Utilice la API REST de S3

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Utilice la API REST de S3 . . . 1
Versiones y actualizaciones compatibles con la API REST de S3 . . . 1
Versiones compatibles . . . 1
Actualizaciones de la compatibilidad con la API REST de S3 . . . 1
Referencia rápida: solicitudes de API de S3 compatibles . . . 4
Parámetros de consulta URI comunes y encabezados de solicitud . . . 5
"AbortarMultipartUpload" . . . 5
"Carga completa de varias partes" . . . 5
"Copiar objeto" . . . 6
"Crear cubo" . . . 7
"Crear carga de varias partes" . . . 7
"Eliminar cubo" . . . 8
"EliminarBucketCors" . . . 8
"Eliminar cifrado del cubo" . . . 8
"Eliminar ciclo de vida del cubo" . . . 8
"Política de eliminación de cubos" . . . 9
"EliminarReplicaciónDeBucket" . . . 9
"Eliminar etiquetado de cubo" . . . 9
"Eliminar objeto" . . . 9
"Eliminar objetos" . . . 10
"Eliminar etiquetado de objetos" . . . 10
"ObtenerBucketAcl" . . . 10
"ObtenerBucketCors" . . . 10
"Obtener cifrado de cubo" . . . 11
"Obtener configuración del ciclo de vida del cubo" . . . 11
"Obtener la ubicación del cubo" . . . 11
"Configuración de GetBucketNotification" . . . 11
"Obtener política de cubo" . . . 11
"Obtener réplica de cubo" . . . 12
"Obtener etiquetado de cubos" . . . 12
"Obtener versiones de Bucket" . . . 12
"Obtener objeto" . . . 12
"ObtenerObjetoAcl" . . . 13
"Obtener retención legal de objeto" . . . 13
"Obtener configuración de bloqueo de objeto" . . . 14
"Obtener retención de objetos" . . . 14
"Obtener etiquetado de objetos" . . . 14
"Cubo de cabeza" . . . 14
"Objeto principal" . . . 14
"Lista de cubos" . . . 15
"Lista de cargas de varias partes" . . . 15
"Lista de objetos" . . . 16
"ListObjectsV2" . . . 16

"Lista de versiones de objetos" 16
"Lista de partes" 17
"PonerBucketCors" 17
"Cifrado de PutBucket" 17
"Configuración del ciclo de vida de PutBucket" 18
"Configuración de notificación de PutBucket" 19
"Política de depósito de basura" 19
"Replicación de PutBucket" 19
"Etiquetado de PutBucket" 20
"Versiones de PutBucket" 20
"PonerObjeto" 20
"PonerObjetoLegalRetención" 21
"Configuración de bloqueo de objeto de colocación" 21
"PonerRetenciónDeObjeto" 21
"Etiquetado de objetos puestos" 22
"Restaurar objeto" 22
"Seleccionar contenido del objeto" 22
"Subir parte" 22
"Subir copia parcial" 23
Probar la configuración de la API REST de S3 24
Cómo StorageGRID implementa la API REST de S3 25
Solicitudes de clientes conflictivas 25
Valores de consistencia 25
Control de versiones de objetos 28
Utilice la API REST de S3 para configurar el bloqueo de objetos de S3 29
Crear la configuración del ciclo de vida de S3 35
Recomendaciones para implementar la API REST de S3 39
Compatibilidad con la API REST de Amazon S3 40
Detalles de implementación de la API REST de S3 40
Autenticar solicitudes 41
Operaciones en el servicio 42
Operaciones en buckets 42
Operaciones sobre objetos 50
Operaciones para cargas multiparte 79
Respuestas de error 87
Operaciones personalizadas de StorageGRID 90
Operaciones personalizadas de StorageGRID 90
Obtener consistencia del bucket 91
Consistencia del depósito PUT 92
GET Hora del último acceso al bucket 93
Hora del último acceso al depósito PUT 94
Configuración de notificación de metadatos del depósito DELETE 95
Configuración de notificación de metadatos del depósito GET 96
Configuración de notificación de metadatos del depósito PUT 99
Solicitud de uso de almacenamiento GET 105

Solicitudes de depósito obsoletas para cumplimiento heredado . . . 106
Políticas de acceso a grupos y buckets . . . 112
Utilice políticas de acceso a grupos y buckets . . . 112
Ejemplos de políticas de depósito . . . 129
Políticas de grupo de ejemplo . . . 135
Operaciones de S3 rastreadas en los registros de auditoría . . . 138
Operaciones de bucket rastreadas en los registros de auditoría . . . 138
Operaciones de objetos rastreadas en los registros de auditoría . . . 139

Utilice la API REST de S3

Versiones y actualizaciones compatibles con la API REST de S3

StorageGRID admite la API del Servicio de almacenamiento simple (S3), que se implementa como un conjunto de servicios web de transferencia de estado representacional (REST).

La compatibilidad con la API REST de S3 le permite conectar aplicaciones orientadas a servicios desarrolladas para servicios web de S3 con almacenamiento de objetos local que utiliza el sistema StorageGRID . Se requieren cambios mínimos en el uso actual de las llamadas API REST de S3 de una aplicación cliente.

Versiones compatibles

StorageGRID admite las siguientes versiones específicas de S3 y HTTP.

Artículo	Versión
Especificación de la API de S3	"Documentación de Amazon Web Services (AWS): Referencia de la API de Amazon Simple Storage Service"
HTTP	1,1 Para obtener más información sobre HTTP, consulte HTTP/1.1 (RFC 7230-35). "IETF RFC 2616: Protocolo de transferencia de hipertexto (HTTP/1.1)" **Nota**: StorageGRID no admite la canalización HTTP/1.1.

Actualizaciones de la compatibilidad con la API REST de S3

Liberar	Comentarios
11,9	• Se agregó soporte para valores de suma de comprobación SHA-256 precalculados para las siguientes solicitudes y encabezados admitidos. Puede utilizar esta función para verificar la integridad de los objetos cargados: ◦ Carga completa de varias partes: `x-amz-checksum-sha256` ◦ Crear carga múltiple: `x-amz-checksum-algorithm` ◦ Obtener objeto: `x-amz-checksum-mode` ◦ Objeto principal: `x-amz-checksum-mode` ◦ Lista de partes ◦ PonerObjeto: `x-amz-checksum-sha256` ◦ Subir parte: `x-amz-checksum-sha256` • Se agregó la capacidad para que el administrador de la red controle la retención a nivel de inquilino y las configuraciones de cumplimiento. Estas configuraciones afectan la configuración de bloqueo de objetos S3. ◦ Modo de retención predeterminado del depósito y modo de retención de objetos: Gobernanza o Cumplimiento, si lo permite el administrador de la red. ◦ Período de retención predeterminado del depósito y objeto Conservar hasta fecha: debe ser menor o igual a lo permitido por el período de retención máximo establecido por el administrador de la red. • Soporte mejorado para `aws-chunked` codificación y transmisión de contenido `x-amz-content-sha256` valores. Limitaciones: ◦ Si está presente, `chunk-signature` es opcional y no validado ◦ Si está presente, `x-amz-trailer` el contenido se ignora
11,8	Se actualizaron los nombres de las operaciones de S3 para que coincidan con los nombres utilizados en el "Documentación de Amazon Web Services (AWS): Referencia de la API de Amazon Simple Storage Service" .
11,7	• Agregado"Referencia rápida: solicitudes de API de S3 compatibles" . • Se agregó soporte para usar el modo GOBERNANCIA con S3 Object Lock. • Se agregó soporte para StorageGRID específico `x-ntap-sg-cgr-replication-status` encabezado de respuesta para solicitudes de objeto GET y objeto HEAD. Este encabezado proporciona el estado de replicación de un objeto para la replicación entre redes. • Las solicitudes SelectObjectContent ahora admiten objetos Parquet.

Liberar	Comentarios
11,6	• Se agregó soporte para el uso de `partNumber` parámetro de solicitud en solicitudes de objeto GET y objeto HEAD. • Se agregó soporte para un modo de retención predeterminado y un período de retención predeterminado a nivel de depósito para S3 Object Lock. • Se agregó soporte para el `s3:object-lock-remaining-retention-days` Clave de condición de política para establecer el rango de períodos de retención permitidos para sus objetos. • Se cambió el tamaño máximo *recomendado* para una sola operación de objeto PUT a 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice la carga multiparte en su lugar.
11,5	• Se agregó soporte para administrar el cifrado de bucket. • Se agregó soporte para S3 Object Lock y solicitudes de cumplimiento heredadas obsoletas. • Se agregó soporte para usar DELETE Multiple Objects en depósitos versionados. • El `Content-MD5` El encabezado de solicitud ahora se admite correctamente.
11,4	• Se agregó soporte para etiquetado de depósito DELETE, etiquetado de depósito GET y etiquetado de depósito PUT. No se admiten etiquetas de asignación de costos. • Para los depósitos creados en StorageGRID 11.4, ya no es necesario restringir los nombres de claves de objeto para cumplir con las mejores prácticas de rendimiento. • Se agregó soporte para notificaciones de depósito en el `s3:ObjectRestore:Post` tipo de evento. • Ahora se aplican los límites de tamaño de AWS para partes multiparte. Cada parte de una carga multiparte debe tener entre 5 MiB y 5 GiB. La última parte puede ser menor a 5 MiB. • Se agregó soporte para TLS 1.3
11,3	• Se agregó soporte para el cifrado del lado del servidor de datos de objetos con claves proporcionadas por el cliente (SSE-C). • Se agregó soporte para operaciones de ciclo de vida de bucket DELETE, GET y PUT (solo acción de vencimiento) y para `x-amz-expiration` encabezado de respuesta. • Se actualizaron Objeto PUT, Objeto PUT - Copiar y Carga multiparte para describir el impacto de las reglas ILM que utilizan la ubicación sincrónica en la ingesta. • Los cifrados TLS 1.1 ya no son compatibles.

Liberar	Comentarios
11,2	Se agregó soporte para la restauración de objetos POST para su uso con grupos de almacenamiento en la nube. Se agregó soporte para usar la sintaxis de AWS para ARN, claves de condición de política y variables de política en políticas de grupo y de depósito. Las políticas de grupo y de depósito existentes que utilizan la sintaxis StorageGRID seguirán siendo compatibles. **Nota:** Los usos de ARN/URN en otras configuraciones JSON/XML, incluidas aquellas utilizadas en funciones personalizadas de StorageGRID , no han cambiado.
11,1	Se agregó soporte para compartir recursos de origen cruzado (CORS), HTTP para conexiones de cliente S3 a nodos de la red y configuraciones de cumplimiento en los buckets.
11,0	Se agregó soporte para configurar servicios de plataforma (replicación de CloudMirror, notificaciones e integración de búsqueda de Elasticsearch) para depósitos. También se agregó soporte para restricciones de ubicación de etiquetado de objetos para depósitos y la consistencia disponible.
10,4	Se agregó soporte para cambios de escaneo ILM en versiones, actualizaciones de la página Nombres de dominio de puntos finales, condiciones y variables en políticas, ejemplos de políticas y el permiso PutOverwriteObject.
10,3	Se agregó soporte para control de versiones.
10,2	Se agregó soporte para políticas de acceso a grupos y buckets, y para copia multiparte (Cargar parte - Copiar).
10,1	Se agregó soporte para carga de varias partes, solicitudes de estilo alojado virtual y autenticación v4.
10,0	Soporte inicial de la API REST S3 por parte del sistema StorageGRID . La versión actualmente compatible de la *Referencia de API de servicio de almacenamiento simple* es 2006-03-01.

Referencia rápida: solicitudes de API de S3 compatibles

Esta página resume cómo StorageGRID admite las API de Amazon Simple Storage Service (S3).

Esta página incluye solo las operaciones S3 compatibles con StorageGRID.

Para ver la documentación de AWS para cada operación, seleccione el enlace en el encabezado.

Parámetros de consulta URI comunes y encabezados de solicitud

A menos que se indique lo contrario, se admiten los siguientes parámetros de consulta URI comunes:

- `versionId`(según sea necesario para las operaciones de objetos)

A menos que se indique lo contrario, se admiten los siguientes encabezados de solicitud comunes:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Información relacionada

- "Detalles de implementación de la API REST de S3"
- "Referencia de la API de Amazon Simple Storage Service: encabezados de solicitud comunes"

"AbortarMultipartUpload"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud, más este parámetro de consulta URI adicional:

- `uploadId`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones para cargas multiparte"

"Carga completa de varias partes"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud, más este parámetro de consulta URI adicional:

- `uploadId`
- `x-amz-checksum-sha256`

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite estas etiquetas XML del cuerpo de solicitud:

- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

Documentación de StorageGRID

"Carga completa de varias partes"

"Copiar objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más estos encabezados adicionales:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Copiar objeto"

"Crear cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más estos encabezados adicionales:

- `x-amz-bucket-object-lock-enabled`

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en buckets"

"Crear carga de varias partes"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más estos encabezados adicionales:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Crear carga de varias partes"

"Eliminar cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Documentación de StorageGRID

"Operaciones en buckets"

"EliminarBucketCors"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Eliminar cifrado del cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Eliminar ciclo de vida del cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

- "Operaciones en buckets"
- "Crear la configuración del ciclo de vida de S3"

"Política de eliminación de cubos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"EliminarReplicaciónDeBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Eliminar etiquetado de cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Eliminar objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más este encabezado de solicitud adicional:

- `x-amz-bypass-governance-retention`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones sobre objetos"

"Eliminar objetos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más este encabezado de solicitud adicional:

- `x-amz-bypass-governance-retention`

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones sobre objetos"

"Eliminar etiquetado de objetos"

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones sobre objetos"

"ObtenerBucketAcl"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"ObtenerBucketCors"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Obtener cifrado de cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Obtener configuración del ciclo de vida del cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

- "Operaciones en buckets"
- "Crear la configuración del ciclo de vida de S3"

"Obtener la ubicación del cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Configuración de GetBucketNotification"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Obtener política de cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Obtener réplica de cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Obtener etiquetado de cubos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Obtener versiones de Bucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Obtener objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud, más estos parámetros de consulta URI adicionales:

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`

- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

Y estos encabezados de solicitud adicionales:

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Obtener objeto"

"ObtenerObjetoAcl"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones sobre objetos"

"Obtener retención legal de objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"

"Obtener configuración de bloqueo de objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"

"Obtener retención de objetos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"

"Obtener etiquetado de objetos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones sobre objetos"

"Cubo de cabeza"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Objeto principal"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más estos encabezados adicionales:

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Objeto principal"

"Lista de cubos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

Operaciones en el servicio › ListBuckets

"Lista de cargas de varias partes"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más estos parámetros adicionales:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Lista de cargas de varias partes"

"Lista de objetos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más estos parámetros adicionales:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"ListObjectsV2"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más estos parámetros adicionales:

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Lista de versiones de objetos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más estos parámetros adicionales:

- `delimiter`

- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en buckets"

"Lista de partes"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más estos parámetros adicionales:

- `max-parts`
- `part-number-marker`
- `uploadId`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Lista de cargas de varias partes"

"PonerBucketCors"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en buckets"

"Cifrado de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite estas etiquetas XML del cuerpo de solicitud:

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

Documentación de StorageGRID

"Operaciones en buckets"

"Configuración del ciclo de vida de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite estas etiquetas XML del cuerpo de solicitud:

- `And`
- `Days`
- `Expiration`
- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

Documentación de StorageGRID

- "Operaciones en buckets"
- "Crear la configuración del ciclo de vida de S3"

"Configuración de notificación de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite estas etiquetas XML del cuerpo de solicitud:

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

Documentación de StorageGRID

"Operaciones en buckets"

"Política de depósito de basura"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Para obtener detalles sobre los campos de cuerpo JSON admitidos, consulte"Utilice políticas de acceso a grupos y buckets" .

"Replicación de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`

- `Rule`
- `Status`
- `StorageClass`

Documentación de StorageGRID

"Operaciones en buckets"

"Etiquetado de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en buckets"

"Versiones de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Parámetros del cuerpo de la solicitud

StorageGRID admite estos parámetros del cuerpo de la solicitud:

- `VersioningConfiguration`
- `Status`

Documentación de StorageGRID

"Operaciones en buckets"

"PonerObjeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más estos encabezados adicionales:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`

- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Cuerpo de la solicitud

- Datos binarios del objeto

Documentación de StorageGRID

"PonerObjeto"

"PonerObjetoLegalRetención"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"

"Configuración de bloqueo de objeto de colocación"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"

"PonerRetenciónDeObjeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes Para esta solicitud, más este encabezado adicional:

- `x-amz-bypass-governance-retention`

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"

"Etiquetado de objetos puestos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones sobre objetos"

"Restaurar objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Para obtener detalles sobre los campos corporales admitidos, consulte"Restaurar objeto" .

"Seleccionar contenido del objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud.

Cuerpo de la solicitud

Para obtener detalles sobre los campos de cuerpo admitidos, consulte lo siguiente:

- "Utilice S3 Select"
- "Seleccionar contenido del objeto"

"Subir parte"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud, más estos parámetros de consulta URI adicionales:

- `partNumber`
- `uploadId`

Y estos encabezados de solicitud adicionales:

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Cuerpo de la solicitud

- Datos binarios de la pieza

Documentación de StorageGRID

"Subir parte"

"Subir copia parcial"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todosparámetros y encabezados comunes para esta solicitud, más estos parámetros de consulta URI adicionales:

- `partNumber`
- `uploadId`

Y estos encabezados de solicitud adicionales:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Subir copia parcial"

Probar la configuración de la API REST de S3

Puede utilizar la interfaz de línea de comandos de Amazon Web Services (AWS CLI) para probar su conexión al sistema y verificar que puede leer y escribir objetos.

Antes de empezar

- Ha descargado e instalado la AWS CLI desde "aws.amazon.com/cli" .
- Opcionalmente, tienes"creó un punto final de balanceador de carga" . De lo contrario, conoce la dirección IP del nodo de almacenamiento al que desea conectarse y el número de puerto a utilizar. Ver "Direcciones IP y puertos para conexiones de cliente" .
- Tienes"creó una cuenta de inquilino S3" .
- Has iniciado sesión en el inquilino y"creó una clave de acceso" .

Para obtener más detalles sobre estos pasos, consulte"Configurar conexiones de cliente" .

Pasos

1. Configure los ajustes de AWS CLI para usar la cuenta que creó en el sistema StorageGRID :
   a. Entrar al modo de configuración: `aws configure`
   b. Introduzca el ID de la clave de acceso para la cuenta que ha creado.
   c. Introduzca la clave de acceso secreta para la cuenta que ha creado.
   d. Introduzca la región predeterminada a utilizar. Por ejemplo, `us-east-1` .
   e. Ingrese el formato de salida predeterminado a utilizar o presione **Enter** para seleccionar JSON.
2. Crear un depósito.

   Este ejemplo supone que configuró un punto final del balanceador de carga para usar la dirección IP 10.96.101.17 y el puerto 10443.

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

   Si el depósito se crea correctamente, se devuelve la ubicación del depósito, como se ve en el siguiente ejemplo:

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

3. Subir 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 depósito para verificar que se cargó el objeto.

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

5. Eliminar 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 depósito.

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

Cómo StorageGRID implementa la API REST de S3

Solicitudes de clientes conflictivas

Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana".

El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación.

Valores de consistencia

La consistencia proporciona un equilibrio entre la disponibilidad de los objetos y la consistencia de esos objetos en diferentes nodos de almacenamiento y sitios. Puede cambiar la consistencia según lo requiera su aplicación.

De forma predeterminada, StorageGRID garantiza la consistencia de lectura tras escritura para los objetos recién creados. Cualquier operación GET posterior a una operación PUT completada con éxito podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, las actualizaciones de metadatos y las eliminaciones son eventualmente consistentes. Las sobrescrituras generalmente tardan segundos o minutos en propagarse, pero pueden demorar hasta 15 días.

Si desea realizar operaciones de objetos con una consistencia diferente, puede:

- Especificar una consistencia paracada cubo .
- Especificar una consistencia paracada operación de API .
- Cambie la consistencia predeterminada de toda la cuadrícula realizando una de las siguientes tareas:
  - En el Administrador de cuadrícula, vaya a **CONFIGURACIÓN** > **Sistema** > **Configuración de almacenamiento** > **Consistencia predeterminada**.

◦ .

> Un cambio en la consistencia de toda la cuadrícula se aplica solo a los depósitos creados después de que se modificó la configuración. Para determinar los detalles de un cambio, consulte el registro de auditoría ubicado en `/var/local/log` (buscar **consistencyLevel**).

Valores de consistencia

La consistencia afecta cómo se distribuyen los metadatos que StorageGRID utiliza para rastrear objetos entre los nodos y, por lo tanto, la disponibilidad de los objetos para las solicitudes de los clientes.

Puede establecer la consistencia de un depósito o una operación de API en uno de los siguientes valores:

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

Utilice la consistencia "Lectura después de nueva escritura" y "Disponible"

Cuando una operación HEAD o GET utiliza la consistencia "Lectura después de nueva escritura", StorageGRID realiza la búsqueda en varios pasos, de la siguiente manera:

- Primero busca el objeto utilizando una consistencia baja.
- Si esa búsqueda falla, se repite la búsqueda en el siguiente valor de consistencia hasta que alcanza una consistencia equivalente al comportamiento de strong-global.

Si una operación HEAD o GET utiliza la consistencia "Lectura después de nueva escritura" pero el objeto no existe, la búsqueda del objeto siempre alcanzará una consistencia equivalente al comportamiento para una globalización fuerte. Debido a que esta consistencia requiere que varias copias de los metadatos del objeto estén disponibles en cada sitio, puede recibir una gran cantidad de errores internos del servidor 500 si dos o más nodos de almacenamiento en el mismo sitio no están disponibles.

A menos que necesite garantías de consistencia similares a Amazon S3, puede evitar estos errores para las operaciones HEAD y GET configurando la consistencia en "Disponible". Cuando una operación HEAD o GET utiliza la consistencia "Disponible", StorageGRID solo proporciona consistencia eventual. No vuelve a intentar una operación fallida con una consistencia creciente, por lo que no requiere que haya varias copias disponibles de los metadatos del objeto.

Especificar la consistencia para la operación de la API

Para establecer la consistencia de una operación de API individual, los valores de consistencia deben ser compatibles con la operación y debe especificar la consistencia en el encabezado de la solicitud. Este ejemplo establece la consistencia en "Strong-site" para una operación GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

Debe utilizar la misma consistencia para las operaciones PutObject y GetObject.

Especificar la consistencia para el depósito

Para establecer la consistencia del bucket, puede utilizar StorageGRID"Consistencia del depósito PUT" pedido. O puedes"cambiar la consistencia de un cubo" del administrador de inquilinos.

Al configurar la consistencia de un depósito, tenga en cuenta lo siguiente:

- La configuración de la consistencia de un depósito determina qué consistencia se utiliza para las operaciones S3 realizadas en los objetos del depósito o en la configuración del depósito. No afecta las operaciones en el bucket en sí.
- La consistencia de una operación de API individual anula la consistencia del depósito.
- En general, los buckets deben usar la consistencia predeterminada: "Lectura después de nueva 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 la consistencia para cada solicitud de API. Establezca la consistencia a nivel de depósito sólo como último recurso.

Cómo interactúan los controles de consistencia y las reglas ILM para afectar la protección de datos

Tanto su elección de consistencia como su regla ILM afectan cómo se protegen los objetos. Estas configuraciones pueden interactuar.

Por ejemplo, la consistencia utilizada cuando se almacena un objeto afecta la ubicación inicial de los metadatos del objeto, mientras que el comportamiento de ingesta seleccionado para la regla ILM afecta la ubicación inicial de las copias del objeto. Debido a que StorageGRID requiere acceso tanto a los metadatos de un objeto como a sus datos para cumplir con las solicitudes de los clientes, seleccionar niveles de protección coincidentes para la consistencia y el comportamiento de ingesta puede brindar una mejor protección de datos inicial y respuestas del sistema más predecibles.

La siguiente"opciones de ingesta" Están disponibles para las reglas ILM:

Compromiso dual
: StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve el éxito al cliente. Cuando sea posible se realizarán las copias especificadas en la regla ILM.

Estricto
: Se deben realizar todas las copias especificadas en la regla ILM antes de devolver el éxito al cliente.

Equilibrado

StorageGRID intenta hacer todas las copias especificadas en la regla ILM durante la ingesta; si esto no es posible, se hacen copias provisionales y se devuelve el resultado exitoso al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Ejemplo de cómo la consistencia y la regla ILM pueden interactuar

Supongamos que tiene una cuadrícula de dos sitios con la siguiente regla ILM y la siguiente consistencia:

- **Regla ILM**: Crea dos copias de objetos, una en el sitio local y otra en un sitio remoto. Utilice el comportamiento de ingesta estricto.
- **Consistencia**: Fuerte-global (los metadatos del objeto se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en la red, StorageGRID realiza copias de los objetos y distribuye metadatos a ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra pérdida en el momento del mensaje de ingesta exitosa. Por ejemplo, si el sitio local se pierde poco después de la ingesta, aún existen copias de los datos del objeto y de los metadatos del objeto en el sitio remoto. El objeto es completamente recuperable.

Si, en cambio, utilizara la misma regla ILM y la consistencia del sitio fuerte, el cliente podría recibir un mensaje de éxito después de que los datos del objeto se repliquen en el sitio remoto pero antes de que los metadatos del objeto se distribuyan allí. En este caso, el nivel de protección de los metadatos del objeto no coincide con el nivel de protección de los datos del objeto. Si el sitio local se pierde poco después de la ingesta, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre la consistencia y las reglas ILM puede ser compleja. Comuníquese con NetApp si necesita ayuda.

Control de versiones de objetos

Puede establecer el estado de control de versiones de un depósito si desea conservar varias versiones de cada objeto. Habilitar el control de versiones de un bucket puede ayudar a proteger contra la eliminación accidental de objetos y le permite recuperar y restaurar versiones anteriores de un objeto.

El sistema StorageGRID implementa control de versiones con soporte para la mayoría de las funciones y con algunas limitaciones. StorageGRID admite hasta 10 000 versiones de cada objeto.

El control de versiones de objetos se puede combinar con la gestión del ciclo de vida de la información (ILM) de StorageGRID o con la configuración del ciclo de vida del bucket S3. Debe habilitar explícitamente el control de versiones para cada depósito. Cuando se habilita el control de versiones para un depósito, a cada objeto agregado al depósito se le asigna un ID de versión, que es generado por el sistema StorageGRID .

No se admite el uso de MFA (autenticación multifactor).

> El control de versiones solo se puede habilitar en depósitos creados con StorageGRID versión 10.3 o posterior.

ILM y control de versiones

Las políticas ILM se aplican a cada versión de un objeto. Un proceso de escaneo ILM escanea continuamente

todos los objetos y los reevalúa en función de la política ILM actual. Cualquier cambio que realice en las políticas de ILM se aplicará a todos los objetos ingeridos previamente. Esto incluye versiones ingeridas previamente si el control de versiones está habilitado. El escaneo ILM aplica nuevos cambios ILM a objetos ingeridos previamente.

Para los objetos S3 en depósitos habilitados para control de versiones, la compatibilidad con control de versiones le permite crear reglas ILM que usan "Hora no actual" como Hora de referencia (seleccione **Sí** para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores?" en"Paso 1 del asistente para crear una regla de ILM"). Cuando se actualiza un objeto, sus versiones anteriores dejan de ser actuales. El uso de un filtro de "Tiempo no actual" le permite crear políticas que reducen el impacto del almacenamiento de versiones anteriores de los objetos.

> Cuando se carga una nueva versión de un objeto mediante una operación de carga multiparte, el tiempo no actual de la versión original del objeto refleja cuándo se creó la carga multiparte para la nueva versión, no cuándo se completó la carga multiparte. En casos limitados, la hora no actual de la versión original puede ser horas o días anterior a la hora de la versión actual.

Información relacionada

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

Utilice la API REST de S3 para configurar el bloqueo de objetos de S3

Si la configuración global de Bloqueo de objetos S3 está habilitada para su sistema StorageGRID , puede crear depósitos con el Bloqueo de objetos S3 habilitado. Puede especificar la retención predeterminada para cada depósito o configuraciones de retención para cada versión de objeto.

Cómo habilitar el bloqueo de objetos S3 para un bucket

Si la configuración global de Bloqueo de objetos S3 está habilitada para su sistema StorageGRID , puede habilitar opcionalmente el Bloqueo de objetos S3 cuando cree cada depósito.

El bloqueo de objetos S3 es una configuración permanente que solo se puede habilitar cuando se crea un depósito. No es posible agregar ni deshabilitar el bloqueo de objetos S3 después de crear un depósito.

Para habilitar el bloqueo de objetos S3 para un depósito, utilice cualquiera de estos métodos:

- Cree el depósito mediante el Administrador de inquilinos. Ver "Crear un depósito S3" .
- Cree el depósito mediante una solicitud CreateBucket con el `x-amz-bucket-object-lock-enabled` encabezado de solicitud. Ver "Operaciones en buckets" .

El bloqueo de objetos S3 requiere control de versiones del depósito, que se habilita automáticamente cuando se crea el depósito. No se puede suspender el control de versiones del depósito. Ver "Control de versiones de objetos" .

Configuración de retención predeterminada para un depósito

Cuando el bloqueo de objetos S3 está habilitado para un depósito, puede habilitar opcionalmente la retención predeterminada para el depósito y especificar un modo de retención predeterminado y un período de retención predeterminado.

Modo de retención predeterminado

- En modo CUMPLIMIENTO:
  - El objeto no se puede eliminar hasta que se alcance su fecha de conservación.
  - La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir.
  - La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha.
- En modo GOBERNANZA:
  - Usuarios con la `s3:BypassGovernanceRetention` El permiso puede utilizar el `x-amz-bypass-governance-retention: true` encabezado de solicitud para omitir la configuración de retención.
  - Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación.
  - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.

Período de retención predeterminado

Cada depósito puede tener un período de retención predeterminado especificado en años o días.

Cómo configurar la retención predeterminada para un depósito

Para establecer la retención predeterminada para un depósito, utilice cualquiera de estos métodos:

- Administre la configuración del depósito desde el Administrador de inquilinos. Ver"Crear un bucket S3" y"Actualizar la retención predeterminada de bloqueo de objetos S3" .
- Emita una solicitud PutObjectLockConfiguration para el depósito para especificar el modo predeterminado y el número predeterminado de días o años.

Configuración de bloqueo de objeto de colocación

La solicitud PutObjectLockConfiguration le permite establecer y modificar el modo de retención predeterminado y el período de retención predeterminado para un depósito que tiene habilitado el bloqueo de objetos S3. También puede eliminar las configuraciones de retención predeterminadas configuradas previamente.

Cuando se incorporan nuevas versiones de objetos al depósito, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` y `x-amz-object-lock-retain-until-date` no están especificados El período de retención predeterminado se utiliza para calcular la fecha de retención hasta si `x-amz-object-lock-retain-until-date` No está especificado.

Si el período de retención predeterminado se modifica después de la ingesta de una versión de objeto, la fecha de retención de la versión del objeto permanece igual y no se vuelve a calcular utilizando el nuevo período de retención predeterminado.

Debes tener el `s3:PutBucketObjectLockConfiguration` permiso, o ser la cuenta root, para completar esta operación.

El `Content-MD5` El encabezado de la solicitud debe especificarse en la solicitud PUT.

Ejemplo de solicitud

Este ejemplo habilita el bloqueo de objetos S3 para un depósito y establece el modo de retención predeterminado en CUMPLIMIENTO y el período de retención predeterminado en 6 años.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Cómo determinar la retención predeterminada para un bucket

Para determinar si S3 Object Lock está habilitado para un bucket y ver el modo de retención predeterminado y el período de retención, utilice cualquiera de estos métodos:

- Ver el depósito en el Administrador de inquilinos. Ver "Ver depósitos S3" .
- Emite una solicitud GetObjectLockConfiguration.

Obtener configuración de bloqueo de objeto

La solicitud GetObjectLockConfiguration le permite determinar si S3 Object Lock está habilitado para un depósito y, si está habilitado, ver si hay un modo de retención predeterminado y un período de retención configurados para el depósito.

Cuando se incorporan nuevas versiones de objetos al depósito, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` No está especificado. El período de retención predeterminado se utiliza para calcular la fecha de retención hasta si `x-amz-object-lock-retain-until-date` No está especificado.

Debes tener el `s3:GetBucketObjectLockConfiguration` permiso, o ser la cuenta root, para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Ejemplo de respuesta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Cómo especificar la configuración de retención para un objeto

Un depósito con el bloqueo de objetos S3 habilitado puede contener una combinación de objetos con y sin configuraciones de retención de bloqueo de objetos S3.

Las configuraciones de retención a nivel de objeto se especifican mediante la API REST de S3. La configuración de retención de un objeto anula cualquier configuración de retención predeterminada para el depósito.

Puede especificar las siguientes configuraciones para cada objeto:

- **Modo de retención**: CUMPLIMIENTO o GOBERNANZA.
- **Retain-until-date**: una fecha que especifica durante cuánto tiempo StorageGRID debe conservar la versión del objeto.

    - En el modo CUMPLIMIENTO, si la fecha de retención hasta está en el futuro, el objeto se puede recuperar, pero no se puede modificar ni eliminar. La fecha de conservación hasta se puede aumentar, pero esta fecha no se puede disminuir ni eliminar.
    - En el modo GOBERNANZA, los usuarios con permiso especial pueden omitir la configuración de conservar hasta la fecha. Pueden eliminar una versión de un objeto antes de que transcurra su período de retención. También pueden aumentar, disminuir o incluso eliminar la fecha de conservación.
- **Retención legal**: al aplicar una retención legal a una versión de un objeto, se bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesites colocar una retención legal en un objeto que esté relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, sino que permanece vigente hasta que se elimina explícitamente.

  La configuración de retención legal de un objeto es independiente del modo de retención y de la fecha de retención. Si una versión de un objeto está bajo retención legal, nadie puede eliminar esa versión.

Para especificar la configuración de bloqueo de objetos S3 al agregar una versión de objeto a un depósito, emita un"PonerObjeto" ,"Copiar objeto" , o"Crear carga de varias partes" pedido.

Puedes utilizar lo siguiente:

- `x-amz-object-lock-mode`, que puede ser CUMPLIMIENTO o GOBERNANZA (sensible a mayúsculas y minúsculas).

  > Si lo 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 de conservación hasta la fecha debe tener el formato `2020-08-10T21:46:00Z` . Se permiten fracciones de segundo, pero solo se conservan 3 dígitos decimales (precisión de milisegundos). No se permiten otros formatos ISO 8601.
    - La fecha de conservación debe ser en el futuro.
- `x-amz-object-lock-legal-hold`

  Si la retención legal está activada (distingue entre mayúsculas y minúsculas), el objeto se coloca bajo una retención legal. Si la retención legal está desactivada, no se aplica ninguna retención legal. Cualquier otro valor generará un error 400 Solicitud incorrecta (argumento inválido).

Si utiliza alguno de estos encabezados de solicitud, tenga en cuenta estas restricciones:

- El `Content-MD5` El encabezado de solicitud es obligatorio si lo hay `x-amz-object-lock-*` El encabezado de solicitud está presente en la solicitud PutObject. `Content-MD5` no es necesario para CopyObject o CreateMultipartUpload.
- Si el depósito no tiene habilitado el bloqueo de objetos S3 y un `x-amz-object-lock-*` Si el encabezado de solicitud está presente, se devuelve un error 400 Solicitud incorrecta (InvalidRequest).
- La solicitud PutObject admite el uso de `x-amz-storage-class: REDUCED_REDUNDANCY` para que coincida con el comportamiento de AWS. Sin embargo, cuando se ingiere un objeto en un bucket con el bloqueo de objetos S3 habilitado, StorageGRID siempre realizará una ingesta de confirmación dual.
- Una respuesta de versión GET o HeadObject posterior 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 la información correcta `s3:Get*` permisos.

Puedes utilizar el `s3:object-lock-remaining-retention-days` Clave de condición de política para limitar los períodos de retención mínimos y máximos permitidos para sus objetos.

Cómo actualizar la configuración de retención de un objeto

Si necesita actualizar la configuración de retención o retención legal para una versión de objeto existente, puede realizar las siguientes operaciones de subrecurso de objeto:

- `PutObjectLegalHold`

  Si el nuevo valor de retención legal está activado, el objeto se coloca bajo una retención legal. Si el valor de retención legal está DESACTIVADO, se levanta la retención legal.

- `PutObjectRetention`
  - El valor del modo puede ser CUMPLIMIENTO o GOBERNANZA (distingue entre mayúsculas y minúsculas).
  - El valor de conservación hasta la fecha debe tener el formato `2020-08-10T21:46:00Z` . Se permiten fracciones de segundo, pero solo se conservan 3 dígitos decimales (precisión de milisegundos). No se permiten otros formatos ISO 8601.
  - Si una versión de objeto tiene una fecha de conservación existente, solo puedes aumentarla. El nuevo valor debe estar en el futuro.

Cómo utilizar el modo GOBERNANZA

Los usuarios que tengan la `s3:BypassGovernanceRetention` El permiso puede omitir la configuración de retención activa de un objeto que utiliza el modo GOBERNANZA. Cualquier operación DELETE o PutObjectRetention debe incluir el `x-amz-bypass-governance-retention:true` encabezado de solicitud. Estos usuarios pueden realizar estas operaciones adicionales:

- Realice las operaciones DeleteObject o DeleteObjects para eliminar una versión de un objeto antes de que transcurra su período de retención.

  Los objetos que están bajo retención legal no se pueden eliminar. La retención legal debe estar DESACTIVADA.

- Realice operaciones PutObjectRetention que cambien el modo de la versión de un objeto de GOBERNANZA a CUMPLIMIENTO antes de que transcurra el período de retención del objeto.

  Nunca se permite cambiar el modo de CUMPLIMIENTO a GOBERNANZA.

- Realice operaciones PutObjectRetention para aumentar, disminuir o eliminar el período de retención de una versión de objeto.

Información relacionada

- "Administrar objetos con S3 Object Lock"
- "Utilice S3 Object Lock para retener objetos"
- "Guía del usuario de Amazon Simple Storage Service: Bloqueo de objetos"

Crear la configuración del ciclo de vida de S3

Puede crear una configuración de ciclo de vida S3 para controlar cuándo se eliminan objetos específicos del sistema StorageGRID .

El ejemplo simple de esta sección ilustra cómo una configuración del ciclo de vida de S3 puede controlar cuándo se eliminan (caducan) determinados objetos de depósitos S3 específicos. El ejemplo de esta sección es sólo para fines ilustrativos. Para obtener detalles completos sobre la creación de configuraciones del ciclo de vida de S3, consulte "Guía del usuario de Amazon Simple Storage Service: Gestión del ciclo de vida de los objetos" . Tenga en cuenta que StorageGRID solo admite acciones de vencimiento; no admite acciones de transición.

¿Qué es la configuración del ciclo de vida?

Una configuración de ciclo de vida es un conjunto de reglas que se aplican a los objetos en depósitos S3 específicos. Cada regla especifica qué objetos se ven afectados y cuándo expirarán esos objetos (en una fecha específica o después de una cierta cantidad de días).

StorageGRID admite hasta 1000 reglas de ciclo de vida en una configuración de ciclo de vida. Cada regla puede incluir los siguientes elementos XML:

- Vencimiento: elimina un objeto cuando se alcanza una fecha específica o cuando se alcanza una cantidad específica de días, a partir del momento en que se ingirió el objeto.
- NoncurrentVersionExpiration: elimina un objeto cuando se alcanza una cantidad específica de días, a partir del momento en que el objeto dejó de ser actual.
- Filtro (Prefijo, Etiqueta)
- Estado
- IDENTIFICACIÓN

Cada objeto sigue la configuración de retención de un ciclo de vida de un bucket S3 o de una política ILM. Cuando se configura un ciclo de vida de un depósito S3, las acciones de vencimiento del ciclo de vida anulan la política de ILM para los objetos que coinciden con el filtro del ciclo de vida del depósito. Los objetos que no coinciden con el filtro del ciclo de vida del depósito utilizan la configuración de retención de la política de ILM. Si un objeto coincide con un filtro de ciclo de vida de depósito y no se especifican explícitamente acciones de vencimiento, no se utilizan las configuraciones de retención de la política ILM y se implica que las versiones del objeto se conservan para siempre. Ver "Prioridades de ejemplo para el ciclo de vida del depósito S3 y la política de ILM" .

Como resultado, es posible que se elimine un objeto de la cuadrícula aunque las instrucciones de ubicación de una regla ILM todavía se apliquen al objeto. O bien, un objeto podría conservarse en la cuadrícula incluso después de que hayan transcurrido las instrucciones de ubicación de ILM para el objeto. Para obtener más información, consulte "Cómo funciona ILM a lo largo de la vida de un objeto" .

> La configuración del ciclo de vida del bucket se puede usar con buckets que tienen habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida del bucket no es compatible con buckets compatibles heredados.

StorageGRID admite el uso de las siguientes operaciones de depósito para administrar las configuraciones del ciclo de vida:

- Eliminar ciclo de vida del cubo

- Obtener configuración del ciclo de vida del cubo
- Configuración del ciclo de vida de PutBucket

Crear configuración de ciclo de vida

Como primer paso para crear una configuración de ciclo de vida, crea un archivo JSON que incluye una o más reglas. Por ejemplo, este archivo JSON incluye tres reglas, como sigue:

1. La regla 1 se aplica únicamente a los objetos que coinciden con el prefijo `category1` / y que tienen una `key2` valor de `tag2` . El `Expiration` El parámetro especifica que los objetos que coincidan con el filtro caducarán a la medianoche del 22 de agosto de 2020.
2. La regla 2 se aplica únicamente a los objetos que coinciden con el prefijo `category2` /. El `Expiration` El parámetro especifica que los objetos que coinciden con el filtro caducarán 100 días después de su ingesta.

   > Las reglas que especifican un número de días son relativas al momento en que se ingirió el objeto. Si la fecha actual excede la fecha de ingesta más la cantidad de días, es posible que se eliminen algunos objetos del depósito tan pronto como se aplique la configuración del ciclo de vida.

3. La regla 3 se aplica únicamente a los objetos que coinciden con el prefijo `category3` /. El `Expiration` El parámetro especifica que cualquier versión no actual de los objetos coincidentes expirará 50 días después de que dejen de estar actuales.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Aplicar la configuración del ciclo de vida al depósito

Después de haber creado el archivo de configuración del ciclo de vida, debe aplicarlo a un depósito emitiendo una solicitud PutBucketLifecycleConfiguration.

Esta solicitud aplica la configuración del ciclo de vida en el archivo de ejemplo a los objetos en un depósito llamado `testbucket` .

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que una configuración de ciclo de vida se aplicó correctamente al depósito, emita una solicitud GetBucketLifecycleConfiguration. Por ejemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Una respuesta exitosa enumera la configuración del ciclo de vida que acaba de aplicar.

Validar que la expiración del ciclo de vida del bucket se aplique al objeto

Puede determinar si una regla de expiración en la configuración del ciclo de vida se aplica a un objeto específico al emitir una solicitud PutObject, HeadObject o GetObject. Si se aplica una regla, la respuesta incluye una `Expiration` parámetro que indica cuándo expira el objeto y qué regla de expiración coincidió.

> Debido a que el ciclo de vida del bucket anula ILM, `expiry-date` Se muestra la fecha real en la que se eliminará el objeto. Para obtener más información, consulte "Cómo se determina la retención de objetos" .

Por ejemplo, esta solicitud PutObject se emitió el 22 de junio de 2020 y coloca un objeto en el `testbucket` balde.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La respuesta de éxito indica que el objeto caducará en 100 días (1 de octubre de 2020) y que coincidió con la Regla 2 de la configuración del ciclo de vida.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Por ejemplo, esta solicitud HeadObject se utilizó para obtener metadatos para el mismo objeto en el depósito testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La respuesta de éxito incluye los metadatos del objeto e indica que el objeto caducará en 100 días y que coincidió con la Regla 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Para los depósitos con control de versiones habilitado, el `x-amz-expiration` El encabezado de respuesta se aplica solo a las versiones actuales de los objetos.

Recomendaciones para implementar la API REST de S3

Debe seguir estas recomendaciones al implementar la API REST S3 para su uso con StorageGRID.

Recomendaciones para HEADs a objetos inexistentes

Si su aplicación verifica rutinariamente si existe un objeto en una ruta en la que no espera que el objeto exista realmente, debe usar la opción "Disponible"."consistencia" . Por ejemplo, debe utilizar la consistencia "Disponible" si su aplicación encabeza una ubicación antes de PUT en ella.

De lo contrario, si la operación HEAD no encuentra el objeto, es posible que reciba una gran cantidad de errores internos del servidor 500 si dos o más nodos de almacenamiento en el mismo sitio no están disponibles o si no se puede acceder a un sitio remoto.

Puede establecer la consistencia "Disponible" para cada depósito utilizando el"Consistencia del depósito PUT" solicitud, o puede especificar la consistencia en el encabezado de la solicitud para una operación de API individual.

Recomendaciones para claves de objeto

Siga estas recomendaciones para los nombres de claves de objeto, según el momento en que se creó el depósito por primera vez.

Cubos creados en StorageGRID 11.4 o anterior

- No utilice valores aleatorios como los primeros cuatro caracteres de las claves de objeto. Esto contrasta con la recomendación anterior de AWS para prefijos clave. En su lugar, utilice prefijos no aleatorios ni únicos, como `image` .
- Si sigue la recomendación anterior de AWS de utilizar caracteres aleatorios y únicos en los prefijos de clave, anteponga a las claves de objeto un nombre de directorio. Es decir, utiliza este formato:

  ```
  mybucket/mydir/f8e3-image3132.jpg
  ```

  En lugar de este formato:

  ```
  mybucket/f8e3-image3132.jpg
  ```

Cubos creados en StorageGRID 11.4 o posterior

No es necesario restringir los nombres de claves de objeto para cumplir con las mejores prácticas de rendimiento. En la mayoría de los casos, puede utilizar valores aleatorios para los primeros cuatro caracteres de los nombres de claves de objeto.

> Una excepción a esto es una carga de trabajo S3 que elimina continuamente todos los objetos después de un corto período de tiempo. Para minimizar el impacto en el rendimiento de este caso de uso, varíe una parte inicial del nombre de la clave cada varios miles de objetos con algo como la fecha. Por ejemplo, supongamos que un cliente S3 normalmente escribe 2000 objetos por segundo y la política de ciclo de vida del ILM o del bucket elimina todos los objetos después de tres días. Para minimizar el impacto en el rendimiento, puedes nombrar las claves utilizando un patrón como este: `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Recomendaciones para "lecturas de rango"

Si el"Opción global para comprimir objetos almacenados" Si está habilitado, las aplicaciones cliente S3 deben evitar realizar operaciones GetObject que especifiquen un rango de bytes que se devolverán. Estas operaciones de "lectura de rango" son ineficientes porque StorageGRID debe descomprimir efectivamente los objetos para acceder a los bytes solicitados. Las operaciones GetObject que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, es ineficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden expirar.

> Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

Compatibilidad con la API REST de Amazon S3

Detalles de implementación de la API REST de S3

El sistema StorageGRID implementa la API de servicio de almacenamiento simple (versión de API 2006-03-01) con soporte para la mayoría de las operaciones y con algunas limitaciones. Debe comprender los detalles de implementación cuando integra aplicaciones cliente de API REST S3.

El sistema StorageGRID admite solicitudes de estilo alojado virtual y solicitudes de estilo de ruta.

Manejo de fechas

La implementación de StorageGRID de la API REST S3 solo admite formatos de fecha HTTP válidos.

El sistema StorageGRID solo admite formatos de fecha HTTP válidos para cualquier encabezado que acepte valores de fecha. La parte horaria de la fecha se puede especificar en formato de Hora Media de Greenwich (GMT) o en formato de Hora Universal Coordinada (UTC) sin diferencia de zona horaria (se debe especificar +0000). Si incluye el `x-amz-date` encabezado en su solicitud, anula cualquier valor especificado en el encabezado de solicitud de Fecha. Al utilizar AWS Signature Version 4, el `x-amz-date` El encabezado debe estar presente en la solicitud firmada porque el encabezado de fecha no es compatible.

Encabezados de solicitud comunes

El sistema StorageGRID admite los encabezados de solicitud comunes definidos por "Referencia de la API de Amazon Simple Storage Service: encabezados de solicitud comunes" , con una excepción.

Encabezado de solicitud	Implementación
Autorización	Soporte completo para AWS Signature Version 2 Compatibilidad con AWS Signature versión 4, con las siguientes excepciones: • Cuando proporciona el valor de suma de comprobación de carga útil real en `x-amz-content-sha256` , el valor se acepta sin validación, como si el valor `UNSIGNED-PAYLOAD` se había previsto para el encabezado. Cuando usted proporciona un `x-amz-content-sha256` valor de encabezado que implica `aws-chunked` transmisión (por ejemplo, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), las firmas del fragmento no se verifican con los datos del fragmento.
token de seguridad x-amz	No implementado. Devoluciones `XNotImplemented` .

Encabezados de respuesta comunes

El sistema StorageGRID admite todos los encabezados de respuesta comunes definidos por la *Referencia de API del servicio de almacenamiento simple*, con una excepción.

Encabezado de respuesta	Implementación
x-amz-id-2	No utilizado

Autenticar solicitudes

El sistema StorageGRID admite el acceso autenticado y anónimo a objetos mediante la API S3.

La API S3 admite las versiones 2 y 4 de Signature para autenticar solicitudes de API S3.

Las solicitudes autenticadas deben firmarse utilizando su ID de clave de acceso y su clave de acceso secreta.

El sistema StorageGRID admite dos métodos de autenticación: HTTP `Authorization` encabezado y uso de parámetros de consulta.

Utilice el encabezado de autorización HTTP

El HTTP `Authorization` El encabezado lo utilizan todas las operaciones de API de S3, excepto las solicitudes anónimas cuando lo permite la política del bucket. El `Authorization` El 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 prefirmar la URL, que puede utilizarse 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.

Operación	Implementación
Lista de cubos (anteriormente llamado Servicio GET)	Implementado con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.
Uso de almacenamiento GET	El StorageGRID"Uso de almacenamiento GET" La solicitud le indica la cantidad total de almacenamiento en uso por una cuenta y para cada depósito asociado con la cuenta. Esta es 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 /` solicitudes al puerto S3 en un nodo de almacenamiento, sin proporcionar credenciales de autenticación S3, para determinar si el nodo de almacenamiento está disponible. Puede utilizar esta solicitud para realizar monitoreo o para permitir que los balanceadores de carga externos identifiquen cuando un nodo de almacenamiento está inactivo.

Operaciones en buckets

El sistema StorageGRID admite un máximo de 5000 depósitos para cada cuenta de inquilino de S3.

Cada cuadrícula puede tener un máximo de 100.000 contenedores.

Para soportar 5000 buckets, cada nodo de almacenamiento en la red debe tener un mínimo de 64 GB de RAM.

Las restricciones de nombre de depósito siguen las restricciones de la región estándar de AWS EE. UU., pero

debe restringirlas aún más a las convenciones de nombres de DNS para admitir solicitudes de estilo alojado virtualmente S3.

Para obtener más información, consulte lo siguiente:

- "Guía del usuario de Amazon Simple Storage Service: cuotas, restricciones y limitaciones de buckets"
- "Configurar nombres de dominio de puntos finales S3"

Las operaciones ListObjects (GET Bucket) y ListObjectVersions (GET Bucket object versions) admiten StorageGRID"valores de consistencia" .

Puede verificar si las actualizaciones de la última hora de acceso están habilitadas o deshabilitadas para depósitos individuales. Ver "GET Hora del último acceso al bucket" .

La siguiente tabla describe cómo StorageGRID implementa las operaciones del bucket de API REST de S3. Para realizar cualquiera de estas operaciones se deberán proporcionar las credenciales de acceso necesarias a la cuenta.

Operación	Implementación
Crear cubo	Crea un nuevo depósito. Al crear el depósito, usted se convierte en el propietario del mismo. • Los nombres de los depósitos deben cumplir con las siguientes reglas: ◦ Debe ser único en cada sistema StorageGRID (no solo único dentro de la cuenta del inquilino). ◦ Debe ser compatible con DNS. ◦ Debe contener al menos 3 y no más de 63 caracteres. ◦ 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 parecer una dirección IP con formato de texto. ◦ No se deben utilizar puntos en solicitudes de estilo alojado virtualmente. Los períodos causarán problemas con la verificación del certificado comodín del servidor. • De forma predeterminada, los depósitos se crean en el `us-east-1` región; sin embargo, puede utilizar el `LocationConstraint` Elemento de solicitud en el cuerpo de la solicitud para especificar una región diferente. Al utilizar el `LocationConstraint` elemento, debe especificar el nombre exacto de una región que se haya definido utilizando el Administrador de cuadrícula o la API de administración de cuadrícula. Comuníquese con su administrador del sistema si no sabe el nombre de la región que debe utilizar. **Nota**: Se producirá un error si su solicitud CreateBucket utiliza una región que no se ha definido en StorageGRID. • Puedes incluir el `x-amz-bucket-object-lock-enabled` encabezado de solicitud para crear un bucket con el bloqueo de objetos S3 habilitado. Ver "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" . Debe habilitar el bloqueo de objetos S3 al crear el depósito. No es posible agregar ni deshabilitar el bloqueo de objetos S3 después de crear un depósito. El bloqueo de objetos S3 requiere control de versiones del depósito, que se habilita automáticamente cuando se crea el depósito.
Eliminar cubo	Elimina el depósito.
EliminarBucketCors	Elimina la configuración CORS para el bucket.
Eliminar cifrado del cubo	Elimina el cifrado predeterminado del depósito. Los objetos cifrados existentes permanecen cifrados, pero cualquier objeto nuevo que se agregue al depósito no se cifra.
Eliminar ciclo de vida del cubo	Elimina la configuración del ciclo de vida del depósito. Ver "Crear la configuración del ciclo de vida de S3" .

Operación	Implementación
Política de eliminación de cubos	Elimina la política asociada al depósito.
EliminarReplicaciónDeBucket	Elimina la configuración de replicación asociada al depósito.
Eliminar etiquetado de cubo	Utiliza el `tagging` subrecurso para eliminar todas las etiquetas de un depósito. **Precaución**: Si se establece una etiqueta de política ILM no predeterminada para este depósito, habrá un `NTAP-SG-ILM-BUCKET-TAG` etiqueta de cubo con un valor asignado a ella. No emita una solicitud DeleteBucketTagging si hay una `NTAP-SG-ILM-BUCKET-TAG` etiqueta de cubo En su lugar, emita una solicitud PutBucketTagging solo con el `NTAP-SG-ILM-BUCKET-TAG` etiqueta y su valor asignado para eliminar todas las demás etiquetas del depósito. No modifique ni elimine el `NTAP-SG-ILM-BUCKET-TAG` etiqueta de cubo
ObtenerBucketAcl	Devuelve una respuesta positiva y el ID, el nombre para mostrar y el permiso del propietario del depósito, lo que indica que el propietario tiene acceso completo al depósito.
ObtenerBucketCors	Devuelve el `cors` configuración para el bucket.
Obtener cifrado de cubo	Devuelve la configuración de cifrado predeterminada para el depósito.
Obtener configuración del ciclo de vida del cubo (anteriormente llamado ciclo de vida del bucket GET)	Devuelve la configuración del ciclo de vida del depósito. Ver "Crear la configuración del ciclo de vida de S3" .
Obtener la ubicación del cubo	Devuelve la región que se configuró utilizando el `LocationConstraint` elemento en la solicitud CreateBucket. Si la región del cubo es `us-east-1` , se devuelve una cadena vacía para la región.
Configuración de GetBucketNotification (anteriormente llamada notificación GET Bucket)	Devuelve la configuración de notificación adjunta al depósito.
Obtener política de cubo	Devuelve la política asociada al depósito.
Obtener réplica de cubo	Devuelve la configuración de replicación asociada al depósito.

Operación	Implementación
Obtener etiquetado de cubos	Utiliza el `tagging` subrecurso para devolver todas las etiquetas de un depósito. **Precaución**: Si se establece una etiqueta de política ILM no predeterminada para este depósito, habrá un `NTAP-SG-ILM-BUCKET-TAG` etiqueta de cubo con un valor asignado a ella. No modifique ni elimine esta etiqueta.
Obtener versiones de Bucket	Esta implementación utiliza el `versioning` subrecurso para devolver el estado de control de versiones de un bucket. • *blank*: El control de versiones nunca se ha habilitado (el depósito está "Sin versión") • Habilitado: el control de versiones está habilitado • Suspendido: el control de versiones estaba habilitado previamente y está suspendido
Obtener configuración de bloqueo de objeto	Devuelve el modo de retención predeterminado del depósito y el período de retención predeterminado, si está configurado. Ver "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" .
Cubo de cabeza	Determina si existe un depósito y tienes permiso para acceder a él. Esta operación devuelve: • `x-ntap-sg-bucket-id`:El UUID del depósito en formato UUID. • `x-ntap-sg-trace-id`:El ID de seguimiento único de la solicitud asociada.
ListObjects y ListObjectsV2 (anteriormente llamado GET Bucket)	Devuelve algunos o todos (hasta 1000) los objetos de un depósito. La clase de almacenamiento para objetos puede tener cualquiera de dos valores, incluso si el objeto se ingirió con el `REDUCED_REDUNDANCY` opción de clase de almacenamiento: • `STANDARD`, lo que indica que el objeto está almacenado en un grupo de almacenamiento que consta de nodos de almacenamiento. • `GLACIER`, lo que indica que el objeto se ha movido al depósito externo especificado por el grupo de almacenamiento en la nube. Si el depósito contiene una gran cantidad de claves eliminadas que tienen el mismo prefijo, la respuesta podría incluir algunas `CommonPrefixes` que no contienen claves.
Lista de versiones de objetos (anteriormente denominadas versiones del objeto GET Bucket)	Con acceso de LECTURA en un bucket, utilizando esta operación con el `versions` El subrecurso enumera los metadatos de todas las versiones de los objetos en el depósito.

Operación	Implementación
PonerBucketCors	Establece la configuración CORS para un depósito para que éste pueda atender solicitudes de origen cruzado. El uso compartido de recursos entre orígenes (CORS) es un mecanismo de seguridad que permite que las aplicaciones web cliente de un dominio accedan a recursos de un dominio diferente. Por ejemplo, supongamos que utiliza un depósito S3 llamado `images` para almacenar gráficos. Al establecer la configuración CORS para el `images` Cubo, puede permitir que las imágenes en ese cubo se muestren en el sitio web `http://www.example.com` .
Cifrado de PutBucket	Establece el estado de cifrado predeterminado de un depósito existente. Cuando el cifrado a nivel de bucket está habilitado, cualquier objeto nuevo que se añada al bucket se cifra. StorageGRID admite el cifrado del lado del servidor con claves administradas StorageGRID. Al especificar la regla de configuración de cifrado del lado del servidor, configure el `SSEAlgorithm` parámetro a `AES256` , y no utilices el `KMSMasterKeyID` parámetro. La configuración de cifrado predeterminada del depósito se ignora si la solicitud de carga de objetos ya especifica el cifrado (es decir, si la solicitud incluye el cifrado). `x-amz-server-side-encryption-*` encabezado de solicitud).
Configuración del ciclo de vida de PutBucket (anteriormente llamado ciclo de vida del bucket PUT)	Crea una nueva configuración de ciclo de vida para el depósito o reemplaza una configuración de ciclo de vida existente. StorageGRID admite hasta 1000 reglas de ciclo de vida en una configuración de ciclo de vida. Cada regla puede incluir los siguientes elementos XML: • Vencimiento (Días, Fecha, ExpiredObjectDeleteMarker) • Caducidad de la versión no actual (versiones no actuales más recientes, días no actuales) • Filtro (Prefijo, Etiqueta) • Estado • IDENTIFICACIÓN StorageGRID no admite estas acciones: • Cancelar carga multiparte incompleta • Transición Ver "Crear la configuración del ciclo de vida de S3" . Para comprender cómo la acción de Vencimiento en el ciclo de vida de un bucket interactúa con las instrucciones de ubicación de ILM, consulte"Cómo funciona ILM a lo largo de la vida de un objeto" . **Nota**: La configuración del ciclo de vida del bucket se puede usar con buckets que tienen habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida del bucket no es compatible con buckets compatibles heredados.

Operación	Implementación

Configuración de notificación de PutBucket
 	
(anteriormente denominada notificación PUT Bucket)
	Configura las notificaciones para el depósito utilizando el XML de configuración de notificaciones incluido en el cuerpo de la solicitud. Debe tener en cuenta los siguientes detalles de implementación:
	
	• StorageGRID admite Amazon Simple Notification Service (Amazon SNS) o temas de Kafka como destinos. No se admiten los puntos finales de Simple Queue Service (SQS) ni de Amazon Lambda.
	• El destino de las notificaciones debe especificarse como la URN de un punto final de StorageGRID . Los puntos finales se pueden crear utilizando el Administrador de inquilinos o la API de administración de inquilinos.
	
	El punto final debe existir para que la configuración de la notificación sea exitosa. Si el punto final no existe, un `400 Bad Request` Se devuelve un error con el código `InvalidArgument` .
	
	• No se puede configurar una notificación para los siguientes tipos de eventos. Estos tipos de eventos **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 otras, como se muestra en la siguiente lista:
	◦ **Fuente del evento**
	
	`sgws:s3`
	
	◦ **awsRegión**
	
	no incluido
	
	◦ **x-amz-id-2**
	
	no incluido
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

Política de depósito de basura	Establece la política asociada al depósito. Ver "Utilice políticas de acceso a grupos y buckets" .

Operación	Implementación
Replicación de PutBucket	Configura"Replicación de StorageGRID CloudMirror" para el depósito que utiliza el XML de configuración de replicación proporcionado en el cuerpo de la solicitud. Para la replicación de CloudMirror, debe tener en cuenta los siguientes detalles de implementación: • StorageGRID solo admite la versión 1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de `Filter` elemento para reglas y sigue las convenciones V1 para la eliminación de versiones de objetos. Para más detalles, véase "Guía del usuario de Amazon Simple Storage Service: Configuración de replicación" . • La replicación de buckets se puede configurar en buckets versionados o no versionados. • Puede especificar un depósito de destino diferente en cada regla del XML de configuración de replicación. Un depósito de origen puede replicarse en más de un depósito de destino. • Los depósitos de destino deben especificarse como el URN de los puntos finales de StorageGRID , tal como se especifica en el Administrador de inquilinos o en la API de administración de inquilinos. Ver "Configurar la replicación de CloudMirror" . El punto final debe existir para que la configuración de la replicación sea exitosa. Si el punto final no existe, la solicitud falla como `400 Bad Request` El mensaje de error dice: `Unable to save the replication policy. The specified endpoint URN does not exist: URN.` • No es necesario especificar un `Role` en el XML de configuración. StorageGRID no utiliza este valor y se ignorará si se envía. • Si omite la clase de almacenamiento del XML de configuración, StorageGRID utiliza la `STANDARD` clase de almacenamiento por defecto. • Si elimina un objeto del depósito de origen o elimina el depósito de origen en sí, el comportamiento de replicación entre regiones es el siguiente: ◦ Si elimina el objeto o el depósito antes de que se haya replicado, el objeto o depósito no se replica y no se le notifica. ◦ Si elimina el objeto o el depósito después de haberlo replicado, StorageGRID sigue el comportamiento de eliminación estándar de Amazon S3 para la versión 1 de la replicación entre regiones.

Operación	Implementación
Etiquetado de PutBucket	Utiliza el `tagging` subrecurso para agregar o actualizar un conjunto de etiquetas para un depósito. Al agregar etiquetas de depósito, tenga en cuenta las siguientes limitaciones: • Tanto StorageGRID como Amazon S3 admiten hasta 50 etiquetas para cada bucket. • Las etiquetas asociadas a un bucket deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener una longitud de hasta 128 caracteres Unicode. • Los valores de las etiquetas pueden tener una longitud de hasta 256 caracteres Unicode. • La clave y los valores distinguen entre mayúsculas y minúsculas. **Precaución**: Si se establece una etiqueta de política ILM no predeterminada para este depósito, habrá un `NTAP-SG-ILM-BUCKET-TAG` etiqueta de cubo con un valor asignado a ella. Asegúrese de que el `NTAP-SG-ILM-BUCKET-TAG` La etiqueta de bucket se incluye con el valor asignado en todas las solicitudes PutBucketTagging. No modifique ni elimine esta etiqueta. **Nota**: Esta operación sobrescribirá cualquier etiqueta actual que el depósito ya tenga. Si se omite alguna etiqueta existente del conjunto, dicha etiqueta se eliminará del depósito.
Versiones de PutBucket	Utiliza el `versioning` subrecurso para establecer el estado de control de versiones de un bucket existente. Puede establecer el estado de la versión con uno de los siguientes valores: • Habilitado: habilita el control de versiones de los objetos en el depósito. Todos los objetos agregados al depósito reciben un ID de versión único. • Suspendido: deshabilita el control de versiones de los objetos en el depósito. Todos los objetos agregados al depósito reciben el ID de la versión `null` .
Configuración de bloqueo de objeto de colocación	Configura o elimina el modo de retención predeterminado del depósito y el período de retención predeterminado. Si se modifica el período de retención predeterminado, la fecha de retención de las versiones de objetos existentes permanece igual y no se vuelve a calcular utilizando el nuevo período de retención predeterminado. Ver"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" para obtener información detallada.

Operaciones sobre objetos

Operaciones sobre objetos

Esta sección describe cómo el sistema StorageGRID implementa operaciones de API REST S3 para objetos.

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

- StorageGRID"valores de consistencia" son compatibles con todas las operaciones sobre objetos, con excepción de las siguientes:
  - ObtenerObjetoAcl
  - `OPTIONS /`
  - PonerObjetoLegalRetención
  - PonerRetenciónDeObjeto
  - Seleccionar contenido del objeto
- Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación.
- Todos los objetos en un depósito StorageGRID son propiedad del propietario del depósito, incluidos los objetos creados por un usuario anónimo o por otra cuenta.
- No se puede acceder a los objetos de datos ingresados al sistema StorageGRID a través de Swift a través de S3.

La siguiente tabla describe cómo StorageGRID implementa las operaciones de objetos de la API REST de S3.

Operación	Implementación
Eliminar objeto	Autenticación multifactor (MFA) y el encabezado de respuesta `x-amz-mfa` no son compatibles Al procesar una solicitud DeleteObject, StorageGRID intenta eliminar inmediatamente todas las copias del objeto de todas las ubicaciones almacenadas. Si tiene éxito, StorageGRID devuelve una respuesta al cliente inmediatamente. Si no se pueden eliminar todas las copias en 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y luego indica el éxito al cliente. **Control de versiones** Para eliminar una versión específica, el solicitante debe ser el propietario del depósito y utilizar el `versionId` subrecurso. El uso de este subrecurso elimina permanentemente la versión. Si el `versionId` corresponde a un marcador de eliminación, el encabezado de respuesta `x-amz-delete-marker` se devuelve establecido en `true` . • Si se elimina un objeto sin el `versionId` subrecurso en un bucket con control de versiones habilitado, esto genera un marcador de eliminación. El `versionId` para el marcador de eliminación se devuelve utilizando el `x-amz-version-id` encabezado de respuesta y el `x-amz-delete-marker` El encabezado de respuesta se devuelve configurado en `true` . • Si se elimina un objeto sin el `versionId` subrecurso en un bucket con control de versiones suspendido, esto da como resultado una eliminación permanente de una versión 'nula' ya existente o un marcador de eliminación 'nulo' y la generación de un nuevo marcador de eliminación 'nulo'. El `x-amz-delete-marker` El encabezado de respuesta se devuelve configurado en `true` . **Nota**: En ciertos casos, pueden existir múltiples marcadores de eliminación para un objeto. Ver"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" para aprender cómo eliminar versiones de objetos en el modo GOBERNANZA.
Eliminar objetos (anteriormente llamado ELIMINAR Múltiples Objetos)	Autenticación multifactor (MFA) y el encabezado de respuesta `x-amz-mfa` no son compatibles Se pueden eliminar varios objetos en el mismo mensaje de solicitud. Ver"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" para aprender cómo eliminar versiones de objetos en el modo GOBERNANZA.

Operación	Implementación
Eliminar etiquetado de objetos	Utiliza el `tagging` subrecurso para eliminar todas las etiquetas de un objeto. **Control de versiones** Si el `versionId` Si 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 depósito versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "Método no permitido" con el `x-amz-delete-marker` encabezado de respuesta establecido en `true` .
Obtener objeto	"Obtener objeto"
ObtenerObjetoAcl	Si se proporcionan las credenciales de acceso necesarias para la cuenta, la operación devuelve una respuesta positiva y el ID, el nombre para mostrar y el permiso del propietario del objeto, lo que indica que el propietario tiene acceso completo al objeto.
Obtener retención legal de objeto	"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"
Obtener retención de objetos	"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"
Obtener etiquetado de objetos	Utiliza el `tagging` subrecurso para devolver todas las etiquetas de un objeto. **Control de versiones** Si el `versionId` Si 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 depósito versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "Método no permitido" con el `x-amz-delete-marker` encabezado de respuesta establecido en `true` .
Objeto principal	"Objeto principal"
Restaurar objeto	"Restaurar objeto"
PonerObjeto	"PonerObjeto"
Copiar objeto (anteriormente llamado Objeto PUT - Copiar)	"Copiar objeto"
PonerObjetoLegalRetención	"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"

Operación	Implementación
PonerRetenciónDeObjeto	"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"
Etiquetado de objetos puestos	Utiliza el `tagging` subrecurso para agregar un conjunto de etiquetas a un objeto existente. **Límites de etiquetas de objetos** Puede agregar etiquetas a objetos nuevos cuando los cargue o puede agregarlas a objetos existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas para cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener una longitud de hasta 128 caracteres Unicode y los valores de etiqueta pueden tener una longitud de hasta 256 caracteres Unicode. La clave y los valores distinguen entre mayúsculas y minúsculas. **Actualizaciones de etiquetas y comportamiento de ingesta** Cuando utiliza PutObjectTagging para actualizar las etiquetas de un objeto, StorageGRID no vuelve a ingerir el objeto. Esto significa que no se utiliza la opción de Comportamiento de ingesta especificada en la regla ILM correspondiente. Cualquier cambio en la ubicación de objetos que se active mediante la actualización se realiza cuando ILM se vuelve a evaluar mediante procesos de fondo normales de ILM. Esto significa que si la regla ILM usa la opción Estricta para el comportamiento de ingesta, no se realiza ninguna acción si no se pueden realizar las ubicaciones de objetos requeridas (por ejemplo, porque una nueva ubicación requerida no está disponible). El objeto actualizado conserva su ubicación actual hasta que sea posible la ubicación requerida. **Resolución de conflictos** Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación. **Control de versiones** Si el `versionId` Si el parámetro de consulta no se especifica en la solicitud, la operación agrega etiquetas a la versión más reciente del objeto en un depósito versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "Método no permitido" con el `x-amz-delete-marker` encabezado de respuesta establecido en `true` .
Seleccionar contenido del objeto	"Seleccionar contenido del objeto"

Utilice S3 Select

StorageGRID admite las siguientes cláusulas Select de Amazon S3, tipos de datos y operadores para"Comando SelectObjectContent" .

> Cualquier artículo que no esté en la lista no será compatible.

Para la sintaxis, véase"Seleccionar contenido del objeto" . Para obtener más información sobre S3 Select, consulte la "Documentación de AWS para S3 Select" .

Solo las cuentas de inquilino que tienen S3 Select habilitado pueden emitir consultas SelectObjectContent. Ver el"Consideraciones y requisitos para el uso de S3 Select" .

Cláusulas

- Lista SELECT
- cláusula FROM
- cláusula WHERE
- Cláusula LIMIT

Tipos de datos

- bool
- entero
- cadena
- flotar
- decimal, numérico
- marca de tiempo

Operadores

Operadores lógicos

- Y
- NO
- O

Operadores de comparación

- <
- >
- ⇐
- >=
- =
- =
- <>

- !=
- ENTRE
- EN

Operadores de coincidencia de patrones

- COMO
- _
- %

Operadores unitarios

- ES NULO
- NO ES NULO

Operadores matemáticos

- +
- -
- *
- /
- %

StorageGRID sigue la precedencia del operador Amazon S3 Select.

Funciones agregadas

- AVG()
- CONTAR(*)
- MÁX()
- MÍNIMO()
- SUMA()

Funciones condicionales

- CASO
- JUNTARSE
- NULLIF

Funciones de conversión

- CAST (para tipos de datos admitidos)

Funciones de fecha

- FECHA_AÑADIR
- FECHA_DIFF

- EXTRACTO
- A_CADENA
- HASTA_LA_MARCA_DE_TIEMPO
- UTCNOW

Funciones de cadena

- LONGITUD_CARACTER, LONGITUD_CARACTER
- MÁS BAJO
- SUBCADENA
- RECORTAR
- SUPERIOR

Utilice cifrado del lado del servidor

El cifrado del lado del servidor le permite proteger los datos de sus objetos en reposo. StorageGRID cifra los datos a medida que escribe el objeto y los descifra cuando accede al objeto.

Si desea utilizar el cifrado del lado del servidor, puede elegir cualquiera de dos opciones mutuamente excluyentes, según cómo se administren las claves de cifrado:

- **SSE (cifrado del lado del servidor con claves administradas por StorageGRID)**: cuando emite una solicitud 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 emite una solicitud S3 para almacenar un objeto, proporciona su propia clave de cifrado. Cuando recupera un objeto, proporciona la misma clave de cifrado como parte de su solicitud. Si las dos claves de cifrado coinciden, el objeto se descifra y se devuelven los datos del objeto.

  Si bien StorageGRID administra todas las operaciones de cifrado y descifrado de objetos, usted debe administrar las claves de cifrado que proporciona.

> Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente.

> Si un objeto está cifrado con SSE o SSE-C, se ignoran todas las configuraciones de cifrado a nivel de bucket o de cuadrícula.

Utilice SSE

Para cifrar un objeto con una clave única administrada por StorageGRID, utilice el siguiente encabezado de solicitud:

```
x-amz-server-side-encryption
```

El encabezado de solicitud SSE es compatible con las siguientes operaciones de objeto:

- "PonerObjeto"

- "Copiar objeto"
- "Crear carga de varias partes"

Utilice SSE-C

Para cifrar un objeto con una clave única que usted administra, utiliza tres encabezados de solicitud:

Encabezado de solicitud	Descripción
`x-amz-server-side-encryption-customer-algorithm`	Especifique el algoritmo de cifrado. El valor del 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 ser de 256 bits y estar codificado en base64.
`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 transmitió sin errores. El valor del resumen MD5 debe estar codificado en base64 de 128 bits.

Los encabezados de solicitud SSE-C son compatibles con las siguientes operaciones de objetos:

- "Obtener objeto"
- "Objeto principal"
- "PonerObjeto"
- "Copiar objeto"
- "Crear carga de varias partes"
- "Subir parte"
- "Subir copia parcial"

Consideraciones para el uso del cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C)

Antes de utilizar SSE-C, tenga en cuenta las siguientes consideraciones:

- Debes utilizar https.

> StorageGRID rechaza cualquier solicitud realizada a través de HTTP al usar SSE-C. Por razones de seguridad, considere que cualquier clave que envíe accidentalmente a través de HTTP está comprometida. Deseche la llave y gírela según corresponda.

- La ETag en la respuesta no es el MD5 de los datos del objeto.
- Debe administrar la asignación de claves de cifrado a los objetos. StorageGRID no almacena claves de cifrado. Usted es responsable de rastrear la clave de cifrado que proporciona para cada objeto.
- Si su depósito tiene habilitada la gestión de versiones, cada versión del objeto debe tener su propia clave de cifrado. Usted es responsable de realizar el seguimiento de la clave de cifrado utilizada para cada versión del objeto.

- Dado que administra las claves de cifrado en el lado del cliente, también debe administrar cualquier protección adicional, como la rotación de claves, en el lado del cliente.

> Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente.

- Si la replicación entre redes o la replicación de CloudMirror están configuradas para el bucket, no podrá ingerir objetos SSE-C. La operación de ingesta fallará.

Información relacionada

"Guía del usuario de Amazon S3: Uso del cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C)"

Copiar objeto

Puede utilizar la solicitud S3 CopyObject para crear una copia de un objeto que ya esté almacenado en S3. Una operación CopyObject es lo mismo que realizar GetObject seguido de PutObject.

Resolver conflictos

Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación.

Tamaño del objeto

El tamaño máximo *recomendado* para una sola operación PutObject es 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice"carga multiparte" en cambio.

El tamaño máximo *admitido* para una sola operación PutObject es 5 TiB (5.497.558.138.880 bytes).

> Si actualizó desde StorageGRID 11.6 o una versión anterior, se activará la alerta de tamaño de objeto PUT de S3 demasiado grande si intenta cargar un objeto que supere los 5 GiB. Si tiene una nueva instalación de StorageGRID 11.7 o 11.8, la alerta no se activará en este caso. Sin embargo, para alinearse con el estándar AWS S3, las futuras versiones de StorageGRID no admitirán cargas de objetos de más de 5 GiB.

Caracteres UTF-8 en metadatos de usuario

Si una solicitud incluye valores UTF-8 (sin escapar) 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 caracteres UTF-8 escapados incluidos en el nombre de clave o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 escapados se tratan como caracteres ASCII:

- Las solicitudes tienen éxito si los metadatos definidos por el usuario incluyen caracteres UTF-8 escapados.
- StorageGRID no devuelve el `x-amz-missing-meta` encabezado si el valor interpretado del nombre o valor de la clave incluye caracteres no imprimibles.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario
- `x-amz-metadata-directive`:El valor predeterminado es `COPY` , que le permite copiar el objeto y los metadatos asociados.

  Puedes especificar `REPLACE` para sobrescribir los metadatos existentes al copiar el objeto o para 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.

  Puedes especificar `REPLACE` para sobrescribir las etiquetas existentes al copiar el objeto o para actualizar las etiquetas.

- Encabezados de solicitud de bloqueo de objetos S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si se realiza una solicitud sin estos encabezados, se utilizan las configuraciones de retención predeterminadas del depósito para calcular el modo de versión del objeto y la fecha de retención. Ver "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" .

- Encabezados de solicitud SSE:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    VerEncabezados de solicitud para el cifrado del lado del servidor

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

  Cuando copia un objeto, si el objeto de origen tiene una suma de comprobación, StorageGRID no copia ese valor de suma de comprobación al nuevo objeto. Este comportamiento se aplica independientemente de si intenta utilizarlo o no. `x-amz-checksum-algorithm` en la solicitud de objeto.

- `x-amz-website-redirect-location`

Opciones de clase de almacenamiento

El `x-amz-storage-class` Se admite el encabezado de solicitud y afecta la cantidad de copias de objetos que crea StorageGRID si la regla ILM correspondiente usa la confirmación dual o equilibrada."opción de ingesta" .

- `STANDARD`

  (Predeterminado) Especifica una operación de ingesta de confirmación dual cuando la regla ILM usa la opción Confirmación dual o cuando la opción Equilibrada recurre a la creación de copias provisionales.

- `REDUCED_REDUNDANCY`

  Especifica una operación de ingesta de confirmación única cuando la regla ILM usa la opción de confirmación dual o cuando la opción Equilibrada recurre a la creación de copias provisionales.

  > Si está ingiriendo un objeto en un depósito con el bloqueo de objetos S3 habilitado, `REDUCED_REDUNDANCY` La opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, el `REDUCED_REDUNDANCY` La opción devuelve un error. StorageGRID siempre realizará una ingesta de confirmación dual para garantizar que se cumplan los requisitos de cumplimiento.

Uso de x-amz-copy-source en CopyObject

Si el depósito de origen y la clave se especifican en el `x-amz-copy-source` encabezado, son diferentes del depósito de destino y la clave, se escribe una copia de los datos del objeto de origen en el destino.

Si el origen y el destino coinciden, y el `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 ingerir el objeto. Esto tiene dos consecuencias importantes:

- No se puede utilizar CopyObject para cifrar un objeto existente en un lugar, ni para cambiar el cifrado de un objeto existente en un lugar. Si usted suministra el `x-amz-server-side-encryption` encabezado o

el `x-amz-server-side-encryption-customer-algorithm` encabezado, StorageGRID rechaza la solicitud y devuelve `XNotImplemented` .

- No se utiliza la opción de Comportamiento de ingestión especificada en la regla ILM correspondiente. Cualquier cambio en la ubicación de objetos que se active mediante la actualización se realiza cuando ILM se vuelve a evaluar mediante procesos de fondo normales de ILM.

  Esto significa que si la regla ILM usa la opción Estricta para el comportamiento de ingesta, no se realiza ninguna acción si no se pueden realizar las ubicaciones de objetos requeridas (por ejemplo, porque una nueva ubicación requerida no está disponible). El objeto actualizado conserva su ubicación actual hasta que sea posible la ubicación requerida.

Encabezados de solicitud para el cifrado del lado del servidor

Si usted"utilizar cifrado del lado 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 está cifrado mediante una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud CopyObject, para que el objeto pueda descifrarse y luego copiarse:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar `AES256` .
  - `x-amz-copy-source-server-side-encryption-customer-key`:Especifique la clave de cifrado que proporcionó cuando creó el objeto de origen.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 que proporcionó cuando creó el objeto de origen.
- Si desea cifrar el objeto de destino (la copia) con una clave única que usted proporciona y administra, incluya los siguientes tres encabezados:
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256` .
  - `x-amz-server-side-encryption-customer-key`:Especifique una nueva clave de cifrado para el objeto de destino.
  - `x-amz-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 de la nueva clave de cifrado.

  > Las claves de cifrado que 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 los objetos, revise las consideraciones para"utilizando cifrado del lado del servidor" .

- Si desea cifrar el objeto de destino (la copia) con una clave única administrada por StorageGRID (SSE), incluya este encabezado en la solicitud CopyObject:
  - `x-amz-server-side-encryption`

  > El `server-side-encryption` El valor del objeto no se puede actualizar. En lugar de eso, haga una copia con un nuevo `server-side-encryption` valor usando `x-amz-metadata-directive` : `REPLACE` .

Control de versiones

Si el depósito de origen tiene versiones, puede utilizar el `x-amz-copy-source` encabezado para copiar la última versión de un objeto. Para copiar una versión específica de un objeto, debe especificar explícitamente la versión a copiar utilizando el `versionId` subrecurso. Si el depósito de destino está versionado, la versión generada se devuelve en el `x-amz-version-id` encabezado de respuesta. Si se suspende el control de versiones para el depósito de destino, entonces `x-amz-version-id` devuelve un valor "nulo".

Obtener objeto

Puede utilizar la solicitud GetObject de S3 para recuperar un objeto de un depósito de S3.

GetObject y objetos multipart

Puedes utilizar el `partNumber` parámetro de solicitud para recuperar una parte específica de un objeto multiparte o segmentado. El `x-amz-mp-parts-count` El elemento de respuesta indica cuántas partes tiene el objeto.

Puedes configurar `partNumber` a 1 tanto para objetos segmentados/multiparte como para objetos no segmentados/no multiparte; sin embargo, el `x-amz-mp-parts-count` El elemento de respuesta solo se devuelve para objetos segmentados o multiparte.

Caracteres UTF-8 en metadatos de usuario

StorageGRID no analiza ni interpreta caracteres UTF-8 escapados en metadatos definidos por el usuario. Las solicitudes GET para 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 la clave incluye caracteres no imprimibles.

Encabezado de solicitud compatible

Se admite el siguiente encabezado de solicitud:

- `x-amz-checksum-mode`: Especificar `ENABLED`

  El `Range` El encabezado no es compatible con `x-amz-checksum-mode` para ObtenerObjeto. Cuando incluyes `Range` en la solicitud con `x-amz-checksum-mode` habilitado, StorageGRID no devuelve un valor de suma de comprobación en la respuesta.

Encabezado de solicitud no compatible

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented` :

- `x-amz-website-redirect-location`

Control de versiones

Si un `versionId` Si no se especifica el subrecurso, la operación obtiene la versión más reciente del objeto en un depósito versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "No encontrado" con el `x-amz-delete-marker` encabezado de respuesta establecido en `true` .

Encabezados de solicitud para cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utilice los tres encabezados si el objeto está encriptado con una clave única que usted proporcionó.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256` .
- `x-amz-server-side-encryption-customer-key`:Especifique su clave de cifrado para el objeto.
- `x-amz-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 de la clave de cifrado del objeto.

> Las claves de cifrado que 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 los objetos, revise las consideraciones en"Utilice cifrado del lado del servidor" .

Comportamiento de GetObject para objetos del grupo de almacenamiento en la nube

Si un objeto ha sido almacenado en un"Grupo de almacenamiento en la nube" , el comportamiento de una solicitud GetObject depende del estado del objeto. Ver"Objeto principal" Para más detalles.

> Si un objeto está almacenado en un grupo de almacenamiento en la nube y también existen una o más copias del objeto en la red, las solicitudes GetObject intentarán recuperar datos de la red, antes de recuperarlos del grupo de almacenamiento en la nube.

Estado del objeto	Comportamiento de GetObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un grupo de almacenamiento tradicional o que utiliza codificación de borrado	`200 OK` Se recupera una copia del objeto.
Objeto en el grupo de almacenamiento en la nube pero que aún no ha pasado a un estado no recuperable	`200 OK` Se recupera una copia del objeto.
Objeto en transición a un estado no recuperable	`403 Forbidden` , `InvalidObjectState` Utilice un"Restaurar objeto" solicitud para restaurar el objeto a un estado recuperable.
Objeto en proceso de restauración desde un estado no recuperable	`403 Forbidden` , `InvalidObjectState` Espere a que se complete la solicitud RestoreObject.
Objeto completamente restaurado al grupo de almacenamiento en la nube	`200 OK` Se recupera una copia del objeto.

Objetos multiparte o segmentados en un grupo de almacenamiento en la nube

Si cargó un objeto de varias partes o si StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el grupo de almacenamiento en la nube mediante el muestreo de un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud GetObject podría devolver incorrectamente `200 OK` cuando algunas partes del objeto ya han sido trasladadas a un estado no recuperable o cuando algunas partes del objeto aún no han sido restauradas.

En estos casos:

- La solicitud GetObject podría devolver algunos datos pero detenerse a mitad de la transferencia.
- Una solicitud GetObject posterior podría devolver `403 Forbidden`.

GetObject y replicación entre cuadrículas

Si estas usando"federación de red" y"replicación entre redes" está habilitado para un bucket, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud GetObject. La respuesta incluye el StorageGRID específico `x-ntap-sg-cgr-replication-status` encabezado de respuesta, que tendrá uno de los siguientes valores:

Red	Estado de replicación
Fuente	• **COMPLETADO**: La replicación fue exitosa. • **PENDIENTE**: El objeto aún no ha sido replicado. • **FALLO**: La replicación falló con un error permanente. Un usuario debe resolver el error.
Destino	**RÉPLICA**: El objeto fue replicado desde la cuadrícula de origen.

> StorageGRID no es compatible con `x-amz-replication-status` encabezamiento.

Objeto principal

Puede utilizar la solicitud S3 HeadObject para recuperar metadatos de un objeto sin devolver el objeto en sí. Si el objeto está almacenado en un grupo de almacenamiento en la nube, puede usar HeadObject para determinar el estado de transición del objeto.

Objetos HeadObject y multipart

Puedes utilizar el `partNumber` parámetro de solicitud para recuperar metadatos para una parte específica de un objeto multiparte o segmentado. El `x-amz-mp-parts-count` El elemento de respuesta indica cuántas partes tiene el objeto.

Puedes configurar `partNumber` a 1 tanto para objetos segmentados/multiparte como para objetos no segmentados/no multiparte; sin embargo, el `x-amz-mp-parts-count` El elemento de respuesta solo se devuelve para objetos segmentados o multiparte.

Caracteres UTF-8 en metadatos de usuario

StorageGRID no analiza ni interpreta caracteres UTF-8 escapados en metadatos definidos por el usuario. Las solicitudes HEAD para 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 la clave incluye caracteres no imprimibles.

Encabezado de solicitud compatible

Se admite el siguiente encabezado de solicitud:

- `x-amz-checksum-mode`

  El `partNumber` parámetro y `Range` Los encabezados no son compatibles con `x-amz-checksum-mode` para HeadObject. Cuando los incluyas en la solicitud con `x-amz-checksum-mode` habilitado, StorageGRID no devuelve un valor de suma de comprobación en la respuesta.

Encabezado de solicitud no compatible

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented` :

- `x-amz-website-redirect-location`

Control de versiones

Si un `versionId` Si no se especifica el subrecurso, la operación obtiene la versión más reciente del objeto en un depósito versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "No encontrado" con el `x-amz-delete-marker` encabezado de respuesta establecido en `true` .

Encabezados de solicitud para cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utilice estos tres encabezados si el objeto está encriptado con una clave única que usted proporcionó.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256` .
- `x-amz-server-side-encryption-customer-key`:Especifique su clave de cifrado para el objeto.
- `x-amz-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 de la clave de cifrado del objeto.

> ⚠ Las claves de cifrado que 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 los objetos, revise las consideraciones en"Utilice cifrado del lado del servidor" .

Respuestas de HeadObject para objetos de Cloud Storage Pool

Si el objeto se almacena en un"Grupo de almacenamiento en la nube" , se devuelven los siguientes encabezados de respuesta:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Los encabezados de respuesta brindan información sobre el estado de un objeto a medida que se mueve a un grupo de almacenamiento en la nube, opcionalmente pasa a un estado no recuperable y se restaura.

Estado del objeto	Respuesta a HeadObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un grupo de almacenamiento tradicional o que utiliza codificación de borrado	`200 OK`(No se devuelve ningún encabezado de respuesta especial).

Objeto en el grupo de almacenamiento en la nube pero que aún no ha pasado a un estado no recuperable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Hasta que el objeto pase a un estado no recuperable, el valor de `expiry-date` Está ambientado en un momento distante en el futuro. El tiempo exacto de transición no está controlado por el sistema StorageGRID .

El objeto ha pasado al estado no recuperable, pero también existe al menos una copia en la cuadrícula	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	El valor de `expiry-date` Está ambientado en un momento distante en el futuro.
	
	Nota: Si la copia en la red no está disponible (por ejemplo, un nodo de almacenamiento está inactivo), debe emitir un"Restaurar objeto" solicitud para restaurar la copia del grupo de almacenamiento en la nube antes de poder recuperar el objeto con éxito.

El objeto pasó a un estado no recuperable y no existe ninguna copia en la cuadrícula	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objeto en proceso de restauración desde un estado no recuperable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Estado del objeto	Respuesta a HeadObject

Objeto completamente restaurado al grupo de almacenamiento en la nube	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	El `expiry-date` Indica cuándo el objeto en el grupo de almacenamiento en la nube volverá a un estado no recuperable.

Objetos multiparte o segmentados en el grupo de almacenamiento en la nube

Si cargó un objeto de varias partes o si StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el grupo de almacenamiento en la nube mediante el muestreo de un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud HeadObject podría devolver incorrectamente `x-amz-restore: ongoing-request="false"` cuando algunas partes del objeto ya han sido trasladadas a un estado no recuperable o cuando algunas partes del objeto aún no han sido restauradas.

Replicación de HeadObject y entre cuadrículas

Si estas usando"federación de red" y"replicación entre redes" está habilitado para un bucket, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud HeadObject. La respuesta incluye el StorageGRID específico `x-ntap-sg-cgr-replication-status` encabezado de respuesta, que tendrá uno de los siguientes valores:

Red	Estado de replicación
Fuente	• **COMPLETADO**: La replicación fue exitosa. • **PENDIENTE**: El objeto aún no ha sido replicado. • **FALLO**: La replicación falló con un error permanente. Un usuario debe resolver el error.
Destino	**RÉPLICA**: El objeto fue replicado desde la cuadrícula de origen.

> StorageGRID no es compatible con `x-amz-replication-status` encabezamiento.

PonerObjeto

Puede utilizar la solicitud S3 PutObject para agregar un objeto a un depósito.

Resolver conflictos

Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una

operación.

Tamaño del objeto

El tamaño máximo *recomendado* para una sola operación PutObject es 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice"carga multiparte" en cambio.

El tamaño máximo *admitido* para una sola operación PutObject es 5 TiB (5.497.558.138.880 bytes).

> Si actualizó desde StorageGRID 11.6 o una versión anterior, se activará la alerta de tamaño de objeto PUT de S3 demasiado grande si intenta cargar un objeto que supere los 5 GiB. Si tiene una nueva instalación de StorageGRID 11.7 o 11.8, la alerta no se activará en este caso. Sin embargo, para alinearse con el estándar AWS S3, las futuras versiones de StorageGRID no admitirán cargas de objetos de más de 5 GiB.

Tamaño de los metadatos del usuario

Amazon S3 limita el tamaño de los metadatos definidos por el usuario dentro de cada encabezado de solicitud PUT a 2 KB. StorageGRID limita los metadatos del usuario a 24 KiB. El tamaño de los metadatos definidos por el usuario se mide tomando la suma de la cantidad de bytes en la codificación UTF-8 de cada clave y valor.

Caracteres UTF-8 en metadatos de usuario

Si una solicitud incluye valores UTF-8 (sin escapar) 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 caracteres UTF-8 escapados incluidos en el nombre de clave o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 escapados se tratan como caracteres ASCII:

- Las solicitudes PutObject, CopyObject, GetObject y HeadObject tienen éxito si los metadatos definidos por el usuario incluyen caracteres UTF-8 escapados.
- StorageGRID no devuelve el `x-amz-missing-meta` encabezado si el valor interpretado del nombre o valor de la clave incluye caracteres no imprimibles.

Límites de etiquetas de objetos

Puede agregar etiquetas a objetos nuevos cuando los cargue o puede agregarlas a objetos existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas para cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener una longitud de hasta 128 caracteres Unicode y los valores de etiqueta pueden tener una longitud de hasta 256 caracteres Unicode. La clave y los valores distinguen entre mayúsculas y minúsculas.

Propiedad de los objetos

En StorageGRID, todos los objetos son propiedad de la cuenta del propietario del depósito, incluidos los objetos creados por una cuenta que no es del propietario o un usuario anónimo.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `Cache-Control`
- `Content-Disposition`

- `Content-Encoding`

  Cuando se especifica `aws-chunked` para`Content-Encoding` StorageGRID no verifica los siguientes elementos:

  - StorageGRID no verifica la `chunk-signature` contra los datos del fragmento.
  - StorageGRID no verifica el valor que usted proporciona `x-amz-decoded-content-length` contra el objeto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  Se admite la codificación de transferencia fragmentada si `aws-chunked` También se utiliza la firma de carga útil.
- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario.

  Al especificar el par nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

  ```
  x-amz-meta-name: value
  ```

  Si desea utilizar la opción **Hora de creación definida por el usuario** como Hora de referencia para una regla ILM, debe utilizar `creation-time` como el nombre de los metadatos que registran cuándo se creó el objeto. Por ejemplo:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  El valor de `creation-time` se evalúa en segundos desde el 1 de enero de 1970.

  > Una regla ILM no puede utilizar tanto un **tiempo de creación definido por el usuario** para el tiempo de referencia como la opción de ingesta equilibrada o estricta. Se devuelve un error cuando se crea la regla ILM.

- `x-amz-tagging`
- Encabezados de solicitud de bloqueo de objetos S3
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

Si se realiza una solicitud sin estos encabezados, se utilizan las configuraciones de retención predeterminadas del depósito para calcular el modo de versión del objeto y la fecha de retención. Ver "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" .

- Encabezados de solicitud SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

  VerEncabezados de solicitud para el cifrado del lado del servidor

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

  El `x-amz-website-redirect-location` el encabezado regresa `XNotImplemented` .

Opciones de clase de almacenamiento

El `x-amz-storage-class` Se admite el encabezado de solicitud. El valor presentado para `x-amz-storage-class` afecta la forma en que StorageGRID protege los datos de los objetos durante la ingesta y no la cantidad de copias persistentes del objeto que se almacenan en el sistema StorageGRID (lo cual está determinado por ILM).

Si la regla ILM que coincide con un objeto ingerido utiliza la opción Ingesta estricta, `x-amz-storage-class` El encabezado no tiene efecto.

Los siguientes valores se pueden utilizar para `x-amz-storage-class` :

- `STANDARD`(Por defecto)
  - **Confirmación dual**: si la regla ILM especifica la opción de confirmación dual para el comportamiento de ingesta, tan pronto como se ingiere un objeto, se crea una segunda copia de ese objeto y se distribuye a un nodo de almacenamiento diferente (confirmación dual). Cuando se evalúa el ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de ubicación de la regla. De lo contrario, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y eliminar las copias provisionales iniciales.
  - **Equilibrado**: si la regla ILM especifica la opción Equilibrado y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en diferentes nodos de almacenamiento.

    Si StorageGRID puede crear inmediatamente todas las copias de objetos especificadas en la regla ILM (ubicación sincrónica), `x-amz-storage-class` El encabezado no tiene ningún efecto.

- `REDUCED_REDUNDANCY`
  - **Confirmación dual**: si la regla ILM especifica la opción de Confirmación dual para Comportamiento de ingesta, StorageGRID crea una única copia provisional a medida que se ingiere el objeto (confirmación única).
  - **Equilibrado**: si la regla ILM especifica la opción Equilibrado, StorageGRID realiza una única copia provisional solo si el sistema no puede realizar inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar la colocación sincrónica, este encabezado no tiene ningún efecto. El `REDUCED_REDUNDANCY` Esta opción se utiliza mejor cuando la regla ILM que coincide con el objeto crea una única copia replicada. En este caso se utiliza `REDUCED_REDUNDANCY` Elimina la creación y eliminación innecesarias de una copia de objeto adicional para cada operación de ingesta.

  Usando el `REDUCED_REDUNDANCY` Esta opción no se recomienda en otras circunstancias. `REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante la ingesta. Por ejemplo, podría perder datos si la copia única se almacena inicialmente en un nodo de almacenamiento que falla antes de que pueda ocurrir la evaluación de ILM.

> Tener solo una copia replicada por un período de tiempo determinado pone los datos en riesgo de pérdida permanente. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

Especificando `REDUCED_REDUNDANCY` Sólo afecta la cantidad de copias que se crean cuando se ingiere un objeto por primera vez. No afecta la cantidad de copias del objeto que se realizan cuando las políticas ILM activas evalúan el objeto y no hace que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID .

> Si está ingiriendo un objeto en un depósito con el bloqueo de objetos S3 habilitado, `REDUCED_REDUNDANCY` La opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, el `REDUCED_REDUNDANCY` La opción devuelve un error. StorageGRID siempre realizará una ingesta de confirmación dual para garantizar que se cumplan los requisitos de cumplimiento.

Encabezados de solicitud para el cifrado del lado del servidor

Puede utilizar los siguientes encabezados de solicitud para cifrar un objeto con cifrado del lado 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 administrada por StorageGRID.
  - `x-amz-server-side-encryption`

    Cuando el `x-amz-server-side-encryption` El encabezado no está incluido en la solicitud PutObject, la cuadrícula completa"configuración de cifrado de objetos almacenados" se omite de la respuesta PutObject.

- **SSE-C**: utilice estos tres encabezados si desea cifrar el objeto con una clave única que usted proporcione y administre.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256` .
  - `x-amz-server-side-encryption-customer-key`:Especifique su clave de cifrado para el nuevo objeto.

- `x-amz-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.

> Las claves de cifrado que 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 los objetos, revise las consideraciones para"utilizando cifrado del lado del servidor" .

> Si un objeto está cifrado con SSE o SSE-C, se ignoran todas las configuraciones de cifrado a nivel de bucket o de cuadrícula.

Control de versiones

Si el control de versiones está habilitado para un bucket, se creará un único `versionId` Se genera automáticamente para la versión del objeto que se está almacenando. Este `versionId` También se devuelve en la respuesta utilizando el `x-amz-version-id` encabezado de respuesta.

Si se suspende el control de versiones, la versión del objeto se almacena con un valor nulo. `versionId` y si ya existe una versión nula, se sobrescribirá.

Cálculos de firma para el encabezado de autorización

Al utilizar el `Authorization` encabezado para autenticar solicitudes, StorageGRID se diferencia de AWS de las siguientes maneras:

- StorageGRID no requiere `host` encabezados que se incluirán dentro `CanonicalHeaders` .
- StorageGRID no requiere `Content-Type` para ser incluido dentro `CanonicalHeaders` .
- StorageGRID no requiere `x-amz-*` encabezados que se incluirán dentro `CanonicalHeaders` .

> Como práctica recomendada general, incluya siempre estos encabezados dentro `CanonicalHeaders` para garantizar que se verifiquen; sin embargo, si excluye estos encabezados, StorageGRID no devuelve un error.

Para más detalles, consulte "Cálculos de firma para el encabezado de autorización: transferencia de carga útil en un solo fragmento (AWS Signature versión 4)" .

Información relacionada

- "Administrar objetos con ILM"
- "Referencia de la API de Amazon Simple Storage Service: PutObject"

Restaurar objeto

Puede utilizar la solicitud S3 RestoreObject para restaurar un objeto almacenado en un grupo de almacenamiento en la nube.

Tipo de solicitud admitido

StorageGRID solo admite solicitudes RestoreObject para restaurar un objeto. No es compatible con el `SELECT` tipo de restauración. Seleccione solicitudes de devolución `XNotImplemented` .

Control de versiones

Opcionalmente, especifique `versionId` para restaurar una versión específica de un objeto en un depósito versionado. Si no lo especifica `versionId` , se restaura la versión más reciente del objeto

Comportamiento de RestoreObject en objetos del grupo de almacenamiento en la nube

Si un objeto ha sido almacenado en un"Grupo de almacenamiento en la nube" Una solicitud RestoreObject tiene el siguiente comportamiento, según el estado del objeto. Ver"Objeto principal" Para más detalles.

> Si un objeto está almacenado en un grupo de almacenamiento en la nube y también existen una o más copias del objeto en la red, no es necesario restaurar el objeto emitiendo una solicitud RestoreObject. En cambio, la copia local se puede recuperar directamente, mediante una solicitud GetObject.

Estado del objeto	Comportamiento de RestoreObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, o el objeto no está en un grupo de almacenamiento en la nube	`403 Forbidden` , `InvalidObjectState`
Objeto en el grupo de almacenamiento en la nube pero que aún no ha pasado a un estado no recuperable	`200 OK`No se realizan cambios **Nota**: Antes de que un objeto pase a un estado no recuperable, no se puede cambiar su `expiry-date` .
Objeto en transición a un estado no recuperable	`202 Accepted`Restaura una copia recuperable del objeto en el grupo de almacenamiento en la nube durante la cantidad de días especificada en el cuerpo de la solicitud. Al final de este período, el objeto vuelve a un estado no recuperable. Opcionalmente, utilice el `Tier` Elemento de solicitud para determinar cuánto tiempo tardará en finalizar el trabajo de restauración(`Expedited` , `Standard` , o `Bulk`). Si no lo especifica `Tier` , el `Standard` Se utiliza el nivel. **Importante**: Si un objeto se ha transferido a S3 Glacier Deep Archive o el grupo de almacenamiento en la nube usa almacenamiento de blobs de Azure, no podrá restaurarlo mediante 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 desde un estado no recuperable	`409 Conflict` , `RestoreAlreadyInProgress`

Estado del objeto	Comportamiento de RestoreObject
Objeto completamente restaurado al grupo de almacenamiento en la nube	`200 OK` **Nota:** Si un objeto se ha restaurado a un estado recuperable, puede cambiar su `expiry-date` volviendo a emitir la solicitud RestoreObject con un nuevo valor para `Days` . La fecha de restauración se actualiza en relación con el momento de la solicitud.

Seleccionar contenido del objeto

Puede utilizar la solicitud S3 SelectObjectContent para filtrar el contenido de un objeto S3 según una declaración SQL simple.

Para más información véase "Referencia de la API de Amazon Simple Storage Service: SelectObjectContent" .

Antes de empezar

- La cuenta de inquilino tiene el permiso S3 Select.
- Tienes `s3:GetObject` Permiso para el objeto que desea consultar.
- El objeto que desea consultar debe estar en uno de los siguientes formatos:
  - **CSV**. Se puede utilizar tal cual o comprimido en archivos GZIP o BZIP2.
  - **Parquet**. Requisitos adicionales para los objetos Parquet:
    - S3 Select solo admite la compresión en columnas mediante GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos Parquet.
    - S3 Select no admite la salida Parquet. Debe especificar el formato de salida como CSV o JSON.
    - El tamaño máximo del grupo de filas sin comprimir es 512 MB.
    - Debe utilizar los tipos de datos especificados en el esquema del objeto.
    - No se pueden utilizar los tipos lógicos INTERVAL, JSON, LIST, TIME o UUID.
- Su expresión SQL tiene una longitud máxima de 256 KB.
- Cualquier registro en la entrada o en los resultados tiene una longitud máxima de 1 MiB.

Ejemplo de sintaxis de solicitud CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Ejemplo de sintaxis de solicitud de Parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Ejemplo de consulta SQL

Esta consulta obtiene el nombre del estado, las poblaciones de 2010, las poblaciones estimadas de 2015 y el porcentaje de cambio de los datos del censo de EE. UU. Los registros del archivo que no son estados se ignoran.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Las primeras líneas del archivo a consultar, `SUB-EST2020_ALL.csv` , luce así:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Ejemplo de uso de AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Las primeras líneas del archivo de salida, `changes.csv` , luce así:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Ejemplo de uso de AWS-CLI (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

Las primeras líneas del archivo de salida, changes.csv, se ven así:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operaciones para cargas multiparte

Operaciones para cargas multiparte

Esta sección describe cómo StorageGRID admite operaciones para cargas multiparte.

Las siguientes condiciones y notas se aplican a todas las operaciones de carga multiparte:

- No debe exceder las 1000 cargas multiparte simultáneas en un solo depósito porque los resultados de las consultas ListMultipartUploads para ese depósito podrían devolver resultados incompletos.
- StorageGRID aplica límites de tamaño de AWS para partes multiparte. Los clientes de S3 deben seguir estas pautas:
  - Cada parte de una carga multiparte debe tener entre 5 MiB (5.242.880 bytes) y 5 GiB (5.368.709.120 bytes).
  - La última parte puede ser menor a 5 MiB (5.242.880 bytes).
  - En general, los tamaños de las piezas deben ser lo más grandes posible. Por ejemplo, utilice tamaños de piezas de 5 GiB para un objeto de 100 GiB. Dado que cada parte se considera un objeto único, el uso de partes de gran tamaño reduce la sobrecarga de metadatos de StorageGRID .
  - Para objetos más pequeños que 5 GiB, considere usar una carga que no sea multiparte.
- ILM se evalúa para cada parte de un objeto multiparte a medida que se ingiere y para el objeto como un todo cuando se completa la carga multiparte, si la regla ILM usa Equilibrado o Estricto."opción de ingesta" . Debes tener en cuenta cómo esto afecta la colocación de objetos y piezas:
  - Si ILM cambia mientras una carga multiparte de S3 está en progreso, es posible que algunas partes del objeto no cumplan con los requisitos de ILM actuales cuando se complete la carga multiparte. Cualquier pieza que no esté colocada correctamente se pone en cola para la reevaluación de ILM y se mueve a la ubicación correcta más tarde.

- Al evaluar ILM para una pieza, StorageGRID filtra el tamaño de la pieza, no el tamaño del objeto. Esto significa que partes de un objeto pueden almacenarse en ubicaciones que no cumplen los requisitos de ILM para el objeto en su totalidad. 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, cada parte de 1 GB de una carga multiparte de 10 partes se almacena en DC2 en la ingesta. Sin embargo, cuando se evalúa ILM para el objeto como un todo, todas las partes del objeto se mueven a DC1.

- Todas las operaciones de carga multiparte son compatibles con StorageGRID"valores de consistencia" .
- Cuando se ingiere un objeto mediante una carga multiparte, el"umbral de segmentación de objetos (1 GiB)" no se aplica
- Según sea necesario, puede utilizar"cifrado del lado del servidor" con cargas multiparte. Para utilizar SSE (cifrado del lado del servidor con claves administradas por StorageGRID), incluya el `x-amz-server-side-encryption` encabezado de solicitud únicamente en la solicitud CreateMultipartUpload. Para utilizar SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente), debe especificar los mismos tres encabezados de solicitud de clave de cifrado en la solicitud CreateMultipartUpload y en cada solicitud UploadPart posterior.

Operación	Implementación
AbortarMultipartUpload	Implementado con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.
Carga completa de varias partes	Ver"Carga completa de varias partes"
Crear carga de varias partes (anteriormente llamado Iniciar carga multiparte)	Ver"Crear carga de varias partes"
Lista de cargas de varias partes	Ver"Lista de cargas de varias partes"
Lista de partes	Implementado con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.
Subir parte	Ver"Subir parte"
Subir copia parcial	Ver"Subir copia parcial"

Carga completa de varias partes

La operación CompleteMultipartUpload completa una carga multiparte de un objeto ensamblando las partes cargadas previamente.

> StorageGRID admite valores no consecutivos en orden ascendente para el `partNumber` parámetro de solicitud con CompleteMultipartUpload. El parámetro puede comenzar con cualquier valor.

Resolver conflictos

Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  El `x-amz-storage-class` El encabezado afecta la cantidad de copias de objetos que crea StorageGRID si la regla ILM correspondiente especifica"Opción de doble confirmación o ingesta equilibrada" .

- `STANDARD`

  (Predeterminado) Especifica una operación de ingesta de confirmación dual cuando la regla ILM usa la opción Confirmación dual o cuando la opción Equilibrada recurre a la creación de copias provisionales.

- `REDUCED_REDUNDANCY`

  Especifica una operación de ingesta de confirmación única cuando la regla ILM usa la opción de confirmación dual o cuando la opción Equilibrada recurre a la creación de copias provisionales.

  > Si está ingiriendo un objeto en un depósito con el bloqueo de objetos S3 habilitado, `REDUCED_REDUNDANCY` La opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, el `REDUCED_REDUNDANCY` La opción devuelve un error. StorageGRID siempre realizará una ingesta de confirmación dual para garantizar que se cumplan los requisitos de cumplimiento.

> Si una carga de varias partes no se completa dentro de los 15 días, la operación se marca como inactiva y todos los datos asociados se eliminan del sistema.

> El `ETag` El valor devuelto no es una suma MD5 de los datos, sino que sigue la implementación de la API de Amazon S3 de la `ETag` valor para objetos multiparte.

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Control de versiones

Esta operación completa una carga de varias partes. Si el control de versiones está habilitado para un bucket, la versión del objeto se crea después de completar la carga de varias partes.

Si el control de versiones está habilitado para un bucket, se creará un único `versionId` Se genera automáticamente para la versión del objeto que se está almacenando. Este `versionId` También se devuelve en la respuesta utilizando 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 el control de versiones está habilitado para un bucket, completar una carga multiparte siempre crea una nueva versión, incluso si hay cargas multiparte simultáneas completadas en la misma clave de objeto. Cuando el control de versiones no está habilitado para un bucket, es posible iniciar una carga multiparte y luego iniciar y completar primero otra carga multiparte en la misma clave de objeto. En los depósitos sin versiones, la carga multiparte que se completa en último lugar tiene prioridad.

Error de replicación, notificación o notificación de metadatos

Si el depósito donde se produce la carga multiparte está configurado para un servicio de plataforma, la carga multiparte se realiza correctamente incluso si falla la acción de replicación o notificación asociada.

Un inquilino puede activar la replicación o notificación fallida actualizando los metadatos o las etiquetas del objeto. Un inquilino puede volver a enviar los valores existentes para evitar realizar cambios no deseados.

Consulte "Solucionar problemas de servicios de la plataforma" .

Crear carga de varias partes

La operación CreateMultipartUpload (anteriormente denominada Iniciar carga multiparte) inicia una carga multiparte para un objeto y devuelve un ID de carga.

El `x-amz-storage-class` Se admite el encabezado de solicitud. El valor presentado para `x-amz-storage-class` afecta la forma en que StorageGRID protege los datos de los objetos durante la ingesta y no la cantidad de copias persistentes del objeto que se almacenan en el sistema StorageGRID (lo cual está determinado por ILM).

Si la regla ILM que coincide con un objeto ingerido utiliza el método Estricto"opción de ingesta" , el `x-amz-storage-class` El encabezado no tiene ningún efecto.

Los siguientes valores se pueden utilizar para `x-amz-storage-class` :

- `STANDARD`(Por defecto)
  - **Confirmación dual**: si la regla ILM especifica la opción de ingesta de confirmación dual, tan pronto como se ingiere un objeto, se crea una segunda copia de ese objeto y se distribuye a un nodo de almacenamiento diferente (confirmación dual). Cuando se evalúa el ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de ubicación de la regla. De lo contrario, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y eliminar las copias provisionales iniciales.
  - **Equilibrado**: si la regla ILM especifica la opción Equilibrado y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en diferentes nodos de almacenamiento.

    Si StorageGRID puede crear inmediatamente todas las copias de objetos especificadas en la regla ILM (ubicación sincrónica), `x-amz-storage-class` El encabezado no tiene ningún efecto.

- `REDUCED_REDUNDANCY`
  - **Confirmación dual**: si la regla ILM especifica la opción de confirmación dual, StorageGRID crea una única copia provisional a medida que se ingiere el objeto (confirmación única).
  - **Equilibrado**: si la regla ILM especifica la opción Equilibrado, StorageGRID realiza una única copia provisional solo si el sistema no puede realizar inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar la colocación sincrónica, este encabezado no tiene ningún efecto. El `REDUCED_REDUNDANCY` Esta opción se utiliza mejor cuando la regla ILM que coincide con el objeto crea una única copia replicada. En este caso se utiliza `REDUCED_REDUNDANCY` Elimina la creación y eliminación innecesarias de una copia de objeto adicional para cada operación de ingesta.

  Usando el `REDUCED_REDUNDANCY` Esta opción no se recomienda en otras circunstancias. `REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante la ingesta. Por ejemplo, podría perder datos si la copia única se almacena inicialmente en un nodo de almacenamiento que falla antes de que pueda ocurrir la evaluación de ILM.

> Tener solo una copia replicada por un período de tiempo determinado pone los datos en riesgo de pérdida permanente. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

Especificando `REDUCED_REDUNDANCY` Sólo afecta la cantidad de copias que se crean cuando se ingiere un objeto por primera vez. No afecta la cantidad de copias del objeto que se realizan cuando las políticas ILM activas evalúan el objeto y no hace que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID .

> Si está ingiriendo un objeto en un depósito con el bloqueo de objetos S3 habilitado, `REDUCED_REDUNDANCY` La opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, el `REDUCED_REDUNDANCY` La opción devuelve un error. StorageGRID siempre realizará una ingesta de confirmación dual para garantizar que se cumplan los requisitos de cumplimiento.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `Content-Type`
- `x-amz-checksum-algorithm`

  Actualmente, solo el valor SHA256 para `x-amz-checksum-algorithm` es compatible.

- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario

  Al especificar el par nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

  ```
  x-amz-meta-_name_: `value`
  ```

  Si desea utilizar la opción **Hora de creación definida por el usuario** como Hora de referencia para una regla ILM, debe utilizar `creation-time` como el nombre de los metadatos que registran cuándo se creó el objeto. Por ejemplo:

```
x-amz-meta-creation-time: 1443399726
```

El valor de `creation-time` se evalúa en segundos desde el 1 de enero de 1970.

> Añadiendo `creation-time` ya que no se permiten metadatos definidos por el usuario si está agregando un objeto a un depósito que tiene habilitado el Cumplimiento heredado. Se devolverá un error.

- Encabezados de solicitud de bloqueo de objetos S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si se realiza una solicitud sin estos encabezados, se utilizan las configuraciones de retención predeterminadas del depósito para calcular la fecha de retención de la versión del objeto.

  "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"

- Encabezados de solicitud SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Encabezados de solicitud para el cifrado del lado del servidor

> Para obtener información sobre cómo StorageGRID maneja los caracteres UTF-8, consulte"PonerObjeto" .

Encabezados de solicitud para el cifrado del lado del servidor

Puede utilizar los siguientes encabezados de solicitud para cifrar un objeto multiparte con cifrado del lado del servidor. Las opciones SSE y SSE-C son mutuamente excluyentes.

- **SSE**: utilice el siguiente encabezado en la solicitud CreateMultipartUpload si desea cifrar el objeto con una clave única administrada por StorageGRID. No especifique este encabezado en ninguna de las solicitudes UploadPart.
  - `x-amz-server-side-encryption`
- **SSE-C**: utilice estos tres encabezados en la solicitud CreateMultipartUpload (y en cada solicitud UploadPart posterior) si desea cifrar el objeto con una clave única que usted proporcione y administre.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256` .
  - `x-amz-server-side-encryption-customer-key`:Especifique su clave de cifrado para el nuevo objeto.

- `x-amz-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.

> Las claves de cifrado que 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 los objetos, revise las consideraciones para"utilizando cifrado del lado del servidor" .

Encabezados de solicitud no admitidos

El siguiente encabezado de solicitud no es compatible:

- `x-amz-website-redirect-location`

  El `x-amz-website-redirect-location` el encabezado regresa `XNotImplemented` .

Control de versiones

La carga multiparte consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

Lista de cargas de varias partes

La operación ListMultipartUploads enumera las cargas multiparte en curso para un depósito.

Se admiten los siguientes parámetros de solicitud:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Control de versiones

La carga multiparte consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

Subir parte

La operación UploadPart carga una parte en una carga multiparte para un objeto.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Encabezados de solicitud para el cifrado del lado del servidor

Si especificó el cifrado SSE-C para la solicitud CreateMultipartUpload, también debe incluir los siguientes encabezados de solicitud en cada solicitud UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256` .
- `x-amz-server-side-encryption-customer-key`:Especifique la misma clave de cifrado que proporcionó en la solicitud CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`:Especifique el mismo resumen MD5 que proporcionó en la solicitud CreateMultipartUpload.

> 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 los objetos, revise las consideraciones en"Utilice cifrado del lado del servidor" .

Si especificó una suma de comprobación SHA-256 durante la solicitud CreateMultipartUpload, también debe incluir el siguiente encabezado de solicitud en cada solicitud UploadPart:

- `x-amz-checksum-sha256`:Especifique la suma de comprobación SHA-256 para esta parte.

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Control de versiones

La carga multiparte consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

Subir copia parcial

La operación UploadPartCopy carga una parte de un objeto copiando datos de un objeto existente como fuente de datos.

La operación UploadPartCopy se implementa con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.

Esta solicitud lee y escribe los datos del objeto especificados en `x-amz-copy-source-range` dentro del

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`

Encabezados de solicitud para el cifrado del lado del servidor

Si especificó el cifrado SSE-C para la solicitud CreateMultipartUpload, también debe incluir los siguientes encabezados de solicitud en cada solicitud UploadPartCopy:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256` .
- `x-amz-server-side-encryption-customer-key`:Especifique la misma clave de cifrado que proporcionó en la solicitud CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`:Especifique el mismo resumen MD5 que proporcionó en la solicitud CreateMultipartUpload.

Si el objeto de origen está cifrado mediante una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud UploadPartCopy, para que el objeto pueda descifrarse y luego copiarse:

- `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 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 los objetos, revise las consideraciones en"Utilice cifrado del lado del servidor" .

Control de versiones

La carga multiparte consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

Respuestas de error

El sistema StorageGRID admite todas las respuestas de error de API REST S3 estándar que corresponden. Además, la implementación de StorageGRID agrega varias respuestas personalizadas.

Códigos de error de la API de S3 compatibles

Nombre	Estado HTTP
Acceso denegado	403 Prohibido
Mal resumen	400 Solicitud incorrecta
El cubo ya existe	409 Conflict
Cubo no vacío	409 Conflict
Cuerpo incompleto	400 Solicitud incorrecta
Error interno	500 Error interno del servidor
ID de clave de acceso no válido	403 Prohibido
Argumento inválido	400 Solicitud incorrecta
Nombre de cubo inválido	400 Solicitud incorrecta
Estado del cubo no válido	409 Conflict
Resumen inválido	400 Solicitud incorrecta
Error de algoritmo de cifrado no válido	400 Solicitud incorrecta
Parte inválida	400 Solicitud incorrecta
Orden de pieza no válida	400 Solicitud incorrecta
Rango inválido	416 Rango solicitado no satisfacible
Solicitud inválida	400 Solicitud incorrecta
Clase de almacenamiento no válida	400 Solicitud incorrecta
Etiqueta inválida	400 Solicitud incorrecta
URI no válido	400 Solicitud incorrecta
Clave demasiado larga	400 Solicitud incorrecta
XML malformado	400 Solicitud incorrecta

Nombre	Estado HTTP
Metadatos demasiado grandes	400 Solicitud incorrecta
Método no permitido	Método 405 no permitido
Longitud de contenido faltante	411 Longitud requerida
Error de cuerpo de solicitud faltante	400 Solicitud incorrecta
Encabezado de seguridad faltante	400 Solicitud incorrecta
NoSuchBucket	404 No encontrado
NoSuchKey	404 No encontrado
NoSuchUpload	404 No encontrado
No implementado	501 No implementado
Política de no usar este cubo	404 No encontrado
Error de configuración de bloqueo de objeto no encontrado	404 No encontrado
Precondición fallida	412 Precondición fallida
RequestTimeTooSkewed	403 Prohibido
Servicio No Disponible	503 Servicio no disponible
La firma no coincide	403 Prohibido
Demasiados cubos	400 Solicitud incorrecta
La clave de usuario debe especificarse	400 Solicitud incorrecta

Códigos de error personalizados de StorageGRID

Nombre	Descripción	Estado HTTP
Ciclo de vida de XBucket no permitido	La configuración del ciclo de vida del bucket no está permitida en un bucket compatible heredado	400 Solicitud incorrecta

Nombre	Descripción	Estado HTTP
Excepción de análisis de política de XBucket	No se pudo analizar el JSON de la política de depósito recibida.	400 Solicitud incorrecta
Conflicto de cumplimiento X	Operación denegada debido a configuraciones de cumplimiento heredadas.	403 Prohibido
XComplianceReducedRedundancyForbidden	No se permite redundancia reducida en el bucket compatible heredado	400 Solicitud incorrecta
Longitud máxima de la política de cubos X excedida	Su póliza excede la longitud máxima permitida de la póliza.	400 Solicitud incorrecta
XMissingInternalRequestHeader	Falta un encabezado de una solicitud interna.	400 Solicitud incorrecta
Cumplimiento de XNoSuchBucket	El depósito especificado no tiene habilitada la conformidad heredada.	404 No encontrado
XNo aceptable	La solicitud contiene uno o más encabezados de aceptación que no se pudieron satisfacer.	406 No aceptable
XNoImplementado	La solicitud que proporcionó implica una funcionalidad que no está implementada.	501 No implementado

Operaciones personalizadas de StorageGRID

Operaciones personalizadas de StorageGRID

El sistema StorageGRID admite operaciones personalizadas que se agregan a la API REST de S3.

La siguiente tabla enumera las operaciones personalizadas compatibles con StorageGRID.

Operación	Descripción
"Obtener consistencia del bucket"	Devuelve la consistencia que se aplica a un depósito en particular.
"Consistencia del depósito PUT"	Establece la consistencia aplicada a un depósito en particular.
"GET Hora del último acceso al bucket"	Devuelve si las actualizaciones del último tiempo de acceso están habilitadas o deshabilitadas para un depósito en particular.

Operación	Descripción
"Hora del último acceso al depósito PUT"	Le permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para un depósito en particular.
"Configuración de notificación de metadatos del depósito DELETE"	Elimina el XML de configuración de notificación de metadatos asociado con un depósito en particular.
"Configuración de notificación de metadatos del depósito GET"	Devuelve el XML de configuración de notificación de metadatos asociado con un depósito en particular.
"Configuración de notificación de metadatos del depósito PUT"	Configura el servicio de notificación de metadatos para un bucket.
"Uso de almacenamiento GET"	Le indica la cantidad total de almacenamiento en uso por una cuenta y para cada depósito asociado con la cuenta.
"Obsoleto: CreateBucket con configuración de cumplimiento"	Obsoleto y no compatible: ya no es posible crear nuevos depósitos con Cumplimiento habilitado.
"Obsoleto: cumplimiento del contenedor GET"	Obsoleto pero compatible: devuelve las configuraciones de cumplimiento actualmente vigentes para un bucket compatible heredado existente.
"Obsoleto: Cumplimiento del contenedor PUT"	Obsoleto pero compatible: le permite modificar la configuración de cumplimiento para un depósito compatible heredado existente.

Obtener consistencia del bucket

La solicitud de consistencia de depósito GET le permite determinar la consistencia que se aplica a un depósito en particular.

La consistencia predeterminada está configurada para garantizar la lectura después de la escritura para los objetos recién creados.

Debe tener el permiso s3:GetBucketConsistency o ser la cuenta root para completar esta operación.

Ejemplo de solicitud

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

Respuesta

En el XML de respuesta, `<Consistency>` devolverá uno de los siguientes valores:

Consistencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o la solicitud fallará.
fuerte-global	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.
sitio fuerte	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes dentro de un sitio.
lectura después de nueva escritura	(Predeterminado) Proporciona consistencia de lectura después de escritura para objetos nuevos y consistencia eventual para actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Recomendado para la mayoría de los casos.
disponible	Proporciona consistencia eventual tanto para objetos nuevos como para actualizaciones de objetos. Para los depósitos S3, úselo solo cuando sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD o GET en claves que no existen). No compatible con depósitos S3 FabricPool .

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

"Valores de consistencia"

Consistencia del depósito PUT

La solicitud de consistencia de PUT Bucket le permite especificar la consistencia que se aplicará a las operaciones realizadas en un bucket.

La consistencia predeterminada está configurada para garantizar la lectura después de la escritura para los objetos recién creados.

Antes de empezar

Debe tener el permiso s3:PutBucketConsistency o ser la cuenta root para completar esta operación.

Pedido

El `x-ntap-sg-consistency` El parámetro debe contener uno de los siguientes valores:

Consistencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o la solicitud fallará.
fuerte-global	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.
sitio fuerte	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes dentro de un sitio.
lectura después de nueva escritura	(Predeterminado) Proporciona consistencia de lectura después de escritura para objetos nuevos y consistencia eventual para actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Recomendado para la mayoría de los casos.
disponible	Proporciona consistencia eventual tanto para objetos nuevos como para actualizaciones de objetos. Para los depósitos S3, úselo solo cuando sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD o GET en claves que no existen). No compatible con depósitos S3 FabricPool .

Nota: En general, debe utilizar la consistencia "Lectura después de nueva 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 la consistencia para cada solicitud de API. Establezca la consistencia a nivel de depósito sólo como último recurso.

Ejemplo de solicitud

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Información relacionada

"Valores de consistencia"

GET Hora del último acceso al bucket

La solicitud de hora de último acceso al bucket GET le permite determinar si las actualizaciones de hora de último acceso están habilitadas o deshabilitadas para buckets individuales.

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

Ejemplo de solicitud

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

Ejemplo de respuesta

Este ejemplo muestra que las actualizaciones del último tiempo de acceso están habilitadas para el depósito.

```
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>
```

Hora del último acceso al depósito PUT

La solicitud de hora de último acceso al depósito PUT le permite habilitar o deshabilitar actualizaciones de hora de último acceso para depósitos individuales. Deshabilitar las actualizaciones del último tiempo de acceso mejora el rendimiento y es la configuración predeterminada para todos los depósitos creados con la versión 10.3.0 o posterior.

Debe tener el permiso s3:PutBucketLastAccessTime para un bucket, o ser root de la cuenta, para completar esta operación.

> A partir de la versión 10.3 de StorageGRID , las actualizaciones de la hora del último acceso están deshabilitadas de manera predeterminada para todos los depósitos nuevos. Si tiene depósitos que se crearon utilizando una versión anterior de StorageGRID y desea que coincidan con el nuevo comportamiento predeterminado, debe deshabilitar explícitamente las actualizaciones de la última hora de acceso para cada uno de esos depósitos anteriores. Puede habilitar o deshabilitar las actualizaciones de la última hora de acceso mediante la solicitud de última hora de acceso del depósito PUT o desde la página de detalles de un depósito en el Administrador de inquilinos. Ver "Habilitar o deshabilitar las actualizaciones de la última hora de acceso" .

Si las actualizaciones del último tiempo de acceso están deshabilitadas para un depósito, se aplica el siguiente comportamiento a las operaciones en el depósito:

- Las solicitudes GetObject, GetObjectAcl, GetObjectTagging y HeadObject no actualizan la hora del último acceso. El objeto no se agrega a las colas para la evaluación de la gestión del ciclo de vida de la información (ILM).
- Las solicitudes CopyObject y PutObjectTagging que actualizan solo los metadatos también actualizan la hora del último acceso. El objeto se agrega a las colas para la evaluación de ILM.
- Si las actualizaciones de la hora del último acceso están deshabilitadas para el depósito de origen, las solicitudes CopyObject no actualizan la hora del último acceso para el depósito de origen. El objeto que se copió no se agrega a las colas para la evaluación de ILM para el depósito de origen. Sin embargo, para el destino, las solicitudes CopyObject siempre actualizan la hora del último acceso. La copia del objeto se agrega a las colas para la evaluación de ILM.
- CompleteMultipartUpload solicita actualizar la hora del último acceso. El objeto completado se agrega a las colas para la evaluación de ILM.

Solicitar ejemplos

Este ejemplo habilita el último tiempo de acceso para un bucket.

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

Este ejemplo deshabilita el tiempo del último acceso para un depósito.

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

Configuración de notificación de metadatos del depósito DELETE

La solicitud de configuración de notificación de metadatos de depósito DELETE le permite deshabilitar el servicio de integración de búsqueda para depósitos individuales eliminando el XML de configuración.

Debe tener el permiso s3:DeleteBucketMetadataNotification para un bucket, o ser raíz de la cuenta, para completar esta operación.

Ejemplo de solicitud

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

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

Configuración de notificación de metadatos del depósito GET

La solicitud de configuración de notificación de metadatos de bucket GET le permite recuperar el XML de configuración utilizado para configurar la integración de búsqueda para buckets individuales.

Debe tener el permiso s3:GetBucketMetadataNotification o ser la cuenta root para completar esta operación.

Ejemplo de solicitud

Esta solicitud recupera la configuración de notificación de metadatos para el depósito denominado `bucket` .

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

Respuesta

El cuerpo de la respuesta incluye la configuración de notificación de metadatos para el depósito. La configuración de notificación de metadatos le permite determinar cómo se configura el depósito para la integración de búsqueda. Es decir, permite determinar qué objetos están indexados y a qué puntos finales se envían sus metadatos de 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 más reglas. Cada regla especifica los objetos a los que se aplica y el destino donde StorageGRID debe enviar los metadatos de los objetos. Los destinos deben especificarse utilizando el URN de un punto final de StorageGRID .

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

Nombre	Descripción	Requerido
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para que coincida con todos los objetos, especifique un prefijo vacío. Incluido en el elemento Regla.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Regla.	Sí
Urna	URN del destino donde se envían los metadatos del objeto. Debe ser la URN de un punto final de StorageGRID con las siguientes propiedades: • `es`Debe ser el tercer elemento. • La URN debe terminar con el índice y tipo donde se almacenan los metadatos, en el formato `domain-name/myindex/mytype` . Los puntos finales se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Toman la siguiente forma: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe configurarse antes de enviar el XML de configuración; de lo contrario, la configuración fallará con un error 404. La urna está incluida en el elemento Destino.	Sí

Ejemplo de respuesta

El XML incluido entre el `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` Las etiquetas muestran cómo se configura la integración con un punto final de integración de búsqueda para el depósito. En este ejemplo, los metadatos del objeto se envían a un índice de Elasticsearch llamado `current` y tipo nombrado `2017` que está alojado 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

"Utilice una cuenta de inquilino"

Configuración de notificación de metadatos del depósito PUT

La solicitud de configuración de notificación de metadatos de PUT Bucket le permite habilitar el servicio de integración de búsqueda para buckets individuales. El XML de configuración de notificación de metadatos que proporciona en el cuerpo de la solicitud especifica los objetos cuyos metadatos se envían al índice de búsqueda de destino.

Debe tener el permiso s3:PutBucketMetadataNotification para un bucket, o ser raíz de la cuenta, para completar esta operación.

Pedido

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 más reglas. Cada regla especifica los objetos a los que se aplica y el destino donde StorageGRID debe enviar los metadatos de los objetos.

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, podría enviar metadatos para objetos con el prefijo `/images` a un destino y 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 los objetos con el prefijo `test` y una segunda regla para los objetos con el prefijo `test2` No se permitiría.

Los destinos deben especificarse utilizando el URN de un punto final de StorageGRID . El punto final debe existir cuando se envía la configuración de notificación de metadatos, o la solicitud falla como resultado. `400`

`Bad Request` El mensaje de error dice: `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>
```

La tabla describe los elementos del XML de configuración de notificación de metadatos.

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

Nombre	Descripción	Requerido
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para que coincida con todos los objetos, especifique un prefijo vacío. Incluido en el elemento Regla.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Regla.	Sí
Urna	URN del destino donde se envían los metadatos del objeto. Debe ser la URN de un punto final de StorageGRID con las siguientes propiedades: • `es`Debe ser el tercer elemento. • La URN debe terminar con el índice y tipo donde se almacenan los metadatos, en el formato `domain-name/myindex/mytype` . Los puntos finales se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Toman la siguiente forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe configurarse antes de enviar el XML de configuración; de lo contrario, la configuración fallará con un error 404. La urna está incluida en el elemento Destino.	Sí

Solicitar ejemplos

Este ejemplo muestra cómo habilitar la integración de búsqueda para un depósito. En este ejemplo, los metadatos de todos los objetos se envían al mismo destino.

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

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

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

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

JSON generado por el servicio de integración de búsqueda

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

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

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

Metadatos de objetos incluidos en las notificaciones de metadatos

La tabla enumera todos los campos que se incluyen en el documento JSON que se envía al punto final de destino cuando se habilita la integración de búsqueda.

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

Tipo	Nombre del artículo	Descripción
Información de depósito y objeto	balde	Nombre del bucket
Información de depósito y objeto	llave	Nombre de la clave del objeto
Información de depósito y objeto	ID de versión	Versión del objeto, para objetos en depósitos versionados
Información de depósito y objeto	región	Región del cubo, por ejemplo `us-east-1`
Metadatos del sistema	tamaño	Tamaño del objeto (en bytes) tal como lo ve un cliente HTTP
Metadatos del sistema	md5	Hash de objeto
Metadatos del usuario	metadatos *`key:value`*	Todos los metadatos de usuario para el objeto, como pares clave-valor

Tipo	Nombre del artículo	Descripción
Etiquetas	etiquetas *key:value*	Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor

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

Información relacionada

"Utilice una cuenta de inquilino"

Solicitud de uso de almacenamiento GET

La solicitud de uso de almacenamiento GET le indica la cantidad total de almacenamiento en uso por una cuenta y para cada depósito asociado con la cuenta.

La cantidad de almacenamiento utilizada por una cuenta y sus depósitos se puede obtener mediante una solicitud ListBuckets modificada con el `x-ntap-sg-usage` parámetro de consulta. El uso del almacenamiento del bucket se rastrea por separado de las solicitudes PUT y DELETE procesadas por el sistema. Puede haber algún retraso antes de que los valores de uso coincidan con los valores esperados en función del procesamiento de las solicitudes, en particular si el sistema está bajo una carga pesada.

De forma predeterminada, StorageGRID intenta recuperar información de uso utilizando una consistencia global fuerte. Si no se puede lograr una consistencia global fuerte, StorageGRID intenta recuperar la información de uso con una consistencia de sitio fuerte.

Debe tener el permiso s3:ListAllMyBuckets o ser la cuenta root para completar esta operación.

Ejemplo de solicitud

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

Ejemplo de respuesta

Este ejemplo muestra una cuenta que tiene cuatro objetos y 12 bytes de datos en dos grupos. Cada contenedor 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>
```

Control de versiones

Cada versión de objeto almacenada contribuirá a la `ObjectCount` y `DataBytes` valores en la respuesta. Los marcadores de eliminación no se agregan a la `ObjectCount` total.

Información relacionada

"Valores de consistencia"

Solicitudes de depósito obsoletas para cumplimiento heredado

Solicitudes de depósito obsoletas para cumplimiento heredado

Es posible que necesite usar la API REST S3 de StorageGRID para administrar los depósitos que se crearon mediante la función de cumplimiento heredada.

Función de cumplimiento obsoleta

La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID está obsoleta y ha sido reemplazada por S3 Object Lock.

Si anteriormente habilitó la configuración de Cumplimiento global, la configuración de Bloqueo de objetos S3 global está habilitada en StorageGRID 11.6. Ya no es posible crear nuevos buckets con Cumplimiento habilitado; sin embargo, según sea necesario, puede usar la API REST de StorageGRID S3 para administrar cualquier bucket Cumplimiento heredado existente.

- "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"
- "Administrar objetos con ILM"
- "Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"

Solicitudes de cumplimiento obsoletas:

- "Obsoleto: modificaciones de la solicitud PUT Bucket para cumplimiento"

  El elemento XML SGCompliance está obsoleto. Anteriormente, podía incluir este elemento personalizado StorageGRID en el cuerpo de la solicitud XML opcional de las solicitudes PUT Bucket para crear un bucket compatible.

- "Obsoleto: cumplimiento del contenedor GET"

  La solicitud de cumplimiento de GET Bucket está obsoleta. Sin embargo, puede seguir usando esta solicitud para determinar las configuraciones de cumplimiento actualmente vigentes para un bucket compatible heredado existente.

- "Obsoleto: cumplimiento del contenedor PUT"

  La solicitud de cumplimiento de PUT Bucket está obsoleta. Sin embargo, puede seguir usando esta solicitud para modificar la configuración de cumplimiento de un depósito compatible heredado existente. Por ejemplo, puede colocar un depósito existente en retención legal o aumentar su período de retención.

Obsoleto: Modificaciones de la solicitud CreateBucket para cumplimiento

El elemento XML SGCompliance está obsoleto. Anteriormente, podía incluir este elemento personalizado StorageGRID en el cuerpo de la solicitud XML opcional de las solicitudes CreateBucket para crear un depósito compatible.

> La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID está obsoleta y ha sido reemplazada por S3 Object Lock. Para más detalles, véase lo siguiente:
>
> - "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"
> - "Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"

Ya no es posible crear nuevos depósitos con la opción Cumplimiento habilitada. Se devuelve el siguiente mensaje de error si intenta utilizar las modificaciones de la solicitud CreateBucket para cumplimiento para crear un nuevo depósito compatible:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsoleto: solicitud de cumplimiento de GET Bucket

La solicitud de cumplimiento de GET Bucket está obsoleta. Sin embargo, puede seguir usando esta solicitud para determinar las configuraciones de cumplimiento actualmente vigentes para un bucket compatible heredado existente.

> La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID está obsoleta y ha sido reemplazada por S3 Object Lock. Para más detalles, véase lo siguiente:
>
> - "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"
> - "Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"

Debe tener el permiso s3:GetBucketCompliance o ser la cuenta root para completar esta operación.

Ejemplo de solicitud

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

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

Ejemplo de respuesta

En el XML de respuesta, `<SGCompliance>` enumera las configuraciones de cumplimiento vigentes para el depósito. Esta respuesta de ejemplo muestra las configuraciones de cumplimiento para un depósito en el que cada objeto se conservará durante un año (525 600 minutos), a partir del momento en que el objeto se ingiere en la red. Actualmente no existe ninguna retención legal sobre este depósito. Cada objeto se eliminará automáticamente después de un año.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nombre	Descripción
Minutos del período de retención	La duración del período de retención de los objetos agregados a este depósito, en minutos. El período de retención comienza cuando el objeto se incorpora a la red.
Retención legal	• Verdadero: Este depósito se encuentra actualmente bajo retención legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la retención legal, incluso si su período de retención ha expirado. • Falso: este depósito no se encuentra actualmente bajo retención legal. Los objetos de este depósito se pueden eliminar cuando expire su período de retención.
Eliminación automática	• Verdadero: Los objetos de este depósito se eliminarán automáticamente cuando expire su período de retención, a menos que el depósito esté bajo una retención legal. • Falso: Los objetos de este depósito no se eliminarán automáticamente cuando expire el período de retención. Debes eliminar estos objetos manualmente si necesitas eliminarlos.

Respuestas de error

Si el depósito no se creó para ser compatible, el código de estado HTTP para la respuesta es `404 Not Found` , con un código de error S3 de `XNoSuchBucketCompliance` .

Obsoleto: Solicitud de cumplimiento de PUT Bucket

La solicitud de cumplimiento de PUT Bucket está obsoleta. Sin embargo, puede seguir usando esta solicitud para modificar la configuración de cumplimiento de un depósito compatible heredado existente. Por ejemplo, puede colocar un depósito existente en retención legal o aumentar su período de retención.

La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID está obsoleta y ha sido reemplazada por S3 Object Lock. Para más detalles, véase lo siguiente:

- "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"
- "Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"

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

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

Ejemplo de solicitud

Esta solicitud de ejemplo modifica la configuración de cumplimiento para el depósito denominado `mybucket` . En este ejemplo, los objetos en `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 incorpora a la red. No existe ninguna retención legal sobre este cubo. Cada objeto se eliminará automáticamente después de dos años.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nombre	Descripción
Minutos del período de retención	La duración del período de retención de los objetos agregados a este depósito, en minutos. El período de retención comienza cuando el objeto se incorpora a la red. **Importante** Al especificar un nuevo valor para RetentionPeriodMinutes, debe especificar un valor que sea igual o mayor que el período de retención actual del depósito. Una vez establecido el período de retención del depósito, no puedes disminuir ese valor; solo puedes aumentarlo.

Nombre	Descripción
Retención legal	• Verdadero: Este depósito se encuentra actualmente bajo retención legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la retención legal, incluso si su período de retención ha expirado. • Falso: este depósito no se encuentra actualmente bajo retención legal. Los objetos de este depósito se pueden eliminar cuando expire su período de retención.
Eliminación automática	• Verdadero: Los objetos de este depósito se eliminarán automáticamente cuando expire su período de retención, a menos que el depósito esté bajo una retención legal. • Falso: Los objetos de este depósito no se eliminarán automáticamente cuando expire el período de retención. Debes eliminar estos objetos manualmente si necesitas eliminarlos.

Coherencia para la configuración de cumplimiento

Cuando actualiza la configuración de cumplimiento de un bucket S3 con una solicitud de cumplimiento de bucket PUT, StorageGRID intenta actualizar los metadatos del bucket en toda la red. De manera predeterminada, StorageGRID utiliza la consistencia **Strong-global** para garantizar que todos los sitios del centro de datos y todos los nodos de almacenamiento que contienen metadatos de bucket tengan consistencia de lectura después de escritura para las configuraciones de cumplimiento modificadas.

Si StorageGRID no puede lograr la consistencia **fuerte-global** porque un sitio de centro de datos o varios nodos de almacenamiento en un sitio no están disponibles, el código de estado HTTP para la respuesta es `503 Service Unavailable`.

Si recibe esta respuesta, debe comunicarse con el administrador de la red para asegurarse de que los servicios de almacenamiento necesarios estén disponibles lo antes posible. Si el administrador de la red no puede poner a disposición suficientes nodos de almacenamiento en cada sitio, el soporte técnico puede indicarle que vuelva a intentar la solicitud fallida forzando la consistencia **Strong-site**.

> Nunca fuerce la consistencia **Strong-site** para el cumplimiento del bucket PUT a menos que el soporte técnico se lo haya indicado y a menos que comprenda las posibles consecuencias de usar este nivel.

Cuando la consistencia se reduce a **Sitio fuerte**, StorageGRID garantiza que las configuraciones de cumplimiento actualizadas tendrán consistencia de lectura después de escritura solo para las solicitudes de clientes dentro de un sitio. Esto significa que el sistema StorageGRID podría tener temporalmente múltiples configuraciones inconsistentes para este depósito hasta que todos los sitios y nodos de almacenamiento estén disponibles. Las configuraciones inconsistentes pueden generar un comportamiento inesperado y no deseado. Por ejemplo, si coloca un depósito bajo una retención legal y fuerza una consistencia menor, las configuraciones de cumplimiento anteriores del depósito (es decir, retención legal) podrían seguir vigentes en algunos sitios de centros de datos. Como resultado, los objetos que usted considera que están en retención legal podrían eliminarse cuando expire su período de retención, ya sea por el usuario o por AutoDelete, si está habilitado.

Para forzar el uso de la consistencia **Strong-site**, vuelva a emitir la solicitud de cumplimiento de PUT Bucket e incluya la `Consistency-Control` Encabezado de solicitud HTTP, como sigue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Respuestas de error

- Si el depósito no se creó para ser compatible, el código de estado HTTP para la respuesta es `404 Not Found`.
- Si `RetentionPeriodMinutes` En la solicitud es menor que el período de retención actual del depósito, el código de estado HTTP es `400 Bad Request`.

Información relacionada

"Obsoleto: modificaciones de la solicitud PUT Bucket para cumplimiento"

Políticas de acceso a grupos y buckets

Utilice políticas de acceso a grupos y buckets

StorageGRID utiliza el lenguaje de políticas de Amazon Web Services (AWS) para permitir que los inquilinos de S3 controlen el acceso a los depósitos y los objetos dentro de esos depósitos. El sistema StorageGRID implementa un subconjunto del lenguaje de políticas de la API REST de S3. Las políticas de acceso para la API S3 están escritas en JSON.

Descripción general de la política de acceso

StorageGRID admite dos tipos de políticas de acceso.

- **Políticas de bucket**, que se administran mediante las operaciones de API S3 GetBucketPolicy, PutBucketPolicy y DeleteBucketPolicy o la API Tenant Manager o Tenant Management. Las políticas de depósito se adjuntan a los depósitos, por lo que están configuradas para controlar el acceso de los usuarios en la cuenta del propietario del depósito u otras cuentas al depósito y a los objetos que contiene. Una política de buckets se aplica solo a un bucket y posiblemente a varios grupos.
- **Políticas de grupo**, que se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Las políticas de grupo están asociadas a un grupo en la cuenta, por lo que están configuradas para permitir que ese grupo acceda a recursos específicos que pertenecen a esa cuenta. Una política de grupo se aplica solo a un grupo y posiblemente a varios grupos.

> No hay diferencia de prioridad entre las políticas de grupo y de grupo.

Las políticas de grupo y de depósito de StorageGRID siguen una gramática específica definida por Amazon. Dentro de cada política hay una serie de declaraciones de políticas, y cada declaración contiene los siguientes elementos:

- ID de declaración (Sid) (opcional)
- Efecto
- Director/No director
- Recurso/NoRecurso

- Acción/No acción
- Condición (opcional)

Las declaraciones de política se crean utilizando esta estructura para especificar permisos: Otorgar <Efecto> para permitir/denegar que <Principal> realice <Acción> en <Recurso> cuando se aplica <Condición>.

Cada elemento de política se utiliza para una función específica:

Elemento	Descripción
Sid	El elemento Sid es opcional. El Sid solo pretende servir como descripción para el usuario. Se almacena pero no es interpretado por el sistema StorageGRID .
Efecto	Utilice el elemento Efecto para establecer si las operaciones especificadas están permitidas o denegadas. Debe identificar las operaciones que permite (o deniega) en depósitos u objetos utilizando las palabras clave del elemento Acción compatible.
Director/No director	Puede permitir que usuarios, grupos y cuentas accedan a recursos específicos y realicen 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, solo la cuenta raíz tiene acceso a los recursos que posee la cuenta. Solo es necesario especificar el elemento Principal en una política de bucket. Para las políticas de grupo, el grupo al que está asociada la política es el elemento Principal implícito.
Recurso/NoRecurso	El elemento Recurso identifica depósitos y objetos. Puede permitir o denegar permisos para depósitos y objetos utilizando el nombre de recurso de Amazon (ARN) para identificar el recurso.
Acción/No acción	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 mismo. Se deniega el acceso a menos que usted asigne permisos específicos, pero puede usar la denegación explícita para anular un permiso otorgado por otra política.
Condición	El elemento Condición es opcional. Las condiciones le permiten crear expresiones para determinar cuándo se debe aplicar una política.

En el elemento Acción, 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 Recurso, puede utilizar los caracteres comodín (*) y (?). Mientras que el asterisco (*) coincide con 0 o más caracteres, el signo de interrogación (?) coincide con cualquier carácter individual.

En el elemento Principal, no se admiten caracteres comodín excepto para establecer acceso anónimo, que otorga permiso a todos. Por ejemplo, establece el comodín (*) como valor principal.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

En el siguiente ejemplo, la declaración utiliza los elementos Efecto, Principal, Acción y Recurso. Este ejemplo muestra una declaración de política de bucket completa que utiliza el efecto "Permitir" para otorgar a los principales, el grupo de administración `federated-group/admin` y el grupo financiero `federated-group/finance` , permisos para realizar la Acción `s3:ListBucket` en el cubo llamado `mybucket` y la Acción `s3:GetObject` en todos los objetos dentro de ese cubo.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

La política de depósito tiene un límite de tamaño de 20 480 bytes y la política de grupo tiene un límite de tamaño de 5120 bytes.

Coherencia de las políticas

De forma predeterminada, cualquier actualización que realice en las políticas de grupo será coherente en el futuro. Cuando una política de grupo se vuelve consistente, los cambios pueden tardar 15 minutos adicionales en surtir efecto, debido al almacenamiento en caché de la política. De forma predeterminada, todas las actualizaciones que realice en las políticas de depósito serán muy coherentes.

Según sea necesario, puede cambiar las garantías de consistencia para las actualizaciones de la política de bucket. Por ejemplo, es posible que desee que un cambio en una política de depósito esté disponible durante una interrupción del sitio.

En este caso, puede configurar el `Consistency-Control` encabezado en la solicitud PutBucketPolicy, o puede utilizar la solicitud de consistencia PUT Bucket. Cuando una política de bucket se vuelve consistente, los cambios pueden tardar 8 segundos adicionales en surtir efecto, debido al almacenamiento en caché de políticas.

> Si establece la consistencia en un valor diferente para solucionar una situación temporal, asegúrese de restablecer la configuración de nivel de depósito a su valor original cuando haya terminado. De lo contrario, todas las futuras solicitudes de bucket utilizarán la configuración modificada.

Utilice ARN en declaraciones de políticas

En las declaraciones de políticas, el ARN se utiliza en los elementos Principal y Recurso.

- Utilice esta sintaxis para especificar el ARN del recurso S3:

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

- Utilice esta sintaxis para especificar el ARN del recurso de identidad (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 del objeto.
- Los caracteres internacionales, que se pueden especificar en la clave del objeto, deben codificarse utilizando JSON UTF-8 o utilizando secuencias de escape JSON \u. No se admite la codificación porcentual.

  "Sintaxis URN RFC 2141"

  El cuerpo de la solicitud HTTP para la operación PutBucketPolicy debe estar codificado con charset=UTF-8.

Especificar recursos en una política

En las declaraciones de políticas, puede utilizar el elemento Recurso para especificar el depósito o el objeto para el cual se permiten o deniegan permisos.

- Cada declaración de política requiere un elemento de recurso. En una política, los recursos se denotan mediante el elemento `Resource` , o alternativamente, `NotResource` para exclusión.
- Usted especifica recursos con un ARN de recurso S3. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- También puede utilizar variables de política dentro de la clave del objeto. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- El valor del recurso puede especificar un depósito que aún no existe cuando se crea una política de grupo.

Especificar los principales en una política

Utilice el elemento Principal para identificar el usuario, grupo o cuenta de inquilino a quien se le permite o deniega el acceso al recurso mediante la declaración de política.

- Cada declaración de política en una política de grupo 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 principales se indican con el elemento "Principal" o, alternativamente, "NoPrincipal" para su exclusión.
- Las identidades basadas en cuentas deben especificarse mediante un ID o un ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- Este ejemplo 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 solo la cuenta raíz:

```
"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 ("Administradores"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Puede especificar un principal anónimo:

```
"Principal": "*"
```

- Para evitar ambigüedades, puede utilizar el UUID del 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 elimina Si un nuevo Alex se une a la organización y se le asigna el mismo `Alex` nombre de usuario, el nuevo usuario podría heredar involuntariamente los permisos otorgados al usuario original.

- El valor principal puede especificar un nombre de grupo/usuario que aún no existe cuando se crea una política de depósito.

Especificar permisos en una política

En una política, el elemento Acción se utiliza para permitir o denegar permisos a un recurso. Hay un conjunto de permisos que puedes especificar en una política, que se indican con el elemento "Acción" o, alternativamente, "No acción" para la exclusión. Cada uno de estos elementos se asigna a operaciones específicas de la API REST de S3.

Las tablas enumeran los permisos que se aplican a los depósitos y los permisos que se aplican a los objetos.

> Amazon S3 ahora usa el permiso s3:PutReplicationConfiguration para las acciones PutBucketReplication y DeleteBucketReplication. StorageGRID utiliza permisos separados para cada acción, lo que coincide con la especificación original de Amazon S3.

> Se realiza una eliminación cuando se utiliza una operación put para sobrescribir un valor existente.

Permisos que se aplican a los buckets

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3:CrearCubo	Crear cubo	Sí. **Nota**: Úselo solo en políticas de grupo.
s3:Eliminar depósito	Eliminar cubo	

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3:Notificación de metadatos de eliminación de depósito	Configuración de notificación de metadatos del depósito DELETE	Sí
s3: Eliminar política de depósito	Política de eliminación de cubos	
s3:Eliminar configuración de replicación	EliminarReplicaciónDeBucket	Sí, permisos separados para PUT y DELETE
s3:ObtenerAcl del depósito	ObtenerBucketAcl	
s3:Obtener cumplimiento del cubo	Cumplimiento de GET Bucket (obsoleto)	Sí
s3: Obtener consistencia del cubo	Obtener consistencia del bucket	Sí
s3:ObtenerBucketCORS	ObtenerBucketCors	
s3:Obtener configuración de cifrado	Obtener cifrado de cubo	
s3: Obtener hora del último acceso al depósito	GET Hora del último acceso al bucket	Sí
s3: Obtener ubicación del depósito	Obtener la ubicación del cubo	
s3:Obtener notificación de metadatos del depósito	Configuración de notificación de metadatos del depósito GET	Sí
s3:Obtener notificación del cubo	Configuración de GetBucketNotification	
s3:Configuración de bloqueo de objeto de depósito	Obtener configuración de bloqueo de objeto	
s3: Obtener política de depósito	Obtener política de cubo	
s3: Obtener etiquetado de cubo	Obtener etiquetado de cubos	
s3: Obtener versiones de Bucket	Obtener versiones de Bucket	
s3:Obtener configuración del ciclo de vida	Obtener configuración del ciclo de vida del cubo	
s3:Obtener configuración de replicación	Obtener réplica de cubo	

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3: Listar todos mis cubos	• Lista de cubos • Uso de almacenamiento GET	Sí, para el uso de almacenamiento GET. **Nota**: Úselo solo en políticas de grupo.
s3:ListBucket	• Lista de objetos • Cubo de cabeza • Restaurar objeto	
s3:ListBucketMultipartUploads	• Lista de cargas de varias partes • Restaurar objeto	
s3:ListBucketVersions	GET Versiones del Bucket	
s3:Cumplimiento de PutBucket	Cumplimiento del contenedor PUT (obsoleto)	Sí
s3:Consistencia del cubo de colocación	Consistencia del depósito PUT	Sí
s3:PonerCuboCORS	• EliminarBucketCors† • PonerBucketCors	
s3:PonerConfiguraciónDeCifrado	• Eliminar cifrado del cubo • Cifrado de PutBucket	
s3:PonerBucketÚltimoAccesoHora	Hora del último acceso al depósito PUT	Sí
s3:Notificación de metadatos de PutBucket	Configuración de notificación de metadatos del depósito PUT	Sí
s3:Notificación de depósito de colocación	Configuración de notificación de PutBucket	
s3:Configuración de bloqueo de objeto PutBucket	• CreateBucket con el `x-amz-bucket-object-lock-enabled: true` encabezado de solicitud (también requiere el permiso s3:CreateBucket) • Configuración de bloqueo de objeto de colocación	
s3:Política de depósito de colocación	Política de depósito de basura	

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3:Etiquetado de cubo de colocación	• Eliminar etiquetado de cubos† • Etiquetado de PutBucket	
s3:Versión de PutBucket	Versiones de PutBucket	
s3:Configuración del ciclo de vida de PutLifecycle	• Eliminar ciclo de vida del cubo† • Configuración del ciclo de vida de PutBucket	
s3:PonerConfiguraciónDeReplicación	Replicación de PutBucket	Sí, permisos separados para PUT y DELETE

Permisos que se aplican a los objetos

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3:AbortarCargaMultiparte	• AbortarMultipartUpload • Restaurar objeto	
s3: Retención de gobernanza de bypass	• Eliminar objeto • Eliminar objetos • PonerRetenciónDeObjeto	
s3:EliminarObjeto	• Eliminar objeto • Eliminar objetos • Restaurar objeto	
s3:EliminarEtiquetadoDeObjeto	Eliminar etiquetado de objetos	
s3: Eliminar etiquetado de versión de objeto	DeleteObjectTagging (una versión específica del objeto)	
s3:EliminarVersiónDeObjeto	DeleteObject (una versión específica del objeto)	
s3:Obtener objeto	• Obtener objeto • Objeto principal • Restaurar objeto • Seleccionar contenido del objeto	

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3:ObtenerAclObjeto	ObtenerObjetoAcl	
s3:ObtenerRetenciónLegalDeObjeto	Obtener retención legal de objeto	
s3:ObtenerRetenciónDeObjeto	Obtener retención de objetos	
s3:Obtener etiquetado de objeto	Obtener etiquetado de objetos	
s3: Obtener etiquetado de versión de objeto	GetObjectTagging (una versión específica del objeto)	
s3:ObtenerVersiónDeObjeto	GetObject (una versión específica del objeto)	
s3:ListaMultiparteSubirPartes	Lista de partes, Restaurar objeto	
s3:PonerObjeto	• PonerObjeto • Copiar objeto • Restaurar objeto • Crear carga de varias partes • Carga completa de varias partes • Subir parte • Subir copia parcial	
s3:PonerObjetoLegalRetenido	PonerObjetoLegalRetención	
s3:PonerRetenciónDeObjeto	PonerRetenciónDeObjeto	
s3:Etiquetado de objetos de colocación	Etiquetado de objetos puestos	
s3:Etiquetado de versión de objeto de colocación	PutObjectTagging (una versión específica del objeto)	
s3:PonerObjetoSobrescrito	• PonerObjeto • Copiar objeto • Etiquetado de objetos puestos • Eliminar etiquetado de objetos • Carga completa de varias partes	Sí
s3:RestaurarObjeto	Restaurar objeto	

Utilice el permiso PutOverwriteObject

El permiso s3:PutOverwriteObject es un permiso de StorageGRID personalizado que se aplica a las operaciones que crean o actualizan objetos. La configuración de este permiso determina si el cliente puede sobrescribir los datos de un objeto, los metadatos definidos por el usuario o el etiquetado de objetos S3.

Las posibles configuraciones para este permiso incluyen:

- **Permitir**: El cliente puede sobrescribir un objeto. Esta es la configuración predeterminada.
- **Denegar**: El cliente no puede sobrescribir un objeto. Cuando se establece en Denegar, el permiso PutOverwriteObject funciona de la siguiente manera:
  - Si se encuentra un objeto existente en la misma ruta:
    - Los datos del objeto, los metadatos definidos por el usuario o el etiquetado del objeto S3 no se pueden sobrescribir.
    - Cualquier operación de ingesta en curso se cancela y se devuelve un error.
    - Si el control de versiones S3 está habilitado, la configuración Denegar evita que las operaciones PutObjectTagging o DeleteObjectTagging modifiquen el TagSet de 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 estuviera configurado Permitir.

> Si la política S3 actual permite sobrescribir y el permiso PutOverwriteObject está configurado en Denegar, el cliente no puede sobrescribir los datos de un objeto, los metadatos definidos por el usuario ni el etiquetado de objetos. Además, si se selecciona la casilla de verificación **Evitar modificación del cliente** (**CONFIGURACIÓN** > **Configuración de seguridad** > **Red y objetos**), esa configuración anula la configuración del permiso PutOverwriteObject.

Especificar condiciones en una póliza

Las condiciones definen cuándo entrará en vigor una política. Las condiciones constan de operadores y pares clave-valor.

Las condiciones utilizan pares clave-valor para la evaluación. Un elemento Condición puede contener múltiples condiciones, y cada condición puede contener múltiples pares clave-valor. El bloque de condición utiliza el siguiente formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

En el siguiente ejemplo, la condición IpAddress utiliza la clave de condición SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Operadores de condición admitidos

Los operadores de condición se clasifican de la siguiente manera:

- Cadena
- Numérico
- Booleano
- Dirección IP
- Comprobación nula

Operadores de condición	Descripción
CadenaIgual	Compara una clave con un valor de cadena basándose en la coincidencia exacta (distingue entre mayúsculas y minúsculas).
CadenaNoIgual	Compara una clave con un valor de cadena basándose en la coincidencia negada (distingue entre mayúsculas y minúsculas).
CadenaIgualIgnorarMayúsculas y Minúsculas	Compara una clave con un valor de cadena basándose en la coincidencia exacta (ignora mayúsculas y minúsculas).
CadenaNoIgualIgnorarMayúsculas y Minúsculas	Compara una clave con un valor de cadena basándose en la coincidencia negada (ignora mayúsculas y minúsculas).
Similar a una cadena	Compara una clave con un valor de cadena basándose en la coincidencia exacta (distingue entre mayúsculas y minúsculas). Puede incluir caracteres comodín * y ?.
CadenaNoMe Gusta	Compara una clave con un valor de cadena basándose en la coincidencia negada (distingue entre mayúsculas y minúsculas). Puede incluir caracteres comodín * y ?.
NumericEquals	Compara una clave con un valor numérico basándose en la coincidencia exacta.
NuméricoNoIgual	Compara una clave con un valor numérico basándose en la coincidencia negada.

Operadores de condición	Descripción
NuméricoMayorQue	Compara una clave con un valor numérico basándose en la coincidencia "mayor que".
NuméricoMayorQueIgual	Compara una clave con un valor numérico basándose en la coincidencia "mayor o igual que".
NuméricoMenosQue	Compara una clave con un valor numérico basándose en la coincidencia "menor que".
NuméricoMenorQueIgual	Compara una clave con un valor numérico basándose en la coincidencia "menor o igual que".
Bool	Compara una clave con un valor booleano basándose en la coincidencia "verdadero o falso".
Dirección IP	Compara una clave con una dirección IP o un rango de direcciones IP.
No dirección IP	Compara una clave con una dirección IP o un rango de direcciones IP basándose en la coincidencia negada.
Nulo	Comprueba si una clave de condición está presente en el contexto de solicitud actual.

Claves de condición admitidas

Claves de condición	Comportamiento	Descripción
aws:FuenteIp	Operadores de IP	Se comparará con la dirección IP desde la que se envió la solicitud. Se puede utilizar para operaciones con cubos o con objetos. **Nota:** Si la solicitud S3 se envió a través del servicio Load Balancer en los nodos de administración y los nodos de puerta de enlace, esto se comparará con la dirección IP ascendente del servicio Load Balancer. **Nota**: Si se utiliza un balanceador de carga de terceros no transparente, esto se comparará con la dirección IP de ese balanceador de carga. Cualquier `X-Forwarded-For` El encabezado se ignorará porque no se puede determinar su validez.
aws:nombre de usuario	Recurso/Identidad	Se comparará con el nombre de usuario del remitente desde el que se envió la solicitud. Se puede utilizar para operaciones con cubos o con objetos.

Claves de condición	Comportamiento	Descripción
s3:delimitador	s3:ListBucket y Permisos s3:ListBucketVersions	Se comparará con el parámetro delimitador especificado en una solicitud ListObjects o ListObjectVersions.
s3:ExistingObjectTag/<clave de etiqueta>	s3:EliminarEtiquetadoDeObjeto s3: Eliminar etiquetado de versión de objeto s3:Obtener objeto s3:ObtenerAclObjeto 3: Obtener etiquetado de objetos s3:ObtenerVersiónDeObjeto s3:ObtenerAcl de versión de objeto s3: Obtener etiquetado de versión de objeto s3:PonerObjetoAcl s3:Etiquetado de objetos de colocación s3:PonerObjetoVersiónAcl s3:Etiquetado de versión de objeto de colocación	Requerirá que el objeto existente tenga la clave y el valor de etiqueta específicos.
s3:máximo de teclas	s3:ListBucket y Permisos s3:ListBucketVersions	Se comparará con el parámetro max-keys especificado en una solicitud ListObjects o ListObjectVersions.

Claves de condición	Comportamiento	Descripción
s3: días de retención restantes del bloqueo de objeto	s3:PonerObjeto	Se compara con la fecha de conservación especificada en el `x-amz-object-lock-retain-until-date` encabezado de solicitud o calculado a partir del período de retención predeterminado del depósito para asegurarse de que estos valores estén dentro del rango permitido para las siguientes solicitudes: • PonerObjeto • Copiar objeto • Crear carga de varias partes
s3: días de retención restantes del bloqueo de objeto	s3:PonerRetenciónDeObjeto	Se compara con la fecha de retención hasta especificada en la solicitud PutObjectRetention para garantizar que esté dentro del rango permitido.
s3:prefijo	s3:ListBucket y Permisos s3:ListBucketVersions	Se comparará con el parámetro de prefijo especificado en una solicitud ListObjects o ListObjectVersions.
s3:RequestObjectTag/<clave de etiqueta>	s3:PonerObjeto s3:Etiquetado de objetos de colocación s3:Etiquetado de versión de objeto de colocación	Requerirá una clave y un valor de etiqueta específicos cuando la solicitud de objeto incluya etiquetado.

Especificar variables en una política

Puede utilizar variables en las políticas para completar la información de políticas cuando esté disponible. Puede utilizar variables de política en el `Resource` elemento y en comparaciones de cadenas en el `Condition` elemento.

En este ejemplo, la variable `${aws:username}` es parte del elemento Recurso:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

En este ejemplo, la variable `${aws:username}` es parte del valor de la condición en el bloque de condición:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variable	Descripción
`${aws:SourceIp}`	Utiliza la clave SourceIp como variable proporcionada.
`${aws:username}`	Utiliza la clave de nombre de usuario como variable proporcionada.
`${s3:prefix}`	Utiliza la clave de prefijo específica del servicio como la variable proporcionada.
`${s3:max-keys}`	Utiliza la clave max-keys específica del servicio como variable proporcionada.
`${*}`	Carácter especial. Utiliza el carácter como un carácter literal *.
`${?}`	Carácter especial. Utiliza el carácter como un carácter literal ?.
`${$}`	Carácter especial. Utiliza el carácter como un carácter literal $.

Crear políticas que requieran un manejo especial

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

Descripción de la política	Tipo de póliza	Comportamiento de Amazon	Comportamiento de StorageGRID
Negarse a sí mismo cualquier permiso a la cuenta raíz	Balde	Válido y aplicado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bucket de S3	Mismo
Negarme cualquier permiso a un usuario o grupo	Grupo	Válido y ejecutado	Mismo

Descripción de la política	Tipo de póliza	Comportamiento de Amazon	Comportamiento de StorageGRID
Permitir a un grupo de cuentas extranjeras cualquier permiso	Balde	Principal inválido	Válido, pero los permisos para todas las operaciones de políticas de bucket S3 devuelven un error 405 Método no permitido cuando lo permite una política
Permitir a una cuenta externa root o a un usuario cualquier permiso	Balde	Válido, pero los permisos para todas las operaciones de políticas de bucket S3 devuelven un error 405 Método no permitido cuando lo permite una política	Mismo
Permitir a todos permisos para todas las acciones	Balde	Válido, pero los permisos para todas las operaciones de política de bucket S3 devuelven un error 405 Método no permitido para la raíz de la cuenta externa y los usuarios	Mismo
Negar a todos los permisos para todas las acciones	Balde	Válido y aplicado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bucket de S3	Mismo
El principal es un usuario o grupo inexistente	Balde	Principal inválido	Válido
El recurso es un bucket S3 inexistente	Grupo	Válido	Mismo
Principal es un grupo local	Balde	Principal inválido	Válido
La política otorga a una cuenta que no es de propietario (incluidas las cuentas anónimas) permisos para colocar objetos.	Balde	Válido. Los objetos son propiedad de la cuenta del creador y la política de buckets no se aplica. La cuenta del creador debe otorgar permisos de acceso para el objeto mediante listas de control de acceso (ACL) de objeto.	Válido. Los objetos son propiedad de la cuenta del propietario del depósito. Se aplica la política de cubos.

Protección de escritura única y lectura múltiple (WORM)

Puede crear depósitos de escritura única y lectura múltiple (WORM) para proteger datos, metadatos de objetos definidos por el usuario y etiquetado de objetos S3. Configura los depósitos WORM para permitir la creación de nuevos objetos y evitar sobrescrituras o eliminaciones de contenido existente. Utilice uno de los enfoques descritos aquí.

Para garantizar que siempre se rechacen las sobrescrituras, puede:

- Desde el Administrador de red, vaya a **CONFIGURACIÓN** > **Seguridad** > **Configuración de seguridad** > **Red y objetos** y seleccione la casilla de verificación **Evitar modificación del cliente**.
- Aplicar las siguientes reglas y políticas S3:
  - Agregue una operación PutOverwriteObject DENY a la política S3.
  - Agregue una operación DeleteObject DENY a la política S3.
  - Agregue una operación PutObject ALLOW a la política S3.

> Establecer DeleteObject como DENY en una política S3 no impide que ILM elimine objetos cuando existe una regla como "cero copias después de 30 días".

> Incluso cuando se aplican todas estas reglas y políticas, no protegen contra escrituras simultáneas (ver Situación A). Protegen contra sobrescrituras completadas secuenciales (ver Situación B).

Situación A: Escrituras concurrentes (sin protección)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situación B: Sobrescrituras secuenciales completadas (protegidas contra)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Información relacionada

- "Cómo las reglas ILM de StorageGRID administran los objetos"
- "Ejemplos de políticas de depósito"
- "Políticas de grupo de ejemplo"
- "Administrar objetos con ILM"
- "Utilice una cuenta de inquilino"

Ejemplos de políticas de depósito

Utilice los ejemplos de esta sección para crear políticas de acceso de StorageGRID para los buckets.

Las políticas de depósito especifican los permisos de acceso para el depósito al que está asociada la política. Puede configurar una política de bucket mediante la API S3 PutBucketPolicy a través de una de estas herramientas:

- "Administrador de inquilinos" .
- AWS CLI usando este comando (consulte"Operaciones en buckets"):

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

Ejemplo: Permitir a todos el acceso de solo lectura a un depósito

En este ejemplo, todos, incluso los anónimos, pueden enumerar objetos en el depósito y realizar operaciones GetObject en todos los objetos del depósito. Se denegarán todas las demás operaciones. Tenga en cuenta que esta política puede no ser particularmente útil porque nadie excepto la cuenta raíz tiene permisos para escribir en el depósito.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Ejemplo: Permitir a todos los usuarios de una cuenta acceso completo y a todos los usuarios de otra cuenta acceso de solo lectura a un depósito.

En este ejemplo, a todos en una cuenta específica se les permite acceso completo a un depósito, mientras que a todos en otra cuenta específica solo se les permite listar el depósito y realizar operaciones GetObject en objetos en el depósito comenzando con el `shared/` prefijo de clave de objeto.

> En StorageGRID, los objetos creados por una cuenta que no es de propietario (incluidas las cuentas anónimas) son propiedad de la cuenta del propietario del depósito. La política de bucket 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 a todos acceso de solo lectura a un depósito y acceso completo a un grupo específico

En este ejemplo, todos, incluido el anónimo, pueden listar el depósito y realizar operaciones GetObject en todos los objetos del depósito, mientras que solo los usuarios que pertenecen al grupo `Marketing` En la cuenta especificada 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 a todos el acceso de lectura y escritura a un depósito si el cliente está en el rango de IP

En este ejemplo, todos, incluso los anónimos, pueden enumerar el depósito y realizar cualquier operación de objeto en todos los objetos del depósito, siempre que las solicitudes provengan de un rango de IP específico (54.240.143.0 a 54.240.143.255, excepto 54.240.143.188). Se rechazarán todas las demás operaciones y todas las solicitudes 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 depósito exclusivamente a un usuario federado específico

En este ejemplo, al usuario federado Alex se le permite acceso completo a la `examplebucket` cubo y sus objetos. A todos los demás usuarios, incluido 'root', se les niega explícitamente todas las operaciones. Sin embargo, tenga en cuenta que a 'root' nunca se le niegan los permisos para Put/Get/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Ejemplo: Permiso PutOverwriteObject

En este ejemplo, el `Deny` El efecto para PutOverwriteObject y DeleteObject garantiza que nadie pueda sobrescribir o eliminar los datos del objeto, los metadatos definidos por el usuario y el etiquetado de objetos S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Políticas de grupo de ejemplo

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

Las políticas de grupo especifican los permisos de acceso para el grupo al que está asociada la política. No hay `Principal` elemento de la política porque es implícito. Las políticas de grupo se configuran mediante el Administrador de inquilinos o la API.

Ejemplo: Establecer una política de grupo mediante el Administrador de inquilinos

Cuando agrega o edita un grupo en el Administrador de inquilinos, puede seleccionar una política de grupo para determinar qué permisos de acceso a S3 tendrán los miembros de este grupo. Ver "Crear grupos para un inquilino de S3" .

- **Sin acceso S3**: Opción predeterminada. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se les conceda acceso con una política de bucket. Si selecciona esta opción, solo el usuario root tendrá acceso a los recursos de S3 de forma predeterminada.
- **Acceso de solo lectura**: los usuarios de este grupo tienen acceso de solo lectura a los recursos de S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puedes editar esta cadena.
- **Acceso completo**: los usuarios de este grupo tienen acceso completo a los recursos de S3, incluidos los buckets. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puedes editar esta cadena.
- **Mitigación de ransomware**: esta política de muestra se aplica a todos los depósitos de este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden eliminar de forma permanente objetos de los depósitos que tienen habilitada la versión de objetos.

  Los usuarios del administrador de inquilinos que tienen el permiso Administrar todos los depósitos pueden anular esta política de grupo. Limite el permiso Administrar todos los depósitos a usuarios de confianza y utilice la autenticación multifactor (MFA) cuando esté disponible.

- **Personalizado**: A los usuarios del grupo se les otorgan los permisos que usted especifique en el cuadro de texto.

Ejemplo: Permitir al grupo acceso completo a todos los depósitos

En este ejemplo, a todos los miembros del grupo se les permite acceso total a todos los depósitos propiedad de la cuenta del inquilino, a menos que la política del depósito lo deniegue explícitamente.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Ejemplo: Permitir acceso de solo lectura al grupo a todos los depósitos

En este ejemplo, todos los miembros del grupo tienen acceso de solo lectura a los recursos de S3, a menos que la política del bucket lo niegue explícitamente. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Ejemplo: Permitir a los miembros del grupo acceso completo únicamente a su "carpeta" en un depósito

En este ejemplo, a los miembros del grupo solo se les permite enumerar y acceder a su carpeta específica (prefijo de clave) en el depósito especificado. Tenga en cuenta que los permisos de acceso de otras políticas de grupo y la política de depósito deben considerarse 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}/*"
    }
  ]
}
```

Operaciones de S3 rastreadas en los registros de auditoría

Los mensajes de auditoría son generados por los servicios de StorageGRID y almacenados en archivos de registro de texto. Puede revisar los mensajes de auditoría específicos de S3 en el registro de auditoría para obtener detalles sobre las operaciones de buckets y objetos.

Operaciones de bucket rastreadas en los registros de auditoría

- Crear cubo
- Eliminar cubo
- Eliminar etiquetado de cubo
- Eliminar objetos
- Obtener etiquetado de cubos
- Cubo de cabeza
- Lista de objetos
- Lista de versiones de objetos
- Cumplimiento del contenedor PUT
- Etiquetado de PutBucket
- Versiones de PutBucket

Operaciones de objetos rastreadas en los registros de auditoría

- Carga completa de varias partes
- Copiar objeto
- Eliminar objeto
- Obtener objeto
- Objeto principal
- PonerObjeto
- Restaurar objeto
- Seleccionar objeto
- UploadPart (cuando una regla ILM utiliza ingesta equilibrada o estricta)
- UploadPartCopy (cuando una regla ILM utiliza ingesta equilibrada o estricta)

Información relacionada

- "Archivo de registro de auditoría de acceso"
- "El cliente escribe mensajes de auditoría"
- "El cliente lee mensajes de auditoría"

Información de copyright

Información de la marca comercial