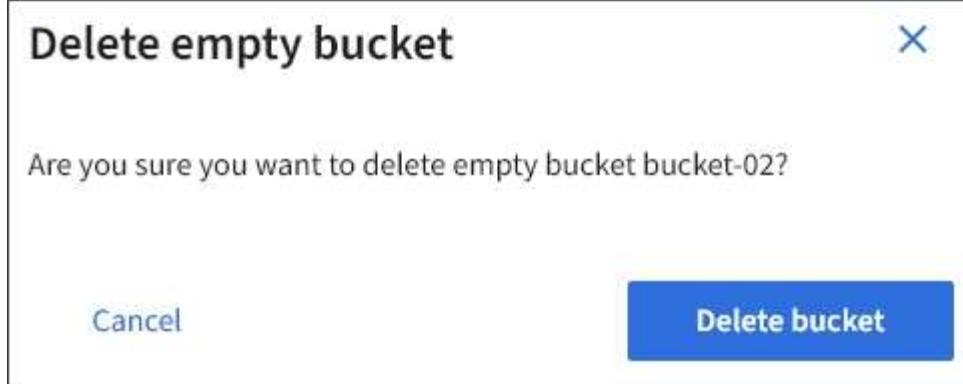
3. En el menú acciones, seleccione **Eliminar segmento vacío**.

Actions ▾

Delete empty bucket

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input checked="" type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

Aparecerá un mensaje de confirmación.



4. Si está seguro de que desea eliminar el bloque, seleccione **Eliminar bloque**.

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

Si el segmento no está vacío, aparece un mensaje de error. Debe eliminar todos los objetos antes de poder eliminar el bloque.



Unable to delete the bucket because it is not empty. You must delete all objects before you can delete this bucket.

Información relacionada

["Gestión de objetos con ILM"](#)

Gestión de servicios de plataforma S3

Si se permite el uso de servicios de plataforma para su cuenta de inquilino de S3, podrá usar servicios de plataforma para aprovechar los servicios externos y configurar la replicación de CloudMirror, notificaciones e integración de búsqueda para bloques de S3.

- ["¿Qué servicios de plataforma son"](#)
- ["Consideraciones sobre el uso de servicios de plataforma"](#)
- ["Configuración de extremos de servicios de plataforma"](#)
- ["Configurar la replicación de CloudMirror"](#)
- ["Configuración de notificaciones de eventos"](#)
- ["Utilizando el servicio de integración de búsqueda"](#)

¿Qué servicios de plataforma son

Los servicios de plataforma de StorageGRID pueden ayudarle a implementar una estrategia de cloud híbrido.

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

- **Duplicación de CloudMirror:** El servicio de replicación de CloudMirror de StorageGRID se utiliza 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:** Las notificaciones de eventos por bloque se usan para 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 Retain hasta fecha y retención legal) de los objetos no se incluirán en los mensajes de notificación.

- **Servicio de integración de búsqueda:** El servicio de integración de búsqueda se usa para enviar metadatos de objetos S3 a un índice de Elasticsearch especificado donde se pueden buscar o analizar los metadatos utilizando el 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 extremos externos que se configuran mediante el 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 extremo, puede habilitar un servicio de plataforma para un bloque agregando la 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:

1. 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.
2. Si también desea enviar notificaciones cuando estos objetos están almacenados en el bloque, debe añadir una configuración de notificaciones.
3. 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>

Consulte las instrucciones para implementar aplicaciones cliente de S3 para obtener detalles sobre cómo StorageGRID implementa estas API.

Información relacionada

["Use S3"](#)

["El servicio de replicación de CloudMirror"](#)

["Notificaciones para bloques"](#)

["Descripción del servicio de integración de búsqueda"](#)

["Consideraciones sobre el uso de servicios de plataforma"](#)

El servicio de replicación de CloudMirror

Puede habilitar la replicación de CloudMirror para un bloque de S3 si desea que

StorageGRID replica 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 ingestión de objetos se realiza correctamente.

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

 Si va a usar la replicación de CloudMirror para copiar objetos en un destino de AWS S3, tenga en cuenta que Amazon S3 limita el tamaño de los metadatos definidos por el usuario en 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 se 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 admite un CloudMirror bidireccional entre dos grids.

La singularidad y el orden de los eventos en el segmento 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.

Información relacionada

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

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 configurar las notificaciones de eventos asociando XML de configuración de notificaciones 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 las siguientes limitaciones:

- No es posible configurar una notificación para los siguientes tipos de eventos. Estos tipos de evento **no** son compatibles.
 - s3:ReducedRedundancyLostObject
 - s3:ObjectRestore:Completed
- Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar excepto que no incluyen algunas claves y utilizan valores específicos para otros, como se muestra en la 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

Información relacionada

["Configuración de notificaciones de eventos"](#)

Descripción del servicio de integración de búsqueda

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. Una vez indexado un documento, no se pueden 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, las notificaciones no se envían para ningún objeto que ya estaba 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 *Interoperability Matrix Tool* para determinar las versiones compatibles de Elasticsearch.

Información relacionada

["Herramienta de matriz de interoperabilidad de NetApp"](#)

["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"](#)

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

Consideraciones sobre el uso de servicios de plataforma

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

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>

Consideración	Detalles
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 que coincida con el comportamiento de eliminación de los servicios CRR y SNS de AWS, las solicitudes de notificación de CloudMirror y eventos no se envían cuando se elimina un objeto del bloque de origen debido a las reglas de ILM 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	El tamaño máximo de los objetos que se pueden replicar en un bloque de destino mediante el servicio de replicación de CloudMirror es 5 TB, que es el mismo que el tamaño máximo de objeto admitido por StorageGRID.
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 cucharón de origen en StorageGRID no están relacionados con los ID de versión para el cubo 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. Como los ID de versión del origen y del destino no están relacionados, no hay manera de garantizar que se replique una actualización de etiqueta a un ID de versión específico.</p> <p>Por el contrario, el servicio CloudMirror replica las solicitudes DE etiquetado PUT Object o ELIMINA las solicitudes de etiquetado de objetos que no especifican un ID de versión. Estas solicitudes actualizan las etiquetas de la clave más reciente (o la versión más reciente si el bloque está versionado). También se replican búsquedas normales con etiquetas (no actualizaciones de etiquetado).</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.
Bloque con S3 Object Lock habilitado	Si el bloque de destino S3 para la replicación de CloudMirror tiene la función S3 Object Lock habilitada, la operación de replicación generará un error ACCESSDENIED.

Información relacionada

["Use S3"](#)

Configuración de extremos de servicios de 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 extremo de servicios de plataforma, debe ser un usuario inquilino con permiso Administrar extremos o acceso raíz, en una cuadrícula cuya red se haya configurado para permitir que los nodos de almacenamiento accedan a recursos de extremo externos. 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 bloque de StorageGRID a un bloque de S3, debe crear un extremo de servicios de plataforma que incluya la información y las credenciales que StorageGRID necesita para acceder al bloque de destino en AWS.

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 extremos de AWS Lambda o simple Queue Service (SQS).

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 en los clouds de AWS u otros lugares.

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 extremo. StorageGRID creará el tipo si es necesario al enviar metadatos de objetos al extremo.

Información relacionada

["Administre StorageGRID"](#)

Se especifica el URN para un extremo de servicios de 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:mysite`, como se indica a continuación:

- Si el servicio está alojado en AWS, utilice `arn:aws`.
- Si el servicio se aloja localmente, utilice `urn:mysite`

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

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

Servicio	Tipo
Replicación de CloudMirror	s3
Notificaciones	sns
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
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

Para entidades AWS, el URN completo es un ARN válido de AWS. 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.

Creación de un extremo de servicios de plataforma

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

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints.
- Se debe haber creado el recurso al que hace referencia el extremo de servicios de la 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.
- Debe tener 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)

["Se especifica el URN para un extremo de servicios de 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
- Certificado de seguridad (si se utiliza un certificado de CA personalizado)

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 3 Verify server

Optional Optional

Enter endpoint details

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

Display name ?

URI ?

URN ?

Cancel

Continue

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

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

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

Utilice uno de los siguientes formatos:

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

Si no especifica un puerto, el puerto 443 se utiliza para los URI HTTPS y el puerto 80 se utiliza para los 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 se utiliza el extremo para el servicio de replicación de CloudMirror, no incluya el nombre de 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 es posible cambiar el URN de un extremo una vez que se creó el extremo.

6. Seleccione **continuar**.

7. Seleccione un valor para **Tipo de autenticación** y, a continuación, introduzca las credenciales necesarias.

Create endpoint

1 Enter details 2 Select authentication type 3 Verify server

Authentication type ?

Select the method used to authenticate connections to the endpoint.

Anonymous

Anonymous
Access Key
Basic HTTP

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

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

Create endpoint X

(1) Enter details (2) Select authentication type (3) Verify server

Optional

Verify server

Use this method to validate the certificate for TLS connections to the endpoint resource. If you select "Use custom CA certificate," copy and paste the custom security certificate in the text box.

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```
-----BEGIN CERTIFICATE-----
abcdefhijkl123456780ABCDEFGHIJKLM
123456/7890ABCDEFabcdefhijkl1ABCD
-----END CERTIFICATE-----
```

[Previous](#) Test and create endpoint [Next](#)

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

10. Seleccione **probar y crear punto final**.

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



Se produce un error en la creación de extremos si los servicios de plataforma no están habilitados para su cuenta de inquilino. Póngase en contacto con el administrador de StorageGRID.

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

Información relacionada

["Se especifica el URN para un extremo de servicios de plataforma"](#)

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

["Configuración de notificaciones de eventos"](#)

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

Comprobación de la conexión para un extremo de servicios de 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.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints.

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.

The screenshot shows a table with the following data:

<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.

The screenshot shows the 'Overview' tab of a Platform Services Endpoint configuration. The endpoint is named 'my-endpoint-1' and is of type 'S3 Bucket'. Its URI is 'http://10.96.104.167:10443' and its URN is 'urn:sgws:s3:::bucket1'. Below the overview, there are two tabs: 'Connection' and 'Configuration', with 'Configuration' being the active tab. Under the 'Configuration' tab, there is a section titled 'Verify connection' with a 'Test connection' button.

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**.

Edición de un 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 se puede cambiar el URN de un extremo de servicios de plataforma.

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints.

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-----  
abcdefghijklmnopqrstuvwxyz0ABCDEFGHIJKLMNOPQRSTUVWXYZ  
-----END CERTIFICATE-----
```

[Test and save changes](#)

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



No es posible cambiar el URN de un extremo una vez que se creó el extremo.

- a. Para cambiar el nombre para mostrar del extremo, seleccione el ícono de edición .
- b. Según sea necesario, cambie el URI.
- c. Según sea necesario, cambie el tipo de autenticación.
 - 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 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**.
- 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**.

Información relacionada

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

Eliminación de un extremo de servicios de plataforma

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

Lo que necesitará

- Debe iniciar sesión en el Administrador de inquilinos con un explorador compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso **Administrar endpoints**.

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

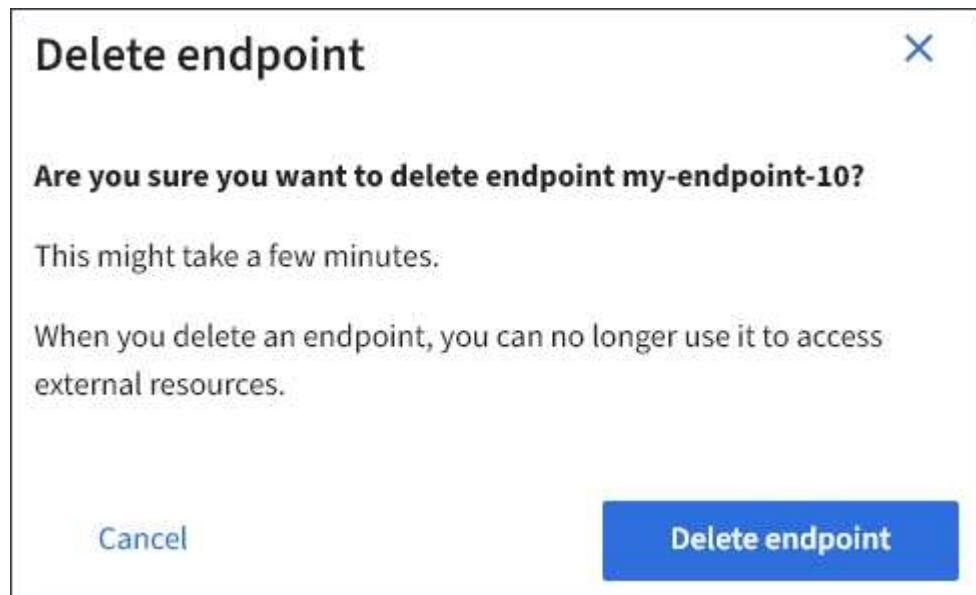
2. Seleccione la casilla de comprobación de cada extremo que desea eliminar.



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

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

Aparecerá un mensaje de confirmación.



4. Seleccione **Eliminar punto final**.

Resolución de problemas de errores de extremos de servicios de plataforma

Si se produce un error cuando StorageGRID intenta comunicarse con un extremo 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.

Determinar si se ha producido un error

Si se han producido errores de extremo de servicios de plataforma en los últimos 7 días, la consola del administrador 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 también aparece en la parte superior de la página de extremos 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)

Comprobando si un 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.

Resolución de 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: Si selecciona **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.

Solución de problemas de servicios de plataforma adicionales

Para obtener información adicional sobre la solución de problemas de los servicios de la plataforma, consulte las instrucciones para administrar StorageGRID.

"Administre StorageGRID"

Información relacionada

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

["Comprobación de la conexión para un extremo de servicios de plataforma"](#)

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

Configurar la replicación de CloudMirror

El servicio de replicación de CloudMirror es uno de los tres servicios de plataforma StorageGRID. Puede usar la replicación de CloudMirror para replicar automáticamente objetos en un bloque de S3 externo.

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque para actuar como origen de replicación.
- El extremo que pretende usar como destino de la replicación de CloudMirror ya debe existir y debe tener su URN.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino. Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el

bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

La replicación de CloudMirror copia los objetos de un bloque de origen en un bloque de destino que se especifique en un extremo. Para 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 la documentación de Amazon sobre la replicación entre regiones (CRR). Para obtener más información sobre cómo StorageGRID implementa la API de configuración de replicación de bloques de S3, consulte las instrucciones para implementar aplicaciones cliente S3.

Si habilita la replicación de CloudMirror en un bloque que contiene objetos, se replican los objetos nuevos agregados al bloque, pero no los objetos existentes en el bloque. 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 se 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. 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 > replicación**.

5. Active la casilla de verificación **Activar 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

["El servicio de replicación de CloudMirror"](#)

["Use S3"](#)

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

Configuración de 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 admite AWS simple Notification Service™ (SNS).

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque para que actúe como el origen de las notificaciones.
- Debe haber el extremo que se pretende usar como destino de las notificaciones de eventos y su URN debe estar presente.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino. 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 más información sobre cómo StorageGRID implementa la API de configuración de notificaciones de bloques de S3, consulte las instrucciones para implementar aplicaciones de 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. Active la casilla de verificación **Activar 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>
```

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

["Notificaciones para bloques"](#)

["Use S3"](#)

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

Utilizando 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 las instrucciones para implementar aplicaciones cliente de S3 para obtener más detalles sobre las siguientes operaciones personalizadas de la API DE REST de StorageGRID S3:

- `DELETE bucket metadata notification Configuration`
- `OBTENGA la solicitud de configuración de notificación de metadatos del bloque`
- `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"](#)

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

["Use 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	<p>Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos.</p> <p>Contiene uno o más elementos Regla.</p>	Sí
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

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 domain-name/myindex/mytype. <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"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <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 S3"](#)

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

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

Configurar 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.

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque de S3 cuyo contenido desea indexar.
- El extremo que pretende usar como destino del servicio de integración de búsqueda ya debe existir y debe tener su URN.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino.
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 bloque 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-
1:111111111111: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. Active la casilla de verificación **Activar integración de búsqueda**.

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

The screenshot shows the 'Platform services' tab selected in the top navigation bar. Under the 'Event notifications' section, there is a checkbox labeled 'Enable search integration' which is checked. Below the checkbox is a code editor containing XML configuration for metadata notification rules. A blue button at the bottom right of the code editor says 'Save changes'.

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



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:

- 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 anule la selección de 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

["Descripción del servicio de integración de búsqueda"](#)

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

["Use S3"](#)

["Creación de 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"  
  }  
}
```

Metadata de objetos incluidos en las notificaciones de metadatos

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

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

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

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



Use S3

Conozca cómo las aplicaciones cliente pueden usar la API de S3 para interactuar con el sistema StorageGRID.

- ["Compatibilidad con la API REST de S3"](#)
- ["Configurar las conexiones y las cuentas de inquilino"](#)
- ["Cómo StorageGRID implementa la API DE REST de S3"](#)
- ["Operaciones y limitaciones compatibles con la API REST de S3"](#)

- "Operaciones de la API de REST de StorageGRID S3"
- "Políticas de acceso a bloques y grupos"
- "Configurar la seguridad para la API DE REST"
- "Supervisión y auditoría de operaciones"
- "Ventajas de las conexiones HTTP activas, inactivas y simultáneas"

Compatibilidad con la API 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 aplicaciones orientadas a los servicios desarrolladas para los servicios web S3 con un almacenamiento de objetos en las instalaciones que usa el sistema StorageGRID. Esto requiere cambios mínimos en el uso actual de llamadas API DE REST de S3 por parte de una aplicación cliente.

- "Cambios en la compatibilidad con la API DE REST de S3"
- "Versiones compatibles"
- "Soporte para servicios de plataforma StorageGRID"

Cambios en la compatibilidad con la API DE REST de S3

Debe estar al tanto de los cambios en la compatibilidad del sistema StorageGRID con la API DE REST de S3.

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.

Liberar	Comentarios
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 s3:ObjectRestore:Post tipo de evento. • Ahora se aplican los límites de tamaño de AWS para piezas multipart. 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. • Se ha agregado compatibilidad con TLS 1.3 y se ha actualizado la lista de conjuntos de cifrado TLS compatibles. • El servicio CLB está obsoleto.
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 x-amz-expiration 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. • Lista actualizada de conjuntos de cifrado TLS admitidos. 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>

Liberar	Comentarios
11.1	Se ha agregado soporte para uso compartido de recursos de origen cruzado (CORS), conexiones de clientes HTTP para S3 a nodos de grid y configuración de cumplimiento en bloques.
11.0	Se añadió compatibilidad para configurar servicios de plataforma (replicación de CloudMirror, notificaciones e integración de búsqueda de Elasticsearch) para los bloques. También se 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.

Versiónes 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

Elemento	Versión
HTTP	<p>1.1</p> <p>Para obtener más información acerca de HTTP, vea HTTP/1.1 (RFC 7230-35).</p> <p>Nota: StorageGRID no admite canalización HTTP/1.1.</p>

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"](#)

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
Notificaciones	Envía notificaciones acerca de eventos en un bloque de StorageGRID de origen a un extremo de servicio simple de notificación (SNS) configurado.	NOTIFICACIÓN DE PUT Bucket
Integración de búsqueda	Envía metadatos de objetos para los objetos almacenados en un bloque de StorageGRID a un índice de Elasticsearch configurado.	<p>PUT bucket metadata notification</p> <p>Nota: se trata de una API StorageGRID S3 personalizada.</p>

Un administrador de grid debe habilitar el uso de los servicios de plataforma para una cuenta de inquilino antes de poder utilizarlos. 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.

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 bloque de S3 en el sistema StorageGRID tiene habilitadas las versiones y la replicación de CloudMirror, NetApp recomienda que el extremo de destino también tenga habilitada el control de versiones de bloque 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.

Información relacionada

["Usar una cuenta de inquilino"](#)

["Administre StorageGRID"](#)

["Operaciones en bloques"](#)

["PUT bucket metadata notification Configuration"](#)

Configurar 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.

Crear y configurar cuentas de inquilinos 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 y usuarios, y contenedores 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. Al crear una cuenta de inquilino de S3, el administrador de grid especifica la siguiente información:

- Nombre para mostrar del arrendatario (el ID de cuenta del arrendatario se asigna automáticamente y no se puede modificar).
- Si la cuenta de inquilino tiene permiso para utilizar los servicios de plataforma. Si se permite el uso de servicios de plataforma, la cuadrícula debe configurarse para que admita su uso.
- Opcionalmente, una 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 está habilitada la federación de identidades para el sistema StorageGRID, el grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.
- Si el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la

contraseña inicial del usuario raíz local del inquilino.

Una vez creada una cuenta de inquilino de S3, los usuarios de inquilinos pueden acceder al administrador de inquilinos para realizar tareas como las siguientes:

- Configure la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) y cree grupos y usuarios locales
- Gestión de claves de acceso de S3
- Cree y gestione bloques de S3, incluidos los bloques con el bloqueo de objetos S3 habilitado
- Utilizar servicios de plataforma (si están habilitados)
- Supervise el uso del almacenamiento



Los usuarios inquilinos S3 pueden crear y gestionar bloques de S3 con el administrador de inquilinos, pero deben tener claves de acceso S3 y usar la API REST de S3 para procesar y gestionar objetos.

Información relacionada

["Administre StorageGRID"](#)

["Usar una cuenta de inquilino"](#)

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 S3 se conectan a StorageGRID para almacenar y recuperar datos. La información específica que necesita para realizar una conexión depende de la configuración elegida.

Las aplicaciones cliente pueden almacenar o recuperar objetos conectándose a cualquiera de los siguientes elementos:

- El servicio Load Balancer en los nodos de administrador o de puerta de enlace, o bien, de forma opcional, la dirección IP virtual de un grupo de alta disponibilidad (ha) de nodos de administración o nodos de puerta de enlace
- El servicio CLB en los nodos de puerta de enlace o, opcionalmente, la dirección IP virtual de un grupo de nodos de puerta de enlace de alta disponibilidad



El servicio CLB está obsoleto. Los clientes configurados antes de la versión StorageGRID 11.3 pueden seguir utilizando el servicio CLB en los nodos de puerta de enlace. El resto de aplicaciones cliente que dependen de StorageGRID para proporcionar equilibrio de carga se deben conectar 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).

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.

Para obtener más información acerca de cada opción, consulte las instrucciones para administrar StorageGRID.

Información relacionada

["Administre StorageGRID"](#)

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. Póngase en contacto con el administrador de StorageGRID para obtener más información o consulte las instrucciones para administrar StorageGRID para obtener una descripción de cómo encontrar esta información en el administrador de grid.

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
Grupo de ALTA DISPONIBILIDAD	CLB Nota: el servicio CLB está en desuso.	La dirección IP virtual de un grupo de alta disponibilidad	<p>Puertos S3 predeterminados:</p> <ul style="list-style-type: none">HTTPS: 8082HTTP: 8084
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

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
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 puerta de enlace	CLB Nota: el servicio CLB está en desuso.	La dirección IP del nodo de puerta de enlace Nota: de forma predeterminada, los puertos HTTP para CLB y LDR no están habilitados.	Puertos S3 predeterminados: <ul style="list-style-type: none"> HTTPS: 8082 HTTP: 8084
Nodo de almacenamiento	LDR	La dirección IP del nodo de almacenamiento	Puertos S3 predeterminados: <ul style="list-style-type: none"> HTTPS: 18082 HTTP: 18084

Ejemplo

Para conectar un cliente S3 al extremo de equilibrio de carga de un grupo ha de nodos de puerta de enlace, utilice una URL estructurada como se muestra a continuación:

- `https://VIP-of-HA-group:_LB-endpoint-port_`

Por ejemplo, si la dirección IP virtual del grupo de alta disponibilidad es 192.0.2.5 y el número de puerto de un extremo de equilibrio de carga de S3 es 10443, un cliente de S3 puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.5:10443`

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.

Información relacionada

["Administre StorageGRID"](#)

Decisión de 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 las conexiones de clientes a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, debe habilitar su uso.

De forma predeterminada, cuando las aplicaciones cliente se conectan a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, deben utilizar HTTPS cifrado para todas las conexiones. Opcionalmente, puede habilitar conexiones HTTP menos seguras seleccionando la opción de cuadrícula **Activar conexión HTTP** en el Administrador de grid. 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, ya que las solicitudes se enviarán sin cifrar.



El servicio CLB está obsoleto.

Si se selecciona la opción **Activar conexión HTTP**, los clientes deben utilizar puertos diferentes para HTTP que los que utilizan para HTTPS. Consulte las instrucciones para administrar StorageGRID.

Información relacionada

["Administre StorageGRID"](#)

["Ventajas de las conexiones HTTP activas, inactivas y simultáneas"](#)

Nombres de dominio extremo para solicitudes de S3

Para poder utilizar los nombres de dominio S3 para las solicitudes de cliente, un administrador de StorageGRID debe configurar el sistema para aceptar conexiones que usen nombres de dominio S3 en solicitudes de estilo de ruta de acceso S3 y de estilo virtual alojado S3.

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 extremo es s3.company.com, El administrador de grid debe asegurarse de que el certificado utilizado para las conexiones HTTPS incluye s3.company.com Nombre alternativo (SAN) del asunto comodín del extremo y del extremo: *.s3.company.com.

- Configure el servidor DNS utilizado por el cliente para incluir registros DNS que coincidan con los nombres de dominio de extremo, 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 equilibrador de carga tiene su propio certificado y cada extremo se puede configurar para reconocer diferentes nombres de dominio de extremo.

Si el cliente conecta nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, el certificado que el administrador de grid configura es el único certificado de servidor personalizado utilizado para la cuadrícula.



El servicio CLB está obsoleto.

Consulte las instrucciones para administrar StorageGRID si desea obtener más información.

Una vez completados estos pasos, puede utilizar solicitudes virtuales de estilo hospedado (por ejemplo, bucket.s3.company.com).

Información relacionada

"Administre StorageGRID"

"Configurar la seguridad para la API DE REST"

Probar la 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.

Lo que necesitará

- Debe haber descargado e instalado la CLI de AWS desde "aws.amazon.com/cli".
- Debe haber creado una cuenta de inquilino de S3 en el sistema StorageGRID.

Pasos

1. Configure los ajustes de Amazon Web Services para que utilicen 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 AWS para la cuenta que creó.
 - c. Introduzca la clave de acceso secreto de AWS para la cuenta que ha creado.
 - 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.

```
aws s3api --endpoint-url https://10.96.101.17:10443  
--no-verify-ssl create-bucket --bucket testbucket
```

Si el bloque se crea correctamente, se devuelve la ubicación del bloque, como se puede ver en el ejemplo siguiente:

```
"Location": "/testbucket"
```

3. Cargue un objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
put-object --bucket testbucket --key s3.pdf --body C:\s3-  
test\upload\s3.pdf
```

Si el objeto se carga correctamente, se devuelve un ETag que es un hash de los datos del objeto.

4. Enumere el contenido del cucharón para verificar que el objeto se ha cargado.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
list-objects --bucket testbucket
```

5. Elimine el objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-object --bucket testbucket --key s3.pdf
```

6. Eliminar el bloque.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-bucket --bucket testbucket
```

Cómo StorageGRID implementa la API DE REST de S3

Una aplicación cliente puede utilizar llamadas API DE REST de S3 para conectarse a StorageGRID y crear, eliminar y modificar bloques, así como almacenar y recuperar objetos.

- "[Solicitudes de clientes en conflicto](#)"
- "[Controles de consistencia](#)"
- "[Cómo gestionan las reglas de ILM de StorageGRID los objetos](#)"
- "[Control de versiones de objetos](#)"
- "[Recomendaciones para implementar la API REST de S3](#)"

Solicitudes de clientes en conflicto

Las solicitudes de clientes en conflicto, como una escritura de dos clientes en la misma clave, se resuelven en base a «'últimas ventas conseguidas'».

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.

Controles de consistencia

Los controles de consistencia proporcionan una compensación entre la disponibilidad de los objetos y la consistencia de dichos objetos en diferentes nodos y sitios de almacenamiento, según lo requiera su 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:

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. Coincide con las garantías de coherencia de Amazon S3. Nota: Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores de Internal Server si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, establezca el control de coherencia en "Available" a menos que necesite garantías de coherencia similares a las de Amazon S3.
Disponible (coherencia eventual para operaciones DE CABEZAL)	Se comporta del mismo modo que el nivel de consistencia "read-after-new-write", pero sólo proporciona consistencia eventual para las operaciones DE CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles. Se diferencia de las garantías de coherencia de Amazon S3 solo para operaciones HEAD.

Utilizando los controles de coherencia "ad-after-new-write" y "available"

Cuando una OPERACIÓN DE CABEZA u OBTIENE utiliza el control de consistencia «read-after-new-write» o UNA operación GET utiliza el control de consistencia «'available'», StorageGRID realiza la búsqueda en varios pasos, de la siguiente manera:

- Primero busca el objeto con una baja consistencia.

- Si esa búsqueda falla, repite la búsqueda en el siguiente nivel de consistencia hasta alcanzar el nivel de consistencia más alto, "all," , lo que requiere que todas las copias de los metadatos del objeto estén disponibles.

Si una operación HEAD o GET utiliza el control de consistencia «read-after-new-write» pero el objeto no existe, la búsqueda de objetos siempre alcanzará el nivel de consistencia «'all'». Debido a que este nivel de consistencia requiere que todas las copias de los metadatos del objeto estén disponibles, puede recibir un número elevado de 500 errores de servidor interno si uno o más nodos de almacenamiento no están disponibles.

A menos que necesite garantías de coherencia similares a las de Amazon S3, puede evitar estos errores en operaciones CON CABEZAL estableciendo el control de coherencia en "disponible". Cuando una operación DE CABEZAL utiliza el control de consistencia "disponible", StorageGRID proporciona únicamente consistencia eventual. No vuelve a intentar una operación fallida hasta que alcanza el nivel de consistencia "all", por lo que no requiere que todas las copias de los metadatos del objeto estén disponibles.

Especifique el control de consistencia para una operación 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: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```



Debe usar el mismo control de coherencia para las operaciones PUT Object y GET Object.

Especificación del control de consistencia de un 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 cucharones deben utilizar el control de coherencia predeterminado, «entre una y otra escritura». Si las solicitudes no funcionan correctamente, cambie el comportamiento del cliente de la 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 consistencia 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:

- **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.
- **Commit doble:** StorageGRID realiza inmediatamente copias provisionales del objeto y 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 ha utilizado la misma regla de ILM y el nivel de coherencia de «un sitio común», puede que el cliente reciba un mensaje de éxito después de replicar los datos del objeto en la ubicación remota, 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 la solicitud de consistencia de bloque"

"PONER solicitud de consistencia de bloque"

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 ingestá**

El método utilizado para proteger los datos de objetos durante el procesamiento: Colocación síncrona (utilizando las opciones equilibradas o estrictas para el comportamiento de ingestá) 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 ingestá
- Clave
- Hora del último acceso



De forma predeterminada, las actualizaciones del último tiempo de acceso se deshabilitan para todos los bloques S3. Si el sistema StorageGRID incluye una regla de ILM que usa la opción Last Access Time, debe habilitar las actualizaciones a la hora del último acceso para los bloques S3 especificados en esa regla. Puede habilitar las actualizaciones de la última hora de acceso mediante LA solicitud DE LA última hora de acceso DE PUT Bucket, la casilla de verificación **S3 > Cuchos > Configurar la última hora de acceso** en el Administrador de inquilinos o mediante la API de administración 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 ubicaciones
- Tamaño del objeto
- Metadatos del usuario
- Etiqueta de objeto

Para obtener más información sobre ILM, consulte las instrucciones para gestionar objetos con la gestión del ciclo de vida de la información.

Información relacionada

["Usar una cuenta de inquilino"](#)

["Gestión de objetos con ILM"](#)

["PUT Bucket última solicitud de tiempo 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.

En el caso de objetos S3 en bloques habilitados para versionado, la compatibilidad con versionado le permite crear reglas de ILM que usen hora no corriente como tiempo de referencia. Cuando se actualiza un objeto, sus versiones anteriores se vuelven no actuales. El uso de un filtro de tiempo no actual permite crear políticas que reduzcan el impacto en el almacenamiento de las versiones anteriores de objetos.

 Cuando se carga una nueva versión de un objeto mediante una operación de carga de varias partes, la hora no actual de la versión original del objeto se refleja cuando se creó la carga de varias partes para la nueva versión, no cuando se completó la carga de varias partes. En casos limitados, la hora no actual de la versión original puede ser horas o días antes de la hora de la versión actual.

Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información para ver un ejemplo de política de ILM para objetos con versiones de S3.

Información relacionada

["Gestión de objetos con ILM"](#)

Recomendaciones para implementar la API REST de S3

Debe seguir estas recomendaciones al implementar la API DE REST de S3 para usar con StorageGRID.

Recomendaciones para las cabezas a los objetos no existentes

Si su aplicación comprueba de forma rutinaria si existe un objeto en una ruta en la que no espera que el objeto exista realmente, debe utilizar 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

En el caso de los bloques creados en StorageGRID 11.4 o posterior, ya no es necesario restringir los nombres de claves 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 claves de objeto.

Para los bloques que se crearon en las versiones anteriores a StorageGRID 11.4, siga estas recomendaciones para los nombres de claves de objetos:

- No debe utilizar valores aleatorios como los primeros cuatro caracteres de claves de objeto. Esto contrasta con la anterior recomendación de AWS para prefijos clave. 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 clave, debe anteponer 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
```

Recomendaciones para «lecturas de rango»

Si se selecciona la opción **Compress Stored Objects** (**Configuración > Opciones de cuadrícula**), las aplicaciones cliente S3 deberían evitar realizar operaciones GET Object que especifiquen un intervalo de bytes que se devolverán. 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.

Información relacionada

["Controles de consistencia"](#)

["PONER solicitud de consistencia de bloque"](#)

["Administre StorageGRID"](#)

Operaciones y limitaciones compatibles con la API REST de S3

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.

- ["Autenticando solicitudes"](#)
- ["Operaciones en el servicio"](#)
- ["Operaciones en bloques"](#)
- ["Operaciones personalizadas en bloques"](#)
- ["Operaciones en objetos"](#)
- ["Operaciones para cargas de varias partes"](#)
- ["Respuestas de error"](#)

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 admite encabezados de solicitudes comunes definidos por el *simple Storage Service API Reference*, 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.
<code>x-amz-token</code> 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
<code>x-amz-id-2</code>	No se utiliza

Información relacionada

["Documentación de Amazon Web Services \(AWS\): Referencia de API de Amazon simple Storage Service"](#)

Autenticando 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.

Uso del 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.

Utilizar 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 le 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
OBTENER servicio	Se implementa con todo el comportamiento de la API DE REST de Amazon S3.
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 la solicitud de 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 nombres de bloque siguen las restricciones de región del estándar estadounidense de AWS, pero debe restringirlas a convenciones de nomenclatura de DNS para admitir solicitudes de estilo hospedado virtual de S3.

["Documentación de Amazon Web Services \(AWS\): Restricciones y limitaciones de buckets"](#)

"Nombres de dominio extremo para la solicitud de 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	Se implementa con todo el comportamiento de la API DE REST de Amazon S3.
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 los nuevos objetos agregados al bloque no están cifrados.
ELIMINAR ciclo de vida de bloque	Esta operación elimina la configuración del ciclo de vida del bloque.
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
GET Bucket (List Objects), versión 1 y versión 2	<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>
GET Bucket acl	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.
OBTENGA los cors del cucharón	Esta operación devuelve el <code>cors</code> configuración del bloque.
OBTENGA el cifrado de bloque	Esta operación devuelve la configuración de cifrado predeterminada del bloque.
OBTENGA el ciclo de vida de la cuchara	Esta operación devuelve la configuración del ciclo de vida del bloque.
OBTENER ubicación de bloque	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.
OBTENGA la notificación DE BUCKET	Esta operación devuelve la configuración de notificación asociada al bloque.
OBTENGA las versiones DE objeto Bucket	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.

Funcionamiento	Implementación
OBTENGA la política de bloques	Esta operación devuelve la política asociada al bloque.
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	Esta implementación usa la <code>versioning</code> subrecurso para devolver el estado de control de versiones de un bloque. El estado de control de versiones devuelto indica si el cucharón está ""no versionado"" o si el cucharón tiene la versión ""habilitado"" o ""acabado"".
OBTENER configuración de bloqueo de objeto	Esta operación determina si el bloqueo de objetos S3 está habilitado para un bloque. "Uso del bloqueo de objetos de S3"
Cubo DE CABEZA	Esta operación determina si existe un bloque y tiene permiso para acceder a él.

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 períodos en solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor. • De forma predeterminada, los bloques se crean en la us-east-1 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. Nota: Se producirá un error si la solicitud PUT Bucket utiliza una región que no se ha definido en StorageGRID. • 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. <p>Debe habilitar S3 Object Lock cuando crea el bloque. No se puede añadir o deshabilitar el bloqueo de objetos de S3 después de crear un bloque. S3 Object Lock requiere el control de versiones de bloques, que se habilita automáticamente al crear el bloque.</p> <p>"Uso del bloqueo de objetos de S3"</p>

Funcionamiento	Implementación
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</p> <p><code>http://www.example.com.</code></p>
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 <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>

Funcionamiento	Implementación
<p>CICLO de vida DE la cuchara</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"> • AbortIncompleteMultipartUpload • ExpiredObjectDeleteMarker • Transición <p>Para comprender cómo la acción de caducidad en el ciclo de vida de un bloque interactúa con las instrucciones de colocación de ILM, consulte ""Cómo funciona ILM durante la vida de un objeto" en las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.</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
NOTIFICACIÓN DE PUT Bucket	<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 extremos 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 400 Bad Request se devuelve un error con el código InvalidArgument.</p> <ul style="list-style-type: none"> No es posible configurar una notificación para los siguientes tipos de eventos. Estos tipos de evento no son compatibles. <ul style="list-style-type: none"> ◦ s3:ReducedRedundancyLostObject ◦ s3:ObjectRestore:Completed Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar excepto que no incluyen algunas claves y utilizan valores específicos para otros, como se muestra en el siguiente listado: <ul style="list-style-type: none"> • EventSource <pre>sgws:s3</pre> <ul style="list-style-type: none"> • * AwsRegion* <p style="padding-left: 2em;">no incluido</p> <ul style="list-style-type: none"> • x-amz-id-2 <p style="padding-left: 2em;">no incluido</p> <ul style="list-style-type: none"> • arn <pre>urn:sgws:s3:::bucket_name</pre>

Funcionamiento	Implementación
POLÍTICA DE PUT Bucket	Esta operación establece la política asociada al bloque.

Funcionamiento	Implementación
PUT Bucket replication	<p>Esta operación configura la replicación de CloudMirror de StorageGRID para el bloque con el XML de configuración de replicación que se proporciona 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 Elemento</code> 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. 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. <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: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code></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 STANDARD 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 null.

Información relacionada

["Documentación de Amazon Web Services \(AWS\): Replicación entre regiones"](#)

["Controles de consistencia"](#)

["GET Bucket última solicitud de tiempo de acceso"](#)

["Políticas de acceso a bloques y grupos"](#)

["Uso del bloqueo de objetos de S3"](#)

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

["Gestión de objetos con ILM"](#)

["Usar una cuenta de inquilino"](#)

Crear 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 detalles completos sobre la creación de configuraciones del ciclo de vida de S3, consulte la sección sobre la gestión del ciclo de vida de objetos en la *Amazon simple Storage Service Developer Guide*. Tenga en cuenta que StorageGRID solo admite acciones de caducidad, no admite acciones de transición.

["Guía para desarrolladores de Amazon simple Storage Service: Gestión del ciclo de vida de los objetos"](#)

Qué es una 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 información detallada, consulte «"Cómo funciona ILM durante la vida de un objeto" en las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.



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

Creando 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 ingestión 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 una configuración de ciclo de vida a un 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:cucharón

```
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 de los bloques se aplica a un 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 coincidido.



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 información detallada, consulte «"Cómo se determina la retención de objetos" en las instrucciones para realizar la administración de StorageGRID.

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": {}
}
```

Información relacionada

["Operaciones en bloques"](#)

["Gestión de objetos con ILM"](#)

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 la solicitud de consistencia de bloque"

Funcionamiento	Descripción	Si quiere más información
PONGA la consistencia del cucharón	Establece el nivel de consistencia aplicado a un bloque determinado.	" PONER solicitud de consistencia de bloque "
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.	" GET Bucket última solicitud de tiempo de acceso "
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 solicitud de tiempo 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 solicitud de configuración de notificación de metadatos del bloque "
PUT bucket metadata notification Configuration	Configura el servicio de notificación de metadatos para un bloque.	" PUT bucket metadata notification Configuration "
PONGA las modificaciones de los cucharones para garantizar el cumplimiento	Obsoleto y no compatible: Ya no puede crear nuevos bloques con el cumplimiento de normativas habilitado.	" Obsoleto: PONGA modificaciones de solicitud de cucharón para el cumplimiento "
Obtenga el cumplimiento de normativas de Bucket	Obsoleto pero compatible: Devuelve la configuración de cumplimiento vigente para un bloque compatible existente.	" Obsoleto: GET Bucket Compliance Request "
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 Request "

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.

- "Uso del bloqueo de objetos de S3"
- "Uso del cifrado del servidor"
- "OBTENER objeto"
- "OBJETO HEAD"
- "Restauración DE objetos posterior"
- "OBJETO PUT"
- "PONER objeto: Copiar"

Las siguientes condiciones se aplican a todas las operaciones de objeto:

- Todas las operaciones en objetos admiten los controles de coherencia StorageGRID, excepto los siguientes:
 - OBTENER ACL de objeto
 - OPTIONS /
 - PONER objeto legal
 - PUT Object retention
- Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en base a «las últimas victorias». La programación de la evaluación «'latest-WINS'» 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 StorageGRID a través de Swift a través de S3.

En la siguiente tabla se describe cómo StorageGRID implementa operaciones de objetos API DE REST de S3.

Funcionamiento	Implementación
<p>ELIMINAR objeto</p>	<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 un plazo de 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y luego indica que el cliente se ha realizado correctamente.</p> <p>Versioning</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 "nula" 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>ELIMINAR varios objetos</p>	<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>

Funcionamiento	Implementación
ELIMINAR etiquetado de objetos	<p>Utiliza la <code>tagging</code> subrecurso para quitar todas las etiquetas de un objeto. Se implementa con todo el comportamiento de la API DE REST de Amazon S3.</p> <p>Versioning</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	<p>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.</p>
OBTENER retención legal de objetos	"Uso del bloqueo de objetos de S3"
OBTENGA retención de objetos	"Uso del bloqueo de objetos de S3"
GET Object tagging	<p>Utiliza la <code>tagging</code> subrecurso para devolver todas las etiquetas de un objeto. Se implementa con todo el comportamiento de la API DE REST de Amazon S3</p> <p>Versioning</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"

Funcionamiento	Implementación
PONER objeto: Copiar	"PONER objeto: Copiar"
PONER objeto legal	"Uso del bloqueo de objetos de S3"
PUT Object retention	"Uso del bloqueo de objetos de S3"

Funcionamiento	Implementación
<p>PUT Object tagging</p>	<p>Utiliza la tagging subrecurso para agregar un conjunto de etiquetas a un objeto existente. Se implementa con todo el comportamiento de la API DE REST de Amazon S3</p> <p>Actualizaciones de etiquetas y comportamiento de procesamiento</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 ingestión 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 procesamiento, no se lleva a cabo ninguna acción si no se pueden realizar las ubicaciones de objetos necesarias (por ejemplo, porque una ubicación recientemente 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». La programación de la evaluación «'latest-WINS'» se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 inician una operación.</p> <p>Versioning</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>

Información relacionada

["Controles de consistencia"](#)

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

Uso del bloqueo de objetos de S3

Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, puede crear bloques con el bloqueo de objetos S3 habilitado y, a continuación, especificar la configuración de retención legal y hasta la fecha para cada versión de objeto que añada a ese bloque.

El bloqueo de objetos S3 permite especificar configuraciones a nivel de objeto para evitar que los objetos se eliminen o se sobrescriban por un tiempo fijo o por tiempo indefinido.

La función de bloqueo de objetos StorageGRID S3 ofrece un único modo de retención equivalente al modo de cumplimiento de normativas Amazon S3. De forma predeterminada, cualquier usuario no puede sobrescribir ni eliminar una versión de objeto protegido. La función de bloqueo de objetos StorageGRID S3 no es compatible con un modo de gobierno y no permite a los usuarios con permisos especiales omitir la configuración de retención o eliminar objetos protegidos.

Habilitar S3 Object Lock para un bloque

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. Es posible usar cualquiera de estos métodos:

- Cree el bloque con el Administrador de arrendatarios.

"Usar una cuenta de inquilino"

- Cree el segmento mediante una solicitud PUT Bucket con el `x-amz-bucket-object-lock_enabled` solicite el encabezado.

"Operaciones en bloques"

No se puede añadir o deshabilitar el bloqueo de objetos de S3 después de crear el bloque. S3 Object Lock requiere el control de versiones de bloques, que se habilita automáticamente al crear el bloque.

Un bloque con S3 Object Lock habilitado puede contener una combinación de objetos con y sin la configuración de S3 Object Lock. StorageGRID no admite la retención predeterminada para los objetos en los bloques de bloqueo de objetos de S3, por lo que no se admite la operación PUT Object Lock Configuration bucket.

Determinar si se habilitó el bloqueo de objetos S3 para un bloque

Para determinar si el bloqueo de objetos S3 está habilitado, utilice LA solicitud GET Object Lock Configuration.

"Operaciones en bloques"

Creación de un objeto con la configuración de Object Lock de S3

Para especificar la configuración de S3 Object Lock (bloqueo de objetos S3) al agregar una versión de objeto a un bloque que tenga habilitado el bloqueo de objetos S3, emita un objeto PUT, PUT Object - Copy o inicie una solicitud de carga de varias partes. Utilice los siguientes encabezados de solicitud.



Debe habilitar S3 Object Lock cuando se crea un bloque. No se puede añadir o deshabilitar el bloqueo de objetos de S3 después de crear un bloque.

- `x-amz-object-lock-mode`, Que debe ser DE CUMPLIMIENTO (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 admiten 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.
- Una solicitud de ELIMINACIÓN de versión de objeto o ELIMINACIÓN de objetos no se realizará correctamente si se encuentra antes de la fecha de retención o si la retención legal está activada.

Actualización de la configuración de bloqueo de objetos de S3

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 del modo debe ser DE CUMPLIMIENTO (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 admiten 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.

Información relacionada

["Gestión de objetos con ILM"](#)

["Usar una cuenta de inquilino"](#)

["OBJETO PUT"](#)

["PONER objeto: Copiar"](#)

["Inicie la carga de varias partes"](#)

["Control de versiones de objetos"](#)

["Guía del usuario de Amazon simple Storage Service: Uso del bloqueo de objetos de S3"](#)

Mediante 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.

Uso de 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

Uso de 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 de CloudMirror está configurada para el bloque, no podrá procesar objetos SSE-C. La operación de ingestá fallará.

Información relacionada

["OBTENER objeto"](#)

["OBJETO HEAD"](#)

["OBJETO PUT"](#)

["PONER objeto: Copiar"](#)

["Inicie la carga de varias partes"](#)

["Cargar artículo"](#)

["Cargar pieza: Copiar"](#)

["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.

No se admite el parámetro de solicitud de número de referencia

La `partNumber` El parámetro `request` no es compatible con GET Object Requests. No puede realizar una solicitud GET para recuperar una parte específica de un objeto de varias partes. Se devuelve un error 501 no implementado con el siguiente mensaje:

```
GET Object by partNumber is not implemented
```

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 en «"uso del cifrado en el servidor"».

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 de un objeto con caracteres UTF-8 escapados en 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`.

Comportamiento de OBTENER objeto para 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), el comportamiento de una solicitud GET Object depende del estado del objeto. Consulte «'HEAD Object'» para obtener más información.



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.

Estado del objeto	Comportamiento DE GET Object
Objeto que ha pasado a un estado no recuperable	403 Forbidden, InvalidObjectState Utilice una solicitud DE restauración POSTERIOR a objetos para restaurar el objeto en 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.

Información relacionada

["Mediante cifrado del servidor"](#)

["Gestión de objetos con ILM"](#)

["Restauración DE objetos posterior"](#)

["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.

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 en «"uso del cifrado en el servidor"».

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 de un objeto con caracteres UTF-8 escapados en 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`

Encabezados de respuesta para objetos de Cloud Storage Pool

Si el objeto se almacena en un grupo de almacenamiento en la nube (consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información), se devuelven los siguientes encabezados 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).

Estado del objeto	Respuesta al OBJETO PRINCIPAL
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 de la cuadrícula no está disponible (por ejemplo, un nodo de almacenamiento está inactivo), debe emitir una solicitud DE restauración DE objetos POST para restaurar la copia desde el grupo de almacenamiento en la nube 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 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 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.

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`.

Información relacionada

["Mediante cifrado del servidor"](#)

["Gestión de objetos con ILM"](#)

["Restauración DE objetos posterior"](#)

["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 XNot Implemented.

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 puede cambiar su expiry-date.
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 Tier elemento para determinar cuánto tiempo tardará el trabajo de restauración en finalizar (Expedited, Standard, o. Bulk). Si no especifica Tier, la Standard se utiliza el nivel. Atención: Si se ha realizado la transición de un objeto a S3 Glacier Deep Archive o el Cloud Storage Pool utiliza Azure Blob Storage, no puede restaurarlo con el Expedited nivel. Se devuelve el siguiente error 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.
Objeto en proceso de restauración a partir de un estado no recuperable	409 Conflict, RestoreAlreadyInProgress

Estado del objeto	Comportamiento DE la restauración POSTERIOR de objetos
Objeto completamente restaurado en el pool de almacenamiento en cloud	<p>200 OK</p> <p>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.</p>

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.

Resolución de conflictos

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.

Tamaño del objeto

StorageGRID admite objetos con un tamaño de hasta 5 TB.

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-<em>name</em>: <em>value</em>
```

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 utilizar un **tiempo de creación definido por el usuario** para el tiempo de referencia y las opciones equilibradas o estrictas para el comportamiento de procesamiento. 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

"Uso del 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

"Operaciones y limitaciones compatibles con la API REST de S3"

Encabezados de solicitud no compatibles

No se admiten los siguientes encabezados 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 ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de colocación en la regla. Si no lo hacen, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y que sea necesario eliminar las copias provisionales iniciales.

- **Balanceado:** Si la regla ILM especifica la opción equilibrada y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en nodos de almacenamiento diferentes.

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).
- **Balanceado:** Si la regla ILM especifica la opción equilibrada, StorageGRID realiza una única copia provisional sólo 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.

Atención: Tener sólo una copia replicada durante cualquier período 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.

Nota: Si está ingiriendo un objeto en un cubo con el bloqueo de objetos S3 activado, 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 ingestión 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.

Atención: las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en «"uso del cifrado en el servidor"».

Nota: Si un objeto está cifrado con SSE o SSE-C, se ignorará cualquier configuración de cifrado a nivel de bloque o a nivel 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.

Información relacionada

["Gestión de objetos con ILM"](#)

["Operaciones en bloques"](#)

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

["Mediante cifrado del servidor"](#)

["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.

Resolución de conflictos

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.

Tamaño del objeto

StorageGRID admite objetos con un tamaño de hasta 5 TB.

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`

"Uso del 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

["Solicitar encabezados para el cifrado del servidor"](#)

Encabezados de solicitud no compatibles

No se admiten los siguientes encabezados 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 ingestión 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 ingestión 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 PONER objeto - Copiar para cifrar un objeto existente en su lugar ni 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 coincide. Cualquier cambio en la ubicación del objeto que se active por la actualización se realice cuando los procesos de ILM normales se reevalúan el ILM en segundo plano.

Esto significa que si la regla ILM utiliza la opción estricta para el comportamiento de procesamiento, no se lleva a cabo ninguna acción si no se pueden realizar las ubicaciones de objetos necesarias (por ejemplo, porque una ubicación recientemente 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` Especifique 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.

Atención: las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en «"uso del cifrado en el 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`

Nota: la `server-side-encryption` el valor del objeto no se puede actualizar. 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"](#)

["Mediante cifrado del servidor"](#)

["Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría"](#)

["OBJETO PUT"](#)

Operaciones para cargas de varias partes

En esta sección se describe cómo StorageGRID admite las operaciones para cargas de varias partes.

- ["Enumerar cargas de varias partes"](#)
- ["Inicie la carga de varias partes"](#)
- ["Cargar artículo"](#)
- ["Cargar pieza: Copiar"](#)
- ["Completar carga 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 multipart. 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. Dado que cada parte se considera un objeto único, el uso de tamaños de pieza grandes 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 tal como 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 estricto o equilibrado del procesamiento. 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 cumplen 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 multipart 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
Enumerar piezas	Se implementa con todo el comportamiento de la API DE REST de Amazon S3

Información relacionada

["Controles de consistencia"](#)

["Mediante 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`
- `max-uploads`
- `key-marker`

- prefix
- upload-id-marker

La delimitación del parámetro request no es compatible.

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 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 ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de colocación en la regla. Si no lo hacen, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y que sea necesario eliminar las copias provisionales iniciales.
 - **Balanceado:** Si la regla ILM especifica la opción equilibrada y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en nodos de almacenamiento diferentes.

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).
 - **Balanceado:** Si la regla ILM especifica la opción equilibrada, StorageGRID realiza una única copia provisional sólo 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.

Atención: Tener sólo una copia replicada durante cualquier período 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.

Nota: Si está ingiriendo un objeto en un cubo con el bloqueo de objetos S3 activado, 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 ingestión 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`

["Uso del 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

["Operaciones y limitaciones compatibles con la API REST de S3"](#)



Para obtener información acerca de cómo StorageGRID maneja 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 este encabezado en ninguna de las solicitudes de artículo de carga.
 - 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.

Atención: las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en «"uso del cifrado en el 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"](#)

["Mediante cifrado del servidor"](#)

"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 en «"uso del 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

["Mediante 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.

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 en «"uso del 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.

Resolución de conflictos

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.

Tamaño del objeto

StorageGRID admite objetos con un tamaño de hasta 5 TB.

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 ingestión 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 ingestión con doble confirmación para garantizar que se cumplen 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 habilitado para un bloque, la versión del objeto se crea al finalizar 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
InvalidArgumentException	400 solicitud incorrecta
InvalidBucketName	400 solicitud incorrecta
InvalidBucketState	409 conflicto
InvalidDigest	400 solicitud incorrecta

Nombre	Estado de HTTP
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
NotImplimed	501 no implementada
NoSuchBucketPolicy	404 no encontrado
ObjectLockConfigurationNotFoundError	404 no encontrado
Error de preconditionError	Error de condición 412

Nombre	Estado de HTTP
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
XNotAcceptable	La solicitud contiene uno o más encabezados de aceptación que no se han podido satisfacer.	406 no aceptable
XNotImplemed	La solicitud que ha proporcionado implica una funcionalidad que no se ha implementado.	501 no implementada

Operaciones de la API de REST de StorageGRID S3

Existen operaciones añadidas en la API DE REST de S3 específicas del sistema StorageGRID.

OBTENGA la solicitud de consistencia de bloque

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.

Debe tener el permiso s3:GetBucketConsistency, o bien ser la raíz de la cuenta, para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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.

Control de consistencia	Descripción
lectura-después-nueva-escritura	<p>(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. Coincide con las garantías de coherencia de Amazon S3.</p> <p>Nota: Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores de Internal Server si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, establezca el control de coherencia en "Available" a menos que necesite garantías de coherencia similares a las de Amazon S3.</p>
Disponible (coherencia eventual para operaciones DE CABEZAL)	<p>Se comporta del mismo modo que el nivel de consistencia "read-after-new-write", pero sólo proporciona consistencia eventual para las operaciones DE CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles. Se diferencia de las garantías de coherencia de Amazon S3 solo para operaciones HEAD.</p>

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"](#)

PONER solicitud de consistencia de bloque

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.

Debe tener el permiso s3:PutBucketConsistency, o bien ser la 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.
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. Coincide con las garantías de coherencia de Amazon S3. Nota: Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores de Internal Server si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, establezca el control de coherencia en "Available" a menos que necesite garantías de coherencia similares a las de Amazon S3.
Disponible (coherencia eventual para operaciones DE CABEZAL)	Se comporta del mismo modo que el nivel de consistencia "read-after-new-write", pero sólo proporciona consistencia eventual para las operaciones DE CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles. Se diferencia de las garantías de coherencia de Amazon S3 solo para operaciones HEAD.

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 la 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Información relacionada

["Controles de consistencia"](#)

GET Bucket última solicitud de tiempo de acceso

La solicitud DE tiempo DE acceso del último bloque DE GET Bucket permite determinar si las actualizaciones de la última hora de acceso están habilitadas o deshabilitadas para bloques individuales.

Para completar esta operación, debe tener el permiso s3:GetBucketLastAccessTime, o ser la raíz de la cuenta.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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 solicitud de tiempo de acceso

La solicitud DE la última hora de acceso al bloque DE PUT permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para bloques individuales. Al deshabilitar las actualizaciones de la última hora de acceso, se mejora el rendimiento, y es la configuración predeterminada para todos los bloques creados con la

versión 10.3.0 o posterior.

Para completar esta operación, debe tener el permiso s3:PutBucketLastAccessTime para un bloque o ser raíz de cuenta.

A partir de la versión 10.3 de StorageGRID, las actualizaciones de la última hora de acceso se deshabilitan de forma predeterminada para todos los bloques nuevos. Si tiene bloques que se crearon con una versión anterior de StorageGRID y desea coincidir con el nuevo comportamiento predeterminado, debe deshabilitar explícitamente las actualizaciones de la última hora de acceso para cada uno de esos bloques anteriores. Puede habilitar o deshabilitar las actualizaciones para la última hora de acceso mediante LA solicitud DE LA última hora de ACCESO DE PUT Bucket, la casilla de verificación **S3 > Cuchos > Cambiar la última configuración de 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 GET Object, GET Object ACL, GET Object Etiquetado y HEAD Object 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 a la hora del último acceso están deshabilitadas para el bloque de origen, PUT Object - Copy Requests 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

En este ejemplo se deshabilita la hora de último acceso para un bloque.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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.

Para completar esta operación, debe tener el permiso s3:DeleteBucketMetadataNotification para un bloque o ser raíz de cuenta.

Ejemplo de solicitud

Este ejemplo muestra cómo deshabilitar el servicio de integración de búsqueda para un bloque.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

OBTENGA la solicitud de configuración de notificación de metadatos del bloque

La solicitud de configuración DE notificación DE metadatos GET Bucket permite recuperar el XML de configuración que se utiliza para configurar la integración de búsqueda de bloques individuales.

Para completar esta operación, debe tener el permiso s3:GetBucketMetadataNotification, o ser raíz de la cuenta.

Ejemplo de solicitud

Esta solicitud recupera la configuración de notificación de metadatos del bloque denominado `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Respuesta

El cuerpo de la respuesta incluye la configuración de notificación de metadatos para el bloque. La configuración de notificaciones de metadatos permite determinar cómo se configura el bloque para la integración de búsquedas. Es decir, permite determinar a qué objetos se indexan y a qué extremos se envían los metadatos de sus objetos.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>

```

Cada configuración de notificación de metadatos incluye una o varias reglas. Cada regla especifica los objetos a los que se aplica y el destino al que StorageGRID debe enviar metadatos de objetos. Los destinos se deben especificar con el URN de un extremo de StorageGRID.

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	<p>Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos.</p> <p>Contiene uno o más elementos Regla.</p>	Sí
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

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

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 domain-name/myindex/mytype. <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"> • arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <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.

Para completar esta operación, debe tener el permiso s3:PutBucketMetadataNotification para un bloque o ser raíz de la cuenta.

Solicitud

La solicitud debe incluir la configuración de notificación de metadatos en el cuerpo de la solicitud. Cada configuración de notificación de metadatos incluye una o varias reglas. Cada regla especifica los objetos a los que se aplica y el destino al que StorageGRID debe enviar metadatos de objetos.

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, puede enviar metadatos 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
MetadataNotificationConfiguration	<p>Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos.</p> <p>Contiene uno o más elementos Regla.</p>	Sí
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

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

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 domain-name/myindex/mytype. <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"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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

["Usar una cuenta de inquilino"](#)

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 us-east-1
Metadatos del sistema	tamaño	Tamaño del objeto (en bytes) visible para un cliente HTTP
Metadatos del sistema	md5	Hash de objeto
Metadatos del usuario	metadatos <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

Nota: para etiquetas y metadatos de usuario, StorageGRID pasa fechas y 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. Una vez indizado un documento, no se pueden editar los tipos de campo del documento en el índice.

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 sólida, StorageGRID intenta recuperar la información de uso con una coherencia de sitio sólida.

Debe tener el permiso `s3>ListAllMyBuckets` o ser la raíz de la cuenta para completar esta operación.

Ejemplo de solicitud

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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 borrado 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 el ajuste de cumplimiento global, la opción de bloqueo de objetos S3 global se habilita automáticamente al actualizar a StorageGRID 11.5. 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.

"Uso del 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"

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.

"Uso del 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.

Información relacionada

"Gestión de objetos con ILM"

"Usar una cuenta de inquilino"

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.

"Uso del 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"

Para completar esta operación, debe tener el permiso s3:GetBucketCompliance o ser la raíz de la cuenta.

Ejemplo de solicitud

Esta solicitud de ejemplo le permite determinar la configuración de cumplimiento para el bloque denominado mybucket.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
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.

Nombre	Descripción
LegalHold	<ul style="list-style-type: none"> • Cierto: Este segmento está actualmente bajo un control legal. Los objetos de este segmento no se pueden eliminar hasta que se levante la retención 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.

Información relacionada

["Gestión de objetos con ILM"](#)

["Usar una cuenta de inquilino"](#)

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.

["Uso del 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"](#)

Debe tener el permiso s3:PutBucketCompliance o ser la raíz de la cuenta para completar esta operación.

Debe especificar un valor para cada campo de la configuración de cumplimiento al emitir una solicitud DE cumplimiento PUT Bucket.

Ejemplo de solicitud

Esta solicitud de ejemplo modifica la configuración de cumplimiento del bloque denominado mybucket. En este ejemplo, los objetos de mybucket ahora se conservarán durante dos años (1,051,200 minutos) en lugar de un año, a partir del momento en que el objeto se ingiere en la cuadrícula. No existe ningún derecho legal en este segmento. Cada objeto se eliminará automáticamente después de dos años.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
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>Atención: al especificar un nuevo valor para RetentionPeriodonMinutes, debe especificar un valor igual o mayor que el período de retención actual del cucharón. Una vez establecido el período de retención del segmento, no podrá disminuir dicho valor; sólo podrá aumentarlo.</p>
LegalHold	<ul style="list-style-type: none">• Cierto: Este segmento está actualmente bajo un control legal. Los objetos de este segmento no se pueden eliminar hasta que se levante la retención 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.

Nombre	Descripción
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** debido a que un sitio de centro de datos o varios nodos de almacenamiento de un sitio no están disponibles, el código de estado HTTP de 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"](#)

["Usar una cuenta de inquilino"](#)

["Gestión de objetos con ILM"](#)

Políticas de acceso a 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.

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, los caracteres comodín no se admiten excepto para establecer el acceso anónimo, que concede 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 s3GetObject 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",
          "s3GetObject"
        ],
        "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.

Información relacionada

["Usar una cuenta de inquilino"](#)

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`.

Uso del ARN en las sentencias de directiva

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.

Especificar 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.

Información relacionada

["Especificar variables en una directiva"](#)

Especificar los principales de 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 declaraciones de política en 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.

Especificación de 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
s3:CreateBucket	COLOQUE el cucharón	
s3:DeleteBucket	ELIMINAR bloque	
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	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
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	
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

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:PutBucketNotification	NOTIFICACIÓN DE PUT Bucket	
s3:PutBucketObjectLockConfiguration	COLOQUE el cucharón con el x-amz-bucket-object-lock-enabled: true Encabezado de solicitud (también requiere el permiso s3:CreateBucket)	
s3:PutBucketPolicy	POLÍTICA DE PUT Bucket	
s3:PutBucketEtiquetado	<ul style="list-style-type: none"> • ELIMINAR etiquetado de bloque† • PUT Bucket etiquetaje 	
s3:PutBucketVersioning	PONER creación de versiones de bloques	
s3:PutLipeycleConfiguration	<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: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)	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
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 	
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	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
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	

Uso del 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:
 - No se pueden sobrescribir los datos, los metadatos definidos por el usuario ni el etiquetado de objetos de S3 del objeto.
 - 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 política actual de S3 permite sobrescribir y el permiso PutOverwriteObject se establece en Deny, el cliente no puede sobrescribir los datos de un objeto, metadatos definidos por el usuario ni el etiquetado de objetos. Además, si la casilla de verificación **evitar modificación de cliente** está activada (**Configuración > Opciones de cuadrícula**), esa configuración anula la configuración del permiso PutOverwriteObject.

Información relacionada

["Ejemplos de políticas de grupo S3"](#)

Especificar condiciones en una directiva

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: {  
    <em>condition_type</em>: {  
        <em>condition_key</em>: <em>condition_values</em>  
    }  
}
```

En el ejemplo siguiente, la condición ipaddress utiliza la clave de condición Sourcelp.

```
"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).
StringEqualIgnoreCase	Compara una clave con un valor de cadena basado en la coincidencia exacta (omite Case).

Operadores de condición	Descripción
StringNotEqualIgnoreCase	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.
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".
NumericLesThanEquals	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 Gpuertas 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 se ignorará el encabezado ya que no se puede comprobar 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.
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.

Especificar variables en una directiva

Las variables de las directivas se pueden utilizar para llenar 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
\${aws:SourceIp}	Utiliza la clave SourceIp como la variable proporcionada.
\${aws:username}	Utiliza la clave de nombre de usuario como la variable proporcionada.
\${s3:prefix}	Utiliza la clave de prefijo específica del servicio como variable proporcionada.
\${s3:max-keys}	Utiliza la clave de max-keys específica del servicio como la variable proporcionada.
\${*}	Carácter especial. Utiliza el carácter como carácter literal *.
\${?}	Carácter especial. Utiliza el carácter como literal ? carácter.
\${\$}	Carácter especial. Utiliza el carácter como carácter literal \$.

Creación de directivas que requieren un manejo especial

A veces, una directiva puede otorgar permisos peligrosos para la seguridad o para operaciones continuas, como bloquear al usuario raíz de la cuenta. La implementación de la API REST de StorageGRID S3 es menos restrictiva durante la validación de políticas que Amazon, pero igual de estricta durante la evaluación de la política.

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
Denegar a sí mismo cualquier permiso a la cuenta raíz	Cucharón	Válido y reforzado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bloques de S3	Igual
Denegar a sí mismo cualquier permiso al usuario o grupo	Grupo	Válido y reforzado	Igual
Permitir cualquier permiso para un grupo de cuentas externo	Cucharón	Principal no válido	Válidos, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un método 405 no permitido cuando lo permite una política
Permitir cualquier permiso para una raíz de cuenta externa o para un usuario	Cucharón	Válidos, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un método 405 no permitido cuando lo permite una política	Igual
Permitir que todos tengan permisos para todas las acciones	Cucharón	Válido, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un error de método 405 no permitido para la raíz de cuenta externa y los usuarios	Igual
Denegar a todos los permisos a todas las acciones	Cucharón	Válido y reforzado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bloques de S3	Igual
Principal es un usuario o grupo inexistente	Cucharón	Principal no válido	Válido
El recurso es un bloque de S3 que no existe	Grupo	Válido	Igual

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
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 > Opciones de cuadrícula** y active la casilla de verificación **evitar modificación de 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 se protegen contra las escrituras simultáneas (véase 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

["Gestión de objetos con ILM"](#)

["Creación de directivas que requieren un manejo especial"](#)

["Cómo gestionan las reglas de ILM de StorageGRID los objetos"](#)

["Ejemplos de políticas de grupo S3"](#)

Ejemplos de políticas de S3

Utilice los ejemplos de esta sección para crear políticas de acceso de StorageGRID para bloques y grupos.

Ejemplos de políticas de bloques de S3

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.

Se puede configurar una política de bloques mediante la CLI de AWS según el siguiente comando:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy  
<em>file://policy.json</em>
```

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 directiva podría no ser particularmente útil ya que nadie, excepto la raíz de la cuenta, tiene permisos para escribir en el bloque.

```
{  
  "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/*"
        }
    ]
}

```

Información relacionada

["Operaciones en bloques"](#)

Ejemplos de políticas de grupo S3

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, ya que 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

Cuando utilice el Administrador de inquilinos para agregar o editar un grupo, puede seleccionar cómo desea crear la política de grupo que define qué miembros de permisos de acceso S3 de este grupo tendrán, de la siguiente manera:

- **Sin acceso S3:** Opción predeterminada. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se conceda el acceso mediante una política de bloques. 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 sólo 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.
- **Personalizado:** A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

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.

The screenshot shows the 'Access Type' section of the AWS IAM Groups configuration. The 'Custom' option is selected, and a note below it says '(Must be a valid JSON formatted string.)'. To the right, a large text area displays a JSON policy document:

```
{  
  "Statement": [  
    {  
      "Sid": "AllowListBucketOfASpecificUserPrefix",  
      "Effect": "Allow",  
      "Action": "s3>ListBucket",  
      "Resource": "arn:aws:s3:::department-bucket",  
      "Condition": {  
        "StringLike": {  
          "s3:prefix": "${aws:username}/*"  
        }  
      }  
    },  
    {  
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",  
      "Effect": "Allow",  
      "Action": "s3:*Object",  
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"  
    }  
  ]  
}
```

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",
        "s3GetObject",
        "s3GetObjectTagging",
        "s3GetObjectVersion",
        "s3GetObjectVersionTagging"
      ],
      "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}/*"
    }
  ]
}

```

Información relacionada

["Usar una cuenta de inquilino"](#)

["Uso del permiso PutOverwriteObject"](#)

["Protección WORM \(escritura única lectura múltiple\)"](#)

Configurar la seguridad para 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 forma predeterminada, StorageGRID utiliza HTTPS para las comunicaciones del cliente con los nodos de almacenamiento y el servicio CLB en los nodos de puerta de enlace.

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.



El servicio CLB está obsoleto.

- 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 administrador, directamente a los nodos de almacenamiento o al servicio CLB en los nodos de Gateway.

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 o al servicio CLB en los nodos de puerta de enlace, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (firmados por la autoridad de certificación del sistema), o un único certificado de servidor personalizado que un administrador de grid suministra para la cuadrícula.

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 información sobre la configuración de extremos de equilibrador de carga y para obtener instrucciones sobre cómo agregar un único certificado de servidor personalizado para conexiones TLS directamente a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace.

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

Problema de seguridad	Implementación de la API DE REST
Autenticación del servidor	Certificado de servidor X.509 firmado por CA del sistema o certificado de servidor personalizado suministrado por el administrador
Autentificación 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

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).

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.

Paquetes de cifrado compatibles

Versión TLS	Nombre IANA de conjunto cifrado
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1.2	TLS_ECDHE_RSA_WITH_CHA20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
1.3	TLS_CHA20_POLY1305_SHA256
1.3	TLS_AES_128_GCM_SHA256

Suites de cifrado obsoletas

Los siguientes conjuntos de cifrado están desaprobados. La compatibilidad con estos cifrados se eliminará en una versión futura.

Nombre de IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Información relacionada

["Cómo se pueden configurar las conexiones de clientes"](#)

Supervisión y auditoría de 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.

- ["Supervisión de las tasas de procesamiento y recuperación de objetos"](#)
- ["Acceder y revisar registros de auditoría"](#)

Supervisión de 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 con un navegador compatible.
2. En la consola, busque la sección Operaciones de protocolo.

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.

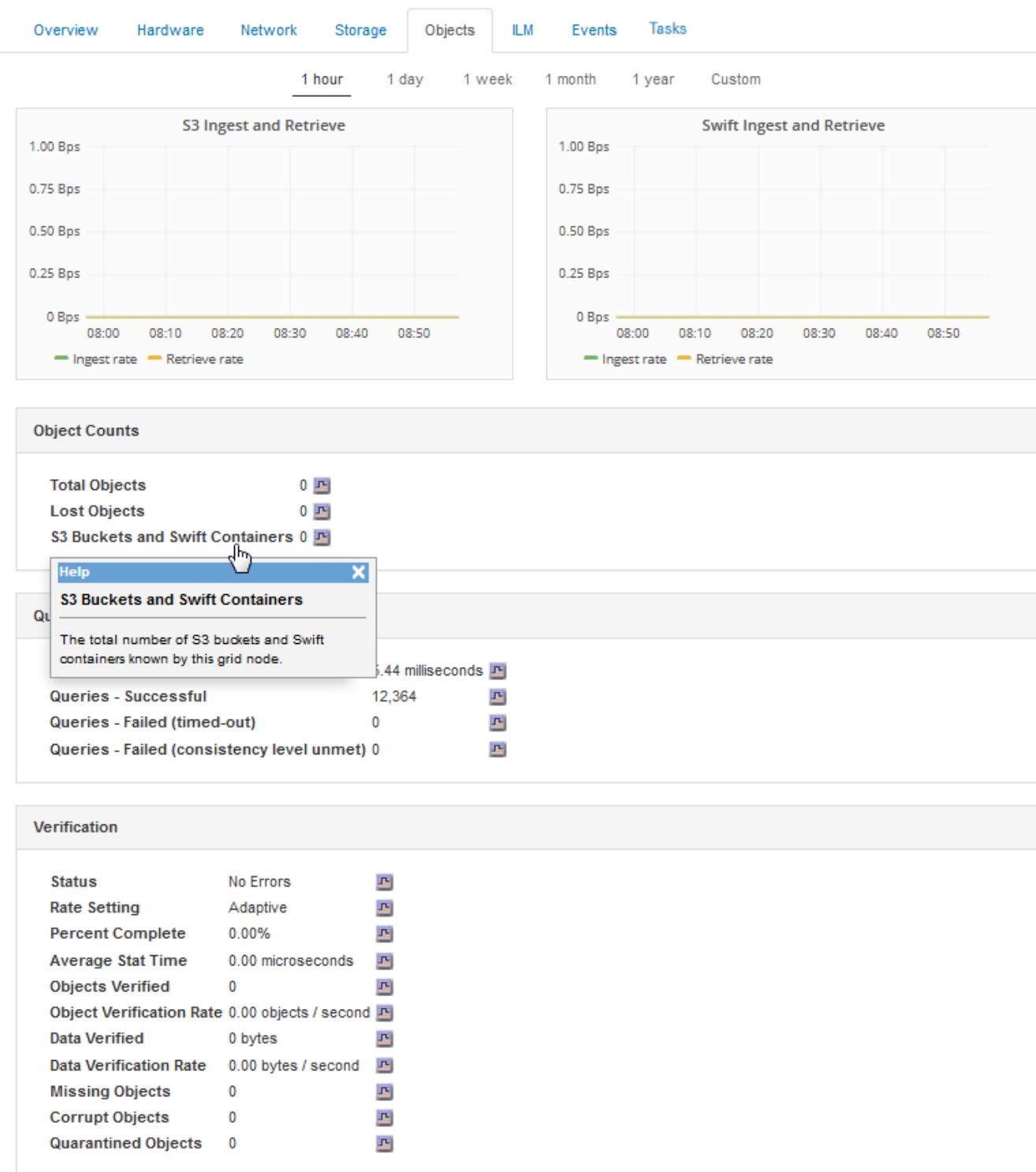
5. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **objetos**.

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.

DC1-S2 (Storage Node)



7. Si desea aún más detalles:

a. Seleccione **Soporte > Herramientas > Topología de cuadrícula**.

b. Seleccione **site > 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.

Lo que necesitará

- 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

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.

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 pieza (cuando la regla ILM usa los comportamientos de consumo estrictos o equilibrados)
- Cargar pieza: Copia (cuando la regla ILM usa los comportamientos de ingesta estrictos o equilibrados)
- 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

Información relacionada

- ["Ventajas de mantener abiertas las conexiones HTTP inactivas"](#)
- ["Ventajas de las conexiones HTTP activas"](#)
- ["Ventajas de las conexiones HTTP simultáneas"](#)
- ["Separación de grupos de conexiones HTTP para operaciones de lectura y escritura"](#)

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 directamente a nodos de almacenamiento o al servicio CLB (obsoleto) en nodos de puerta de enlace, 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 conexiones de clientes a nodos de almacenamiento o al servicio CLB, limitar las conexiones HTTP activas proporciona las siguientes ventajas:

- Permite un balanceo de carga óptimo en el sistema StorageGRID.

Cuando utilice el servicio CLB, debe evitar conexiones TCP/IP de larga duración para optimizar el equilibrio de carga en todo el sistema StorageGRID. Debe configurar las aplicaciones cliente para realizar un seguimiento de la duración de cada conexión HTTP y cerrar la conexión HTTP después de una hora establecida para que la conexión HTTP se pueda restablecer y reequilibrar.

El servicio CLB equilibra la carga a través del sistema StorageGRID en el momento en que una aplicación cliente establece una conexión HTTP. 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.



El servicio CLB está obsoleto.

- 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 inicien 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 cliente no es limitada, las conexiones activas pueden tardar varios minutos en terminarse 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.

Use Swift

Conozca cómo las aplicaciones cliente pueden usar la API Swift de OpenStack para interactuar con el sistema StorageGRID.

- "[Compatibilidad con la API de OpenStack Swift en StorageGRID](#)"
- "[Configurar las conexiones y las cuentas de inquilino](#)"
- "[Operaciones compatibles con la API REST de Swift](#)"
- "[Operaciones de la API de REST de StorageGRID Swift](#)"
- "[Configurar la seguridad para la API DE REST](#)"
- "[Supervisión y auditoría de operaciones](#)"

Compatibilidad con la API de OpenStack Swift en StorageGRID

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

Elemento	Versión
HTTP	<p>1.1 para obtener más información acerca de HTTP, consulte HTTP/1.1 (RFC 7230-35).</p> <p>Nota: StorageGRID no admite canalización HTTP/1.1.</p>

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
11.5	Se ha eliminado el control de consistencia débil. En su lugar, se utilizará el nivel de consistencia disponible.
11.4	Se ha agregado compatibilidad con TLS 1.3 y se ha actualizado la lista de conjuntos de cifrado TLS compatibles. CLB está en desuso. 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. Lista actualizada de conjuntos de cifrado TLS admitidos. 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.

Liberar	Comentarios
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. Las reglas y políticas de ILM determinan la manera en que StorageGRID crea y distribuye copias de datos de objetos y la manera en que las administra. 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 administrador de StorageGRID si necesita comprender cómo las políticas y las reglas de ILM de la cuadricula afectarán a los objetos de la cuenta de inquilino de Swift.

Solicitudes de clientes en conflicto

Las solicitudes de clientes en conflicto, como una escritura de dos clientes en la misma clave, se resuelven en base a «'últimas ventas conseguidas'». La programación de la evaluación de «'latest-WINS'» se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de Swift iniciaron 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. 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.

StorageGRID también le permite controlar la coherencia de cada contenedor. Puede cambiar el control de coherencia para compensar la disponibilidad de los objetos y la coherencia de dichos objetos en diferentes nodos y sitios de almacenamiento, según lo requiera su aplicación.

Información relacionada

"[Gestión de objetos con ILM](#)"

"[OBTENGA la solicitud de consistencia del contenedor](#)"

"[PONGA la solicitud de consistencia del contenedor](#)"

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 su aplicación comprueba de forma rutinaria si existe un objeto en una ruta en la que no espera que el objeto exista realmente, debe utilizar 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 coherencia "disponible" para cada contenedor utilizando la solicitud DE consistencia DEL contenedor PUT.

Recomendaciones para los nombres de objetos

No debe utilizar valores aleatorios como los primeros cuatro caracteres de nombres de objetos. En su lugar, debe utilizar prefijos no aleatorios y no únicos, como la imagen.

Si necesita utilizar caracteres aleatorios y únicos en prefijos de nombres de objetos, debe asignar un prefijo a los nombres de objetos 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 se selecciona la opción **Compress Stored Objects** ([Configuración > Configuración del sistema > Opciones de cuadrícula](#)), las aplicaciones cliente Swift deberían evitar realizar operaciones GET object que especifiquen 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.

Información relacionada

["OBTENGA la solicitud de consistencia del contenedor"](#)

["PONGA la solicitud de consistencia del contenedor"](#)

["Administre StorageGRID"](#)

Configurar 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.

Crear y configurar cuentas de inquilinos 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.

Al crear una cuenta de inquilino de Swift, el administrador de grid especifica la siguiente información:

- Nombre para mostrar del inquilino (el ID de cuenta del inquilino se asigna automáticamente y no se puede cambiar)
- Opcionalmente, una 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 el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la contraseña inicial del usuario raíz local del inquilino.
- Si SSO está habilitado, qué 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 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 tener el permiso acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso Root Access no permite que los usuarios se autentiquen 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.

Información relacionada

["Administre StorageGRID"](#)

["Usar una cuenta de inquilino"](#)

["Extremos de API de Swift compatibles"](#)

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 a cualquiera de los siguientes elementos:

- El servicio Load Balancer en los nodos de administrador o de puerta de enlace, o bien, de forma opcional, la dirección IP virtual de un grupo de alta disponibilidad (ha) de nodos de administración o nodos de puerta de enlace
- El servicio CLB en los nodos de puerta de enlace o, opcionalmente, la dirección IP virtual de un grupo de nodos de puerta de enlace de alta disponibilidad



El servicio CLB está obsoleto. Los clientes configurados antes de la versión StorageGRID 11.3 pueden seguir utilizando el servicio CLB en los nodos de puerta de enlace. El resto de aplicaciones cliente que dependen de StorageGRID para proporcionar equilibrio de carga se deben conectar 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).

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.

Para obtener más información acerca de cada opción, consulte las instrucciones para administrar StorageGRID.

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. Póngase en contacto con el administrador de StorageGRID para obtener más información o consulte las instrucciones para administrar StorageGRID para obtener una descripción de cómo encontrar esta información en el administrador de grid.

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
Grupo de ALTA DISPONIBILIDAD	CLB Nota: el servicio CLB está en desuso.	La dirección IP virtual de un grupo de alta disponibilidad	Puertos Swift predeterminados: <ul style="list-style-type: none">HTTPS: 8083HTTP: 8085
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 puerta de enlace	CLB Nota: el servicio CLB está en desuso.	La dirección IP del nodo de puerta de enlace Nota: de forma predeterminada, los puertos HTTP para CLB y LDR no están habilitados.	Puertos Swift predeterminados: <ul style="list-style-type: none">HTTPS: 8083HTTP: 8085
Nodo de almacenamiento	LDR	La dirección IP del nodo de almacenamiento	Puertos Swift predeterminados: <ul style="list-style-type: none">HTTPS: 18083HTTP: 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.

Decisión de 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 las conexiones de clientes a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, debe habilitar su uso.

De forma predeterminada, cuando las aplicaciones cliente se conectan a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, deben utilizar HTTPS cifrado para todas las conexiones.

Opcionalmente, puede habilitar conexiones HTTP menos seguras seleccionando la opción de cuadrícula

Activar conexión HTTP en el Administrador de grid. 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, ya que las solicitudes se enviarán sin cifrar.



El servicio CLB está obsoleto.

Si se selecciona la opción **Activar conexión HTTP**, los clientes deben utilizar puertos diferentes para HTTP que los que utilizan para HTTPS. Consulte las instrucciones para administrar StorageGRID.

Información relacionada

["Administre StorageGRID"](#)

Probar 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.

Lo que necesitará

- Debe haber descargado e instalado python-swiftclient, el cliente de línea de comandos de Swift.
- 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

["Crear y configurar cuentas de inquilinos de Swift"](#)

["Configurar la seguridad para 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. No se puede configurar el usuario raíz del inquilino para usar la API DE 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

["Cómo se pueden configurar las conexiones de clientes"](#)

["Crear y configurar cuentas de inquilinos de Swift"](#)

["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

["Se realizó un seguimiento de las operaciones de Swift en los registros de auditoría"](#)

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

["Se realizó un seguimiento de las operaciones de Swift en los registros de auditoría"](#)

Operaciones de objeto

Las siguientes operaciones de la API de Swift se realizan en objetos.

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 un plazo de 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y luego indica que el cliente se ha realizado correctamente.

Para obtener más información sobre cómo eliminar objetos, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

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.

StorageGRID admite objetos con un tamaño de hasta 5 TB.



Las solicitudes de clientes en conflicto, como una escritura de dos clientes en la misma clave, se resuelven en base a «'últimas ventas conseguidas'». La programación de la evaluación de «'latest-WINS'» 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 chunked 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 comprimido ni descomprimido 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 las reglas de la ubicación síncrona y ILM, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

- 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 denominado 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 ingestión, StorageGRID crea una única copia provisional mientras se ingiere el objeto (COMMIT único).
- **Balanceado:** Si la regla ILM especifica la opción equilibrada, StorageGRID realiza una única copia provisional sólo 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

Información relacionada

["Gestión de objetos con ILM"](#)

["Se realizó un seguimiento de las operaciones de Swift en los registros de auditoría"](#)

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 OPTIONS no se puede utilizar con la dirección 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
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
NotImplimed	501 no implementada
Error de precondiciónError	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

El nivel de coherencia establece una compensación entre la disponibilidad de los objetos y la coherencia de dichos objetos en los diferentes nodos y sitios de almacenamiento. 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
X-Auth-Token	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
Date	La fecha y la hora de la respuesta.
Connection	Si la conexión con el servidor está abierta o cerrada.
X-Trans-Id	Identificador de transacción único para la solicitud.
Content-Length	La longitud del cuerpo de respuesta.

Encabezado HTTP de respuesta	Descripción
x-ntap-sg-consistency	<p>El nivel de control de consistencia que se aplica al contenedor. Se admiten los siguientes valores:</p> <ul style="list-style-type: none"> • Todos: Todos los nodos reciben los datos inmediatamente o la solicitud falla. • 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: Proporciona consistencia de lectura-after-write para nuevos objetos y eventual consistencia para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. <p>Nota: Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores internos del servidor si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, utilice el nivel "disponible".</p> <ul style="list-style-type: none"> • Disponible (eventual consistencia para las operaciones DE LA CABEZA): Se comporta igual que el nivel de consistencia "entre-después-nueva-escritura", pero sólo proporciona consistencia eventual para las operaciones DE LA CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles.

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

```

Información relacionada

["Usar una cuenta de inquilino"](#)

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
X-Auth-Token	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> <ul style="list-style-type: none">• Todos: Todos los nodos reciben los datos inmediatamente o la solicitud falla.• 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: Proporciona consistencia de lectura-after-write para nuevos objetos y eventual consistencia para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. <p>Nota: Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores internos del servidor si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, utilice el nivel "disponible".</p> <ul style="list-style-type: none">• Disponible (eventual consistencia para las operaciones DE LA CABEZA): Se comporta igual que el nivel de consistencia "entre-después-nueva-escritura", pero sólo proporciona consistencia eventual para las operaciones DE LA CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles.
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

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:

- **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.
- **Commit doble:** StorageGRID realiza inmediatamente copias provisionales del objeto y 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 «strong-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.
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
```

Información relacionada

["Usar una cuenta de inquilino"](#)

Configurar la seguridad para 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 forma predeterminada, StorageGRID utiliza HTTPS para las comunicaciones del cliente con los nodos de almacenamiento y el servicio CLB en los nodos de puerta de enlace.

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.



El servicio CLB está obsoleto.

- 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 administrador, directamente a los nodos de almacenamiento o al servicio CLB en los nodos de Gateway.

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 o al servicio CLB en los nodos de puerta de enlace, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (firmados por la autoridad de certificación del sistema), o un único certificado de servidor personalizado que un administrador de grid suministra para la cuadrícula.

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 información sobre la configuración de extremos de equilibrador de carga y para obtener instrucciones sobre cómo agregar un único certificado de servidor personalizado para conexiones TLS directamente a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace.

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
Autentificación 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

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).

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.

Paquetes de cifrado compatibles

Versión TLS	Nombre IANA de conjunto cifrado
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

Suites de cifrado obsoletas

Los siguientes conjuntos de cifrado están desaprobados. La compatibilidad con estos cífrados se eliminará en una versión futura.

Nombre de IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Información relacionada

["Cómo se pueden configurar las conexiones de clientes"](#)

Supervisión y auditoría de 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.

Supervisión de 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 con un navegador compatible.
2. En la consola, busque la sección Operaciones de protocolo.

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.

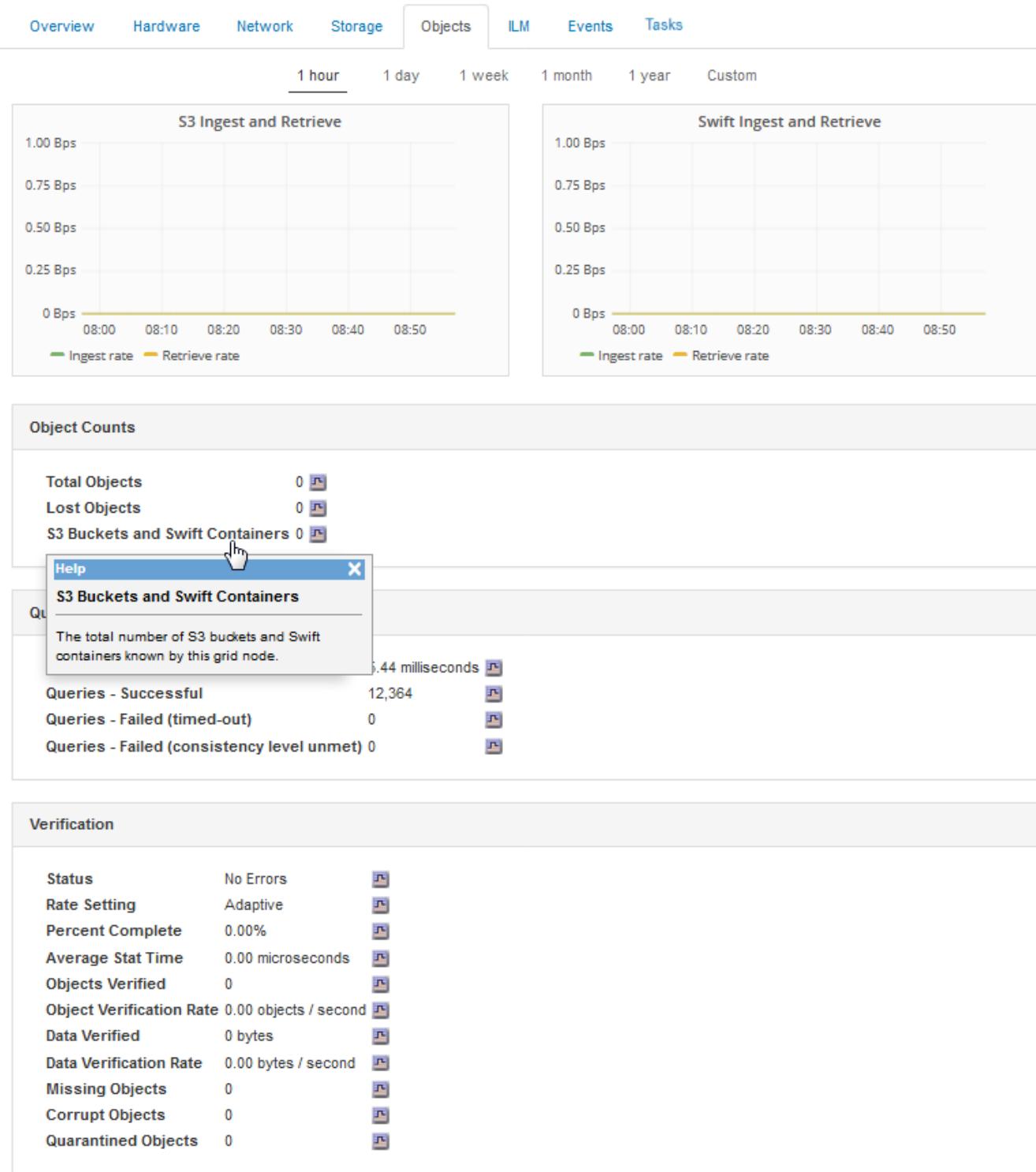
5. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **objetos**.

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.

DC1-S2 (Storage Node)



7. Si desea aún más detalles:

- Seleccione **Soporte > Herramientas > Topología de cuadrícula**.
- Seleccione **site > 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.

Lo que necesitará

- 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

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 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.
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.

Información relacionada

["Revisar los registros de auditoría"](#)

Se realizó un seguimiento de las operaciones de Swift en los registros de auditoría

Se realiza un seguimiento de todas las operaciones DE ELIMINACIÓN, GET, HEAD, POST y PUT de almacenamiento correctamente en el registro de auditoría de StorageGRID. Los fallos no se registran ni se registran solicitudes de información, autenticación u OPCIONES.

Consulte *Descripción de los mensajes de auditoría* para obtener detalles sobre la información de la que se realiza el seguimiento 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 relacionada

["Revisar los registros de auditoría"](#)

["Operaciones de cuentas"](#)

["Operaciones de contenedor"](#)

["Operaciones de 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.