



USE LA API DE REST DE S3

StorageGRID software

NetApp

February 12, 2026

Tabla de contenidos

USE LA API DE REST DE S3	1
Versiones y actualizaciones compatibles con la API de REST DE S3.....	1
Versiones compatibles	1
Actualizaciones del soporte de la API de REST DE S3	1
Referencia rápida: Solicitudes de API de S3 admitidas	4
Parámetros de consulta URI comunes y cabeceras de solicitud.....	5
AbortMultipartUpload	5
CompleteMultipartUpload	5
CopyObject	6
CreateBucket	7
CreateMultipartUpload	7
DeleteBucket	8
DeleteBucketCors	8
DeleteBucketEncryption	8
DeleteBucketLifecycle	8
DeleteBucketPolicy	9
DeleteBucketReplication	9
DeleteBucketTagging	9
DeleteObject	9
DeleteObjects	10
DeleteObjectTagging	10
GetBucketAcl	10
GetBucketCors	10
GetBucketEncryption	11
GetBucketLifecycleConfiguration	11
GetBucketLocation	11
GetBucketNotificationConfiguration	11
GetBucketPolicy	11
GetBucketReplication	12
Etiquetado de GetBucketTagging	12
GetBucketVersioning	12
GetObject	12
GetObjectAcl	13
GetObjectLegalHold	13
GetObjectLockConfiguration	14
GetObjectRetention	14
GetObjectEtiquetado	14
Segmento de cabeza	14
Objeto principal	14
ListCuchers	15
ListCargas multipartitas	15
ListObjects	16
ListObjectsV2	16

"ListObjectVersions"	16
"ListParts"	17
"A cargo de PutBucketCors"	17
"PutBucketEncryption"	17
"PutBucketLifecycleConfiguration"	18
"PutBucketNotificationConfiguration"	19
"Política de PutBucketPolicy"	19
"PutBucketReplication"	19
"PutBucketTagging"	20
"PutBucketVersioning"	20
"Objeto de puta"	20
"PutObjectLegalHold"	21
"PutObjectLockConfiguration"	21
"PutObjectRetention"	21
"PutObjectEtiquetado"	22
"RestoreObject"	22
"SelectObjectContent"	22
"UploadPart"	22
"UploadPartCopy"	23
Probar la configuración de la API de REST S3	24
Cómo StorageGRID implementa la API DE REST de S3	25
Solicitudes de clientes en conflicto	25
Coherencia	25
Control de versiones de objetos	28
Use la API REST DE S3 para configurar el bloqueo de objetos de S3	29
Cree una configuración del ciclo de vida de S3.	35
Recomendaciones para implementar la API REST de S3	39
Soporte para la API de REST DE Amazon S3	41
S3 Detalles de implementación de la API de REST	41
Autenticar solicitudes	42
Operaciones en el servicio	42
Operaciones en bloques	43
Operaciones en objetos	51
Operaciones para cargas de varias partes	80
Respuestas de error	89
Operaciones personalizadas de StorageGRID	91
Operaciones personalizadas de StorageGRID	91
OBTENGA coherencia de bloques	92
PONGA la consistencia del cucharón	94
GET Bucket última hora de acceso	95
PUT Bucket última hora de acceso	95
Configuración de notificaciones de metadatos de DELETE Bucket	97
OBTENGA la configuración de notificación de metadatos del bloque de datos	97
Configuración de notificaciones de metadatos de PUT Bucket	100
OBTENGA la solicitud de uso del almacenamiento	106

Solicitudes de bloque obsoletas para cumplimiento de normativas heredadas	107
Administrar políticas de acceso	113
Utilizar políticas de acceso	113
Ejemplo de política de sesión	131
Ejemplo de políticas de bloque	131
Ejemplo de políticas de grupo	137
Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría	140
Se realizó un seguimiento de las operaciones de bloque en los registros de auditoría	140
Se realizó un seguimiento de las operaciones de objetos en los registros de auditoría	141

USE LA API DE REST DE S3

Versiones y actualizaciones compatibles con la API de REST DE S3

StorageGRID admite la API de simple Storage Service (S3), que se implementa como un conjunto de servicios web de transferencia de estado de representación (REST).

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

Versiones compatibles

StorageGRID admite las siguientes versiones específicas de STS, S3 y HTTP:

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

Actualizaciones del soporte de la API de REST DE S3

Liberar	Comentarios
12,0	<ul style="list-style-type: none">Se agregó soporte para compartir recursos de origen cruzado (CORS) para una interfaz de administración, lo que permite que otro dominio acceda a datos en StorageGRID mediante API de administración. "Leer más".Se agregó soporte para STS AssumeRole y la política de sesión. Ver "un ejemplo de una política de sesión". Puede configurar AssumeRole en grupos de inquilinos.

Liberar	Comentarios
11,9	<ul style="list-style-type: none"> • Se ha agregado soporte para valores de suma de comprobación SHA-256 calculados previamente para las siguientes solicitudes y cabeceras soportadas. Puede utilizar esta función para verificar la integridad de los objetos cargados: <ul style="list-style-type: none"> ◦ Completa multipartCarga: <code>x-amz-checksum-sha256</code> ◦ CreateMultipartUpload: <code>x-amz-checksum-algorithm</code> ◦ GetObject: <code>x-amz-checksum-mode</code> ◦ Objeto de cabecera: <code>x-amz-checksum-mode</code> ◦ ListParts ◦ Objeto PutObject: <code>x-amz-checksum-sha256</code> ◦ Parte de carga: <code>x-amz-checksum-sha256</code> • Se ha añadido la capacidad del administrador de grid de controlar la retención a nivel de inquilino y la configuración de cumplimiento de normativas. Esta configuración afecta a la configuración de bloqueo de objetos S3. <ul style="list-style-type: none"> ◦ Modo de retención predeterminado de buckets y modo de retención de objetos: Gobernanza o cumplimiento de normativas, si lo permite el administrador de grid. ◦ Período de retención por defecto del depósito y fecha de retención del objeto: Debe ser menor o igual que lo permitido por el período de retención máximo definido por el administrador de grid. • Soporte mejorado para <code>aws-chunked</code> codificación de contenido y valores de streaming <code>x-amz-content-sha256</code>. Limitaciones: <ul style="list-style-type: none"> ◦ Si está presente, <code>chunk-signature</code> es opcional y no está validado ◦ Si está presente, <code>x-amz-trailer</code> el contenido se ignora
11,8	Se han actualizado los nombres de las operaciones S3 para que coincidan con los nombres utilizados en el " "Documentación de Amazon Web Services (AWS): Referencia de API de Amazon simple Storage Service" ".
11,7	<ul style="list-style-type: none"> • Agregado ""Referencia rápida: Solicitudes de API de S3 admitidas"". • Se ha añadido soporte para el uso del modo de GOBIERNO con S3 Object Lock. • Se ha añadido soporte para la cabecera de respuesta específica de StorageGRID <code>x-ntap-sg-cgr-replication-status</code> para las solicitudes de objetos GET Object y HEAD Object. Este encabezado proporciona el estado de replicación de un objeto para la replicación entre grid. • Las solicitudes SelectObjectContent ahora admiten objetos de Parquet.

Liberar	Comentarios
11,6	<ul style="list-style-type: none"> • Se ha agregado soporte para el uso partNumber del parámetro request en las solicitudes GET Object y HEAD Object. • Se añadió compatibilidad con un modo de retención predeterminado y un período de retención predeterminado en el nivel de bloque para S3 Object Lock. • Se ha añadido compatibilidad con s3:object-lock-remaining-retention-days la clave de condición de política para establecer el rango de períodos de retención permitidos para los objetos. • Se ha cambiado el tamaño máximo de recommended para una única operación PUT Object a 5 GiB (5.368.709.120 bytes). Si tiene objetos que sean mayores de 5 GiB, utilice la carga de varias partes en su lugar.
11,5	<ul style="list-style-type: none"> • Se ha agregado compatibilidad para gestionar el cifrado de bloques. • Se añadió compatibilidad con el bloqueo de objetos S3 y las solicitudes de cumplimiento heredadas obsoletas. • Se ha agregado soporte para el uso DE DELETE Multiple Objects en cubos con versiones. • El Content-MD5 encabezado de solicitud ahora está correctamente soportado.
11,4	<ul style="list-style-type: none"> • Se añadió compatibilidad con el etiquetado DE bloques DE DELETE, GET Bucket y PUT Bucket. No se admiten etiquetas de asignación de costes. • En el caso de bloques creados en StorageGRID 11.4, ya no es necesario restringir los nombres de claves de objetos para cumplir con las prácticas recomendadas de rendimiento. • Se ha añadido soporte para las notificaciones de bloques en el s3:ObjectRestore:Post tipo de evento. • Ahora se aplican los límites de tamaño de AWS para piezas multiparte. Cada parte de una carga de varias partes debe tener entre 5 MiB y 5 GiB. La última parte puede ser menor que 5 MiB. • Añadido soporte para TLS 1,3
11,3	<ul style="list-style-type: none"> • Se ha añadido compatibilidad con el cifrado en el servidor de los datos de objetos con las claves proporcionadas por el cliente (SSE-C). • Se ha añadido soporte para operaciones de ciclo de vida de SUPRESIÓN, OBTENCIÓN y COLOCACIÓN DE bloques (sólo acción de caducidad) y para x-amz-expiration la cabecera de respuesta. • Se han actualizado PUT Object, PUT Object - Copy y Multipart Upload para describir el impacto de las reglas de ILM que utilizan la colocación síncrona en el procesamiento. • Ya no se admiten los cifrados TLS 1.1.

Liberar	Comentarios
11,2	<p>Compatibilidad añadida para la restauración DE objetos POSTERIOR para uso con pools de almacenamiento en cloud. Se añadió compatibilidad con el uso de la sintaxis AWS para ARN, claves de condición de política y variables de política en políticas de grupos y bloques. Se seguirán soportando las políticas de grupo y bloque existentes que utilicen la sintaxis StorageGRID.</p> <p>Nota: los usos de ARN/URN en otra configuración JSON/XML, incluidos los utilizados en las características personalizadas de StorageGRID, no han cambiado.</p>
11,1	Se ha añadido soporte para el uso compartido de recursos de origen cruzado (CORS), HTTP para conexiones de clientes S3 a nodos de grid y configuraciones de cumplimiento en bloques.
11,0	Se añadió compatibilidad para configurar servicios de plataforma (replicación de CloudMirror, notificaciones e integración de búsqueda de Elasticsearch) para los bloques. También se ha agregado soporte para las restricciones de ubicación de etiquetado de objetos para bloques y la coherencia disponible.
10,4	Se ha agregado compatibilidad con los cambios de análisis de ILM en las versiones, las actualizaciones de página de nombres de dominio de extremo, las condiciones y variables en las directivas, los ejemplos de directivas y el permiso PutOverwriteObject.
10,3	Se ha añadido compatibilidad con las versiones.
10,2	Se ha añadido compatibilidad con las políticas de acceso a grupos y bloques y para la copia de varias partes (cargar artículo - copia).
10,1	Se añadió compatibilidad con la carga de varias partes, las solicitudes de estilo hospedado virtual y la autenticación v4.
10,0	Soporte inicial de la API REST S3 por parte del sistema StorageGRID . La versión actualmente compatible de la <i>Referencia de API del servicio de almacenamiento simple</i> es 2006-03-01.

Referencia rápida: Solicitudes de API de S3 admitidas

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

Esta página incluye solo las operaciones S3 compatibles con StorageGRID.



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

Parámetros de consulta URI comunes y cabeceras de solicitud

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

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

A menos que se indique lo contrario, se admiten las siguientes cabeceras de solicitud comunes:

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

Información relacionada

- "[S3 Detalles de implementación de la API de REST](#)"
- "[Referencia de API de Amazon Simple Storage Service: Encabezados de solicitud comunes](#)"

"AbortMultipartUpload"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID soporta todos [parámetros y cabeceras comunes](#) para esta solicitud, además de este parámetro de consulta URI adicional:

- `uploadID`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones para cargas de varias partes"](#)

"CompleteMultipartUpload"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID soporta todos [parámetros y cabeceras comunes](#) para esta solicitud, además de este parámetro de consulta URI adicional:

- `uploadID`
- `x-amz-checksum-sha256`

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

Documentación de StorageGRID

["CompleteMultipartUpload"](#)

"CopyObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo [parámetros y cabeceras comunes](#) para esta solicitud, además de estos encabezados adicionales:

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

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"CopyObject"

"CreateBucket"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo [parámetros y cabeceras comunes](#) para esta solicitud, además de estos encabezados adicionales:

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

Solicitar el cuerpo

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

Documentación de StorageGRID

"Operaciones en bloques"

"CreateMultipartUpload"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo [parámetros y cabeceras comunes](#) para esta solicitud, además de estos encabezados adicionales:

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

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["CreateMultipartUpload"](#)

"DeleteBucket"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Documentación de StorageGRID

["Operaciones en bloques"](#)

"DeleteBucketCors"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"DeleteBucketEncryption"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"DeleteBucketLifecycle"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

- ["Operaciones en bloques"](#)
- ["Cree una configuración del ciclo de vida de S3"](#)

"DeleteBucketPolicy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"DeleteBucketReplication"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"DeleteBucketTagging"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"DeleteObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo [parámetros y cabeceras comunes](#) para esta solicitud, además de este encabezado de solicitud adicional:

- x-amz-bypass-governance-retention

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en objetos"](#)

"DeleteObjects"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo [parámetros y cabeceras comunes](#) para esta solicitud, además de este encabezado de solicitud adicional:

- x-amz-bypass-governance-retention

Solicitar el cuerpo

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

Documentación de StorageGRID

["Operaciones en objetos"](#)

"DeleteObjectTagging"

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en objetos"](#)

"GetBucketAcl"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"GetBucketCors"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"GetBucketEncryption"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"GetBucketLifecycleConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

- ["Operaciones en bloques"](#)
- ["Cree una configuración del ciclo de vida de S3"](#)

"GetBucketLocation"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"GetBucketNotificationConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"GetBucketPolicy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketReplication"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"Etiquetado de GetBucketTagging"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketVersioning"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID soporta todos [parámetros y cabeceras comunes](#) para esta solicitud, además de estos parámetros de consulta URI adicionales:

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

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

Y estos encabezados de solicitud adicionales:

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

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["GetObject"](#)

"GetObjectAcl"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en objetos"](#)

"GetObjectLegalHold"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)

"GetObjectLockConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)

"GetObjectRetention"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)

"GetObjectEtiquetado"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en objetos"](#)

"Segmento de cabeza"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"Objeto principal"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo [parámetros y cabeceras comunes](#) para esta solicitud, además de estos encabezados adicionales:

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

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Objeto principal"

"ListCuchers"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

[Operaciones en el servicio](#) › [ListBuckets](#)

"ListCargas multipartitas"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos los [parámetros y cabeceras comunes](#) casos de esta solicitud, además de estos parámetros adicionales:

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

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["ListCargas multipartitas"](#)

"ListObjects"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos los [parámetros y cabeceras comunes](#)casos de esta solicitud, además de estos parámetros adicionales:

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

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"ListObjectsV2"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos los [parámetros y cabeceras comunes](#)casos de esta solicitud, además de estos parámetros adicionales:

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

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"ListObjectVersions"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos los [parámetros y cabeceras comunes](#)casos de esta solicitud, además de estos parámetros adicionales:

- delimiter

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

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["Operaciones en bloques"](#)

"ListParts"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos los [parámetros y cabeceras comunes](#)casos de esta solicitud, además de estos parámetros adicionales:

- max-parts
- part-number-marker
- uploadID

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["ListCargas multipartitas"](#)

"A cargo de PutBucketCors"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

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

Documentación de StorageGRID

["Operaciones en bloques"](#)

"PutBucketEncryption"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentación de StorageGRID

"[Operaciones en bloques](#)"

"PutBucketLifecycleConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

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

Documentación de StorageGRID

- "[Operaciones en bloques](#)"
- "[Cree una configuración del ciclo de vida de S3](#)"

"PutBucketNotificationConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

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

Documentación de StorageGRID

"Operaciones en bloques"

"Política de PutBucketPolicy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Para obtener detalles sobre los campos de cuerpo JSON admitidos, consulte "[Utilice las políticas de acceso de bloques y grupos](#)".

"PutBucketReplication"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Etiquetas XML de cuerpo de solicitud

- Bucket
- Destination
- Prefix
- ReplicationConfiguration

- Rule
- Status
- StorageClass

Documentación de StorageGRID

"Operaciones en bloques"

"PutBucketTagging"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

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

Documentación de StorageGRID

"Operaciones en bloques"

"PutBucketVersioning"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Parámetros de cuerpo de solicitud

StorageGRID admite los siguientes parámetros de cuerpo de solicitud:

- VersioningConfiguration
- Status

Documentación de StorageGRID

"Operaciones en bloques"

"Objeto de puta"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo [parámetros y cabeceras comunes](#) para esta solicitud, además de estos encabezados adicionales:

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

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

Solicitar el cuerpo

- Datos binarios del objeto

Documentación de StorageGRID

["Objeto de puta"](#)

"PutObjectLegalHold"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

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

Documentación de StorageGRID

["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)

"PutObjectLockConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

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

Documentación de StorageGRID

["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)

"PutObjectRetention"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todo [parámetros y cabeceras comunes](#) para esta solicitud, además de este encabezado adicional:

- x-amz-bypass-governance-retention

Solicitar el cuerpo

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

Documentación de StorageGRID

"[Use la API REST DE S3 para configurar el bloqueo de objetos de S3](#)"

"PutObjectEtiquetado"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

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

Documentación de StorageGRID

"[Operaciones en objetos](#)"

"RestoreObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

Para obtener más información sobre los campos de cuerpo admitidos, consulte "["RestoreObject"](#)".

"SelectObjectContent"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos [parámetros y cabeceras comunes](#) para esta solicitud.

Solicitar el cuerpo

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

- "[Utilice S3 Select](#)"
- "[SelectObjectContent](#)"

"UploadPart"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID soporta todos [parámetros y cabeceras comunes](#) para esta solicitud, además de estos parámetros de consulta URI adicionales:

- partNumber
- uploadId

Y estos encabezados de solicitud adicionales:

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

Solicitar el cuerpo

- Datos binarios de la pieza

Documentación de StorageGRID

["UploadPart"](#)

"UploadPartCopy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID soporta todos [parámetros y cabeceras comunes](#) para esta solicitud, además de estos parámetros de consulta URI adicionales:

- partNumber
- uploadId

Y estos encabezados de solicitud adicionales:

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

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

["UploadPartCopy"](#)

Probar la configuración de la API de REST S3

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

Antes de empezar

- Ha descargado e instalado la CLI de AWS desde "aws.amazon.com/cli".
- Opcionalmente, usted tiene "["se ha creado un punto final de equilibrio de carga"](#)". De lo contrario, conoce la dirección IP del nodo de almacenamiento al que desea conectarse y el número de puerto que se va a utilizar. Consulte "[Puertos y direcciones IP para las conexiones de cliente](#)".
- Tienes "["Se ha creado una cuenta de inquilino de S3"](#)".
- Ha iniciado sesión en el inquilino y "["se creó una clave de acceso"](#)".

Para obtener más información sobre estos pasos, consulte "["Configurar conexiones de cliente"](#)".

Pasos

1. Configure los ajustes de la CLI de AWS para usar la cuenta que creó en el sistema StorageGRID:
 - a. Acceda al modo de configuración: `aws configure`
 - b. Introduzca el ID de clave de acceso de la cuenta que creó.
 - c. Introduzca la clave de acceso secreta de la cuenta que creó.
 - d. Introduzca la región por defecto que se va a utilizar. Por ejemplo, `us-east-1`.
 - e. Introduzca el formato de salida predeterminado que se va a utilizar o pulse **Intro** para seleccionar JSON.
2. Crear un bucket.

En este ejemplo se supone que ha configurado un punto final de equilibrio de carga para utilizar la dirección IP 10.96.101.17 y el puerto 10443.

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

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

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

3. Cargue un objeto.

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

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

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

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

5. Elimine el objeto.

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

6. Eliminar el bloque.

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

Cómo StorageGRID implementa la API DE REST de S3

Solicitudes de clientes en conflicto

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias".

El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Coherencia

La consistencia proporciona un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios. Puede cambiar la consistencia según lo requiera la aplicación.

De forma predeterminada, StorageGRID garantiza la consistencia de lectura tras escritura para los objetos recién creados. Cualquier operación GET posterior a una operación PUT completada con éxito podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, las actualizaciones de metadatos y las eliminaciones son eventualmente consistentes.

Si desea realizar operaciones de objeto en otra coherencia, puede:

- Especificar una consistencia para [cada cucharón](#) .
- Especifique una consistencia para [Cada operación de API](#).
- Cambie la consistencia predeterminada en toda la cuadrícula realizando una de las siguientes tareas:
 - En el Administrador de cuadrícula, vaya a **Configuración > Sistema > Configuración de almacenamiento > Consistencia del depósito predeterminado**.
 - .



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

Valores de coherencia

La consistencia afecta cómo se distribuyen los metadatos que StorageGRID utiliza para rastrear objetos entre los nodos. La consistencia afecta la disponibilidad de los objetos para las solicitudes del cliente.

Puede establecer la coherencia de un bloque o una operación de API en uno de los valores siguientes:

- **Todos:** Todos los nodos reciben metadatos de objeto inmediatamente o la solicitud fallará.
- **Strong-global:** garantiza la consistencia de lectura después de escritura para todas las solicitudes de clientes en todos los sitios. Cuando se configura la semántica de quórum, se aplican los siguientes comportamientos:
 - Permite la tolerancia a fallas del sitio para las solicitudes de los clientes cuando las redes tienen tres o más sitios. Las redes de dos sitios no tendrán tolerancia a fallas del sitio.
 - Las siguientes operaciones S3 no tendrán éxito si un sitio está inactivo:
 - DeleteBucketEncryption
 - PonerBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Si es necesario, puedes ["Configurar la semántica de quórum de StorageGRID para lograr una consistencia global sólida"](#).

- **Strong-site:** Los metadatos de objetos se distribuyen inmediatamente a otros nodos en el sitio. Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
- **Read-after-new-write:** Proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
- **Disponible:** Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Utilice los elementos de consistencia «Read-after-new-write» y «available»

Cuando una operación de CABEZAL u OBTENCIÓN utiliza la consistencia de lectura después de nueva escritura, StorageGRID realiza la búsqueda en varios pasos de la siguiente manera:

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

Si una operación HEAD u GET utiliza la coherencia «Read-after-new-write» pero el objeto no existe, la búsqueda de objetos siempre alcanzará una coherencia equivalente al comportamiento de un nivel global sólido. Debido a que esta consistencia requiere que haya disponibles varias copias de los metadatos del objeto en cada sitio, puede recibir un número elevado de errores de servidor interno 500 si hay dos o más nodos de almacenamiento en el mismo sitio disponibles.

A menos que necesite garantías de consistencia similares a Amazon S3, puede evitar estos errores para las operaciones HEAD y GET estableciendo la consistencia en “Disponible”. Cuando una operación de CABEZAL u OBTENCIÓN utiliza la consistencia «disponible», StorageGRID solo proporciona consistencia eventual. No vuelve a intentar una operación fallida en el aumento de la coherencia, por lo que no es necesario que haya varias copias de los metadatos del objeto disponibles.

Especifique la consistencia para el funcionamiento de la API

Para configurar la coherencia de una operación de API individual, los valores de coherencia deben ser compatibles con la operación y debe especificar la coherencia en el encabezado de solicitud. Este ejemplo establece la coherencia en «sitio fuerte» para una operación GetObject.

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



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

Especificación de la consistencia para el depósito

Para configurar la coherencia del bloque, puede usar la solicitud StorageGRID "[PONGA la consistencia del cucharón](#)". O puede "[cambiar la consistencia de un cucharón](#)" hacerlo desde el Administrador de inquilinos.

Al establecer la coherencia de un cucharón, tenga en cuenta lo siguiente:

- La configuración de la coherencia de un bloque determina la coherencia que se usa para las operaciones S3 realizadas en los objetos del bloque o en la configuración de bloque. No afecta a las operaciones del propio cucharón.
- La coherencia de una operación API individual anula la coherencia del bloque.
- En general, los bloques deben utilizar la consistencia predeterminada «Read-after-new-write». Si las solicitudes no funcionan correctamente, cambie el comportamiento del cliente de aplicación si es posible. O bien, configure el cliente para especificar la consistencia de cada solicitud API. Defina la consistencia en el nivel del cucharón sólo como último recurso.

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

Tanto la elección de coherencia como la regla de ILM afectan al modo de protección de los objetos. Estos ajustes pueden interactuar.

Por ejemplo, la consistencia utilizada cuando se almacena un objeto afecta la ubicación inicial de los metadatos del objeto, mientras que el comportamiento de procesamiento seleccionado para la regla de ILM afecta la ubicación inicial de las copias de objetos. Dado que StorageGRID requiere acceso a los metadatos de un objeto y a sus datos para satisfacer las solicitudes de los clientes, seleccionar niveles de protección

correspondientes para la coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas del sistema más predecibles.

Los siguientes "opciones de procesamiento" se encuentran disponibles para las reglas de ILM:

Registro doble

StorageGRID realiza de inmediato copias provisionales del objeto y devuelve la operación correcta al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Estricto

Todas las copias especificadas en la regla de ILM deben realizarse antes de devolver correctamente al cliente.

Equilibrado

StorageGRID intenta realizar todas las copias especificadas en la regla de gestión del ciclo de vida de la información durante el procesamiento; si no es posible, se realizarán copias provisionales y se devolverán correctamente al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Ejemplo de cómo pueden interactuar la regla de consistencia e ILM

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

- **Regla ILM:** Crear tres copias de objetos, una en el sitio local y una en cada sitio remoto. Utilice el comportamiento de ingesta estricto.
- **Consistencia:** Fuerte-global (los metadatos del objeto se distribuyen inmediatamente a múltiples sitios).

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

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

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

La interrelación entre las reglas de coherencia y de ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Control de versiones de objetos

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

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

El control de versiones de objetos puede combinarse con la gestión del ciclo de vida de la información (ILM)

de StorageGRID o con la configuración del ciclo de vida de bloques de S3. Debe activar el control de versiones de forma explícita para cada bloque. Cuando se habilita el control de versiones para un bloque, a cada objeto agregado al bloque se le asigna un ID de versión, que genera el sistema StorageGRID.

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



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

ILM y versiones

Las políticas de ILM se aplican a cada versión de un objeto. Un proceso de análisis de ILM analiza continuamente todos los objetos y los vuelve a evaluar en relación con la política actual de ILM. Todos los cambios realizados en las políticas de ILM se aplican a todos los objetos procesados anteriormente. Esto incluye versiones que se han ingerido previamente si la versión está activada. El análisis de ILM aplica nuevos cambios de ILM a los objetos procesados previamente.

Para los objetos S3 en bloques con control de versiones, el soporte de control de versiones le permite crear reglas de ILM que utilicen 'Tiempo no corriente' como Tiempo de referencia (seleccione **Sí** para la pregunta, '¿Aplicar esta regla solo a versiones de objetos anteriores?' en "[Paso 1 del asistente Crear una regla de ILM](#)"). Cuando se actualiza un objeto, sus versiones anteriores se vuelven no actuales. El uso de un filtro de tiempo no corriente permite crear políticas que reduzcan el impacto en el almacenamiento de las versiones anteriores de objetos.



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

Información relacionada

- ["Cómo se eliminan los objetos con versiones de S3"](#)
- ["Reglas de ILM y políticas para objetos con versiones de S3 \(ejemplo 4\)"](#).

Use la API REST DE S3 para configurar el bloqueo de objetos de S3

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

Cómo habilitar S3 Object Lock para un bucket

Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, también puede habilitar el bloqueo de objetos S3 al crear cada bloque.

S3 Bloqueo de objetos es un ajuste permanente que solo se puede activar cuando se crea un depósito. No puede agregar o deshabilitar S3 Object Lock después de crear un bucket.

Para activar el bloqueo de objetos S3 para un depósito, utilice uno de estos métodos:

- Cree el bloque con el Administrador de arrendatarios. Consulte "[Crear bloque de S3](#)".

- Cree el depósito mediante una solicitud CreateBucket con la `x-amz-bucket-object-lock-enabled` cabecera de solicitud. Consulte ["Operaciones en bloques"](#).

S3 Object Lock requiere el control de versiones de bloque, que se habilita automáticamente cuando se crea el bloque. No puede suspender el control de versiones del depósito. Consulte ["Control de versiones de objetos"](#).

Configuración de retención predeterminada para un bloque

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

Modo de retención predeterminado

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

Período de retención predeterminado

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

Cómo establecer la retención predeterminada para un depósito

Para definir la retención predeterminada de un depósito, utilice uno de estos métodos:

- Gestione la configuración de bloques desde el Gestor de inquilinos. Consulte ["Cree un bloque de S3"](#) y ["Actualizar S3 Retención predeterminada de bloqueo de objetos"](#).
- Emite una solicitud PutObjectLockConfiguration para el depósito para especificar el modo por defecto y el número por defecto de días o años.

PutObjectLockConfiguration

La solicitud PutObjectLockConfiguration le permite establecer y modificar el modo de retención predeterminado y el período de retención predeterminado para un depósito que tiene S3 Object Lock activado. También es posible eliminar los ajustes de retención predeterminados previamente configurados.

Cuando se ingieren nuevas versiones de objetos en el depósito, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` no se especifican y `x-amz-object-lock-retain-until-date`. El período de retención por defecto se utiliza para calcular la fecha de retención hasta si `x-amz-object-lock-retain-until-date` no se especifica.

Si el período de retención predeterminado se modifica tras recibir una versión de objeto, la fecha de retención hasta la de la versión del objeto sigue siendo la misma y no se vuelve a calcular con el nuevo período de

retención predeterminado.

Debe tener `s3:PutBucketObjectLockConfiguration` el permiso, o ser account root, para completar esta operación.

`Content-MD5` La cabecera de solicitud se debe especificar en la solicitud de VENTA.

Ejemplo de solicitud

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

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

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

Cómo determinar la retención predeterminada de un depósito

Para determinar si S3 Object Lock está activado para un depósito y para ver el modo de retención y el período de retención predeterminados, utilice uno de estos métodos:

- Ver el depósito en el Gestor de inquilinos. Consulte "[Ver S3 cubos](#)".
- Emitir una solicitud `GetObjectLockConfiguration`.

GetObjectLockConfiguration

La solicitud `GetObjectLockConfiguration` le permite determinar si el bloqueo de objetos S3 está habilitado para un depósito y, si está activado, consulte si hay un modo de retención predeterminado y un período de retención configurado para el depósito.

Cuando se ingieren nuevas versiones de objetos en el depósito, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` no se especifica. El período de retención por defecto se utiliza para calcular la fecha de retención hasta si `x-amz-object-lock-retain-until-date` no se especifica.

Debe tener `s3:GetBucketObjectLockConfiguration` el permiso, o ser account root, para completar esta operación.

Ejemplo de solicitud

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

Ejemplo de respuesta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB70XXJRkRH1Fivq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

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

Cómo especificar la configuración de retención para un objeto

Un bucket con S3 Object Lock habilitado puede contener una combinación de objetos con y sin la configuración de retención de S3 Object Lock.

La configuración de retención en el nivel de objeto se especifica mediante la API DE REST S3. La configuración de retención de un objeto anula cualquier configuración de retención predeterminada del bloque.

Puede especificar los siguientes ajustes para cada objeto:

- **Modo de retención:** Ya sea CUMPLIMIENTO o GOBIERNO.
- **Retain-until-date:** Una fecha que especifica cuánto tiempo la versión del objeto debe ser retenida por StorageGRID.
 - En el modo de CUMPLIMIENTO DE NORMATIVAS, si la fecha de retención hasta la fecha es posterior, el objeto se puede recuperar, pero no se puede modificar ni eliminar. Se puede aumentar la fecha de retención hasta la fecha, pero esta fecha no se puede reducir ni eliminar.
 - En el modo de GOBIERNO, los usuarios con permiso especial pueden omitir la configuración Retener hasta la fecha. Pueden eliminar una versión de objeto antes de que haya transcurrido su período de retención. También pueden aumentar, disminuir o incluso eliminar la fecha de retención hasta la fecha.
- **Retención legal:** La aplicación de una retención legal a una versión de objeto bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesite poner una retención legal en un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, pero permanece en su lugar hasta que se elimina explícitamente.

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

Para especificar la configuración de bloqueo de objetos S3 al agregar una versión de objeto a un depósito, emita una "["Objeto de puta"](#)" "["CopyObject"](#)", o "["CreateMultipartUpload"](#)" una solicitud.

Puede utilizar lo siguiente:

- **x-amz-object-lock-mode**, Que puede ser CUMPLIMIENTO o GOBERNANZA (distingue entre mayúsculas y minúsculas).
-  Si especifica **x-amz-object-lock-mode**, también debe especificar **x-amz-object-lock-retain-until-date**.
- **x-amz-object-lock-retain-until-date**
 - El valor **Retain-until-date** debe tener el formato 2020-08-10T21:46:00Z. Se permiten segundos fraccionarios, pero sólo se conservan 3 dígitos decimales (precisión de milisegundos). No se permiten otros formatos ISO 8601.
 - La fecha de retención debe ser futura.
 - **x-amz-object-lock-legal-hold**

Si la conservación legal está ACTIVADA (distingue entre mayúsculas y minúsculas), el objeto se colocará bajo una retención legal. Si se HA DESACTIVADO la retención legal, no se ha colocado ningún tipo de retención legal. Cualquier otro valor produce un error 400 Bad Request (InvalidArgumentException).

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

- **Content-MD5** La cabecera de solicitud es necesaria si hay alguna **x-amz-object-lock-*** cabecera de solicitud presente en la solicitud PutObject. **Content-MD5** No es necesario para **CopyObject** o **CreateMultipartUpload**.

- Si el depósito no tiene S3 Object Lock activado y hay un `x-amz-object-lock-*` encabezado de solicitud, se devuelve un error de 400 Bad Request (InvalidRequest).
- La solicitud PutObject admite el uso de `x-amz-storage-class: REDUCED_REDUNDANCY` para que coincida con el comportamiento de AWS. Sin embargo, cuando un objeto se procesa en un bucket con el bloqueo de objetos S3 habilitado, StorageGRID siempre ejecuta un procesamiento de compromiso doble.
- Una respuesta posterior a la versión GET o HeadObject incluirá las cabeceras `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date` y `x-amz-object-lock-legal-hold`, si está configurada y si el remitente de la solicitud tiene los permisos correctos `s3:Get*`.

Puede utilizar `s3:object-lock-remaining-retention-days` la clave de condición de política para limitar los períodos de retención mínimos y máximos permitidos para los objetos.

Cómo actualizar la configuración de retención de un objeto

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

- `PutObjectLegalHold`

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

- `PutObjectRetention`

- El valor de modo puede ser CUMPLIMIENTO o GOBIERNO (distingue entre mayúsculas y minúsculas).
- El valor Retain-until-date debe tener el formato `2020-08-10T21:46:00Z`. Se permiten segundos fraccionarios, pero sólo se conservan 3 dígitos decimales (precisión de milisegundos). No se permiten otros formatos ISO 8601.
- Si una versión de objeto tiene una fecha de retención existente, sólo puede aumentarla. El nuevo valor debe ser el futuro.

Cómo utilizar el modo de GOBIERNO

Los usuarios que tienen el `s3:BypassGovernanceRetention` permiso pueden omitir la configuración de retención activa de un objeto que utiliza el modo de GOBIERNO. Cualquier operación DELETE u `PutObjectRetention` debe incluir la `x-amz-bypass-governance-retention:true` cabecera de solicitud. Estos usuarios pueden realizar las siguientes operaciones adicionales:

- Realice las operaciones `DeleteObject` o `DeleteObjects` para eliminar una versión de objeto antes de que haya transcurrido su período de retención.

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

- Realice operaciones `PutObjectRetention` que cambian el modo de una versión de objeto de GOBIERNO a CUMPLIMIENTO antes de que haya transcurrido el período de retención del objeto.

Cambiar el modo de CUMPLIMIENTO a GOBIERNO nunca está permitido.

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

Información relacionada

- ["Gestione objetos con S3 Object Lock"](#)
- ["Utilice Bloqueo de objetos S3 para retener objetos"](#)
- ["Guía del usuario de Amazon Simple Storage Service: Bloqueo de objetos"](#)

Cree una configuración del ciclo de vida de S3

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

El ejemplo sencillo de esta sección muestra cómo puede controlar una configuración del ciclo de vida de S3 cuando se eliminan ciertos objetos (caducados) de bloques S3 específicos. El ejemplo de esta sección es solo con fines ilustrativos. Para obtener información detallada sobre la creación de configuraciones del ciclo de vida S3, consulte ["Guía del usuario de Amazon Simple Storage Service: Gestión del ciclo de vida de los objetos"](#). Tenga en cuenta que StorageGRID solo admite acciones de caducidad, no admite acciones de transición.

Qué es la configuración del ciclo de vida

Una configuración de ciclo de vida es un conjunto de reglas que se aplican a los objetos en bloques de S3 específicos. Cada regla especifica qué objetos se ven afectados y cuándo caducarán dichos objetos (en una fecha específica o después de un número determinado de días).

StorageGRID admite hasta 1,000 reglas de ciclo de vida en una configuración del ciclo de vida. Cada regla puede incluir los siguientes elementos XML:

- Caducidad: Elimine un objeto cuando se alcance una fecha especificada o cuando se alcance un número especificado de días, empezando desde el momento en que se ingirió el objeto.
- NoncurrentVersionExpiration: Elimine un objeto cuando se alcance un número especificado de días, empezando desde el momento en que el objeto se volvió no actual.
- Filtro (prefijo, etiqueta)
- Estado
- ID

Cada objeto sigue la configuración de retención de un ciclo de vida de bloques de S3 o una política de ILM. Cuando se configura el ciclo de vida de un bloque de S3, las acciones de caducidad del ciclo de vida anulan la política de ILM de los objetos que coinciden con el filtro de ciclo de vida del bloque. Los objetos que no coinciden con el filtro de ciclo de vida del bloque utilizan la configuración de retención de la política de ILM. Si un objeto coincide con un filtro de ciclo de vida del bloque y no se especifica ninguna acción de caducidad explícitamente, no se utiliza la configuración de retención de la política de ILM y se implica que las versiones de los objetos se retienen permanentemente. Consulte ["Ejemplo de prioridades del ciclo de vida del bloque de S3 y de una política de ILM"](#).

Como resultado, es posible que se elimine un objeto de la cuadrícula aunque las instrucciones de colocación de una regla de ILM aún se apliquen al objeto. O bien, es posible que un objeto se conserve en la cuadrícula incluso después de que hayan transcurrido las instrucciones de colocación de ILM para el objeto. Para obtener más información, consulte ["Cómo funciona ILM durante la vida de un objeto"](#).



La configuración del ciclo de vida de bloques se puede usar con bloques que tienen habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida de bloques no se admite para bloques compatibles con versiones anteriores.

StorageGRID admite el uso de las siguientes operaciones de bloques para gestionar las configuraciones del ciclo de vida:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Cree la configuración del ciclo de vida

Como primer paso en la creación de una configuración de ciclo de vida, se crea un archivo JSON que incluye una o varias reglas. Por ejemplo, este archivo JSON incluye tres reglas, de la siguiente manera:

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



Las reglas que especifican un número de días son relativas al momento en que se ingirió el objeto. Si la fecha actual supera la fecha de ingestión más el número de días, es posible que algunos objetos se eliminen del bloque en cuanto se aplique la configuración del ciclo de vida.

3. La regla 3 se aplica sólo a los objetos que coinciden con el prefijo `category3/`. `Expiration`El parámetro especifica que todas las versiones no corrientes de los objetos coincidentes caducarán 50 días después de que dejen de ser actuales.

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

Aplicar la configuración del ciclo de vida al bloque

Después de crear el archivo de configuración de ciclo de vida, se aplica a un depósito emitiendo una solicitud PutBucketLifecycleConfiguration.

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

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

Para validar que una configuración del ciclo de vida se ha aplicado correctamente al bloque, emita una solicitud GetBucketLifecycleConfiguration. Por ejemplo:

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

Una respuesta correcta muestra la configuración del ciclo de vida que acaba de aplicar.

Validar que la caducidad del ciclo de vida del bloque se aplica al objeto

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



Como el ciclo de vida del bloque anula el ciclo de vida de la información, la `expiry-date` que se muestra es la fecha real que se eliminará el objeto. Para obtener más información, consulte ["Cómo se determina la retención de objetos"](#).

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

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

La respuesta correcta indica que el objeto caducará en 100 días (01 de octubre de 2020) y que coincide con la regla 2 de la configuración del ciclo de vida.

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

Por ejemplo, esta solicitud HeadObject se ha utilizado para obtener metadatos para el mismo objeto en el cubo de testbucket.

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

La respuesta correcta incluye los metadatos del objeto e indica que el objeto caducará en 100 días y que coincide con la regla 2.

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



Para los bloques con control de versiones activado, `x-amz-expiration` la cabecera de respuesta sólo se aplica a las versiones actuales de los objetos.

Recomendaciones para implementar la API REST de S3

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

Recomendaciones para las cabezas a los objetos no existentes

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

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

Puede establecer la consistencia «disponible» para cada depósito mediante ["PONGA la consistencia del](#)

cucharón" la solicitud o puede especificar la coherencia en el encabezado de solicitud para una operación de API individual.

Recomendaciones para las claves de objeto

Siga estas recomendaciones para los nombres de clave del objeto, según cuándo se creó el bloque por primera vez.

Bloques creados en StorageGRID 11,4 o versiones anteriores

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

`mybucket/mydir/f8e3-image3132.jpg`

En lugar de este formato:

`mybucket/f8e3-image3132.jpg`

Bloques creados en StorageGRID 11,4 o versiones posteriores

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

Una excepción a esto es una carga de trabajo S3 que elimina continuamente todos los objetos después de un breve periodo de tiempo. Para minimizar el impacto en el rendimiento de este caso de uso, varíe una parte inicial del nombre de la clave cada varios miles de objetos con algo similar a la fecha. Por ejemplo, suponga que un cliente S3 normalmente escribe 2.000 objetos por segundo y la política de ciclo de vida de la gestión de la vida útil de la información o del bloque elimina los objetos al cabo de tres días. Para minimizar el impacto en el rendimiento, puede asignar un nombre a las claves utilizando un patrón como el siguiente:
`/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Recomendaciones para lecturas de rango

Si "opción global para comprimir objetos almacenados" está activado, las aplicaciones cliente S3 deben evitar realizar operaciones GetObject que especifiquen un rango de bytes. Estas operaciones de «lectura de rango» son ineficientes, puesto que StorageGRID debe descomprimir los objetos de forma efectiva para acceder a los bytes solicitados. Las operaciones GetObject que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, no es eficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden tener un tiempo de espera.

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

Soporte para la API de REST DE Amazon S3

S3 Detalles de implementación de la API de REST

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

El sistema StorageGRID admite tanto solicitudes virtuales de tipo hospedado como solicitudes de tipo path.

Gestión de fechas

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

El sistema StorageGRID sólo admite formatos de fecha HTTP válidos para cualquier encabezado que acepte valores de fecha. La parte horaria de la fecha puede especificarse en formato de hora media de Greenwich (GMT) o en formato de hora universal coordinada (UTC) sin desplazamiento de zona horaria (se debe especificar +0000). Si incluye `x-amz-date` la cabecera en la solicitud, sustituye cualquier valor especificado en la cabecera de solicitud Fecha. Cuando se utiliza la versión 4 de firma de AWS, el `x-amz-date` encabezado debe estar presente en la solicitud firmada porque no se admite el encabezado de fecha.

Encabezados de solicitud comunes

El sistema StorageGRID soporta las cabeceras de solicitud comunes definidas por "[Referencia de API de Amazon Simple Storage Service: Encabezados de solicitud comunes](#)", con una excepción.

Solicite el encabezado	Implementación
Autorización	Compatibilidad completa con la firma AWS Versión 2 Compatibilidad con la versión 4 de la firma de AWS, con las siguientes excepciones: <ul style="list-style-type: none">Al proporcionar el valor de suma de comprobación de carga útil real en <code>x-amz-content-sha256</code>, el valor se acepta sin validación, como si se hubiera proporcionado el valor <code>UNSIGNED-PAYLOAD</code> para la cabecera. Cuando se proporciona un <code>x-amz-content-sha256</code> valor de encabezado que implica <code>aws-chunked</code> la transmisión (por ejemplo, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), las firmas de fragmento no se verifican contra los datos del fragmento.

Encabezados de respuesta comunes

El sistema StorageGRID admite todos los encabezados de respuesta comunes definidos por *simple Storage Service API Reference*, con una excepción.

Encabezado de respuesta	Implementación
<code>x-amz-id-2</code>	No se utiliza

Autenticar solicitudes

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

La API S3 admite la versión 2 de Signature y la versión 4 de Signature para autenticar solicitudes de API S3.

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

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

Utilice el encabezado autorización HTTP

El encabezado HTTP `Authorization` es utilizado por todas las operaciones de la API S3 excepto las solicitudes anónimas cuando lo permite la política de bloque. 'Authorization' El encabezado contiene toda la información de firma necesaria para autenticar una solicitud.

Utilice los parámetros de consulta

Puede utilizar parámetros de consulta para agregar información de autenticación a una URL. Esto se conoce como firma previa de la dirección URL, que se puede utilizar para otorgar acceso temporal a recursos específicos. Los usuarios con la URL prefirmada no necesitan conocer la clave de acceso secreta para acceder al recurso, lo que permite proporcionar acceso restringido de terceros a un recurso.

Operaciones en el servicio

El sistema StorageGRID admite las siguientes operaciones en el servicio.

Funcionamiento	Implementación
ListCuchers (Anteriormente llamado GET Service)	Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones.
Obtenga el uso del almacenamiento	La solicitud StorageGRID " Obtenga el uso del almacenamiento " le indica la cantidad total de almacenamiento que utiliza una cuenta y de cada bloque asociado a la cuenta. Se trata de una operación en el servicio con una ruta de acceso de / y un parámetro de consulta personalizado (?x-ntap-sg-usage) agregada.
OPCIONES /	Las aplicaciones cliente pueden emitir OPTIONS / solicitudes al puerto S3 de un nodo de almacenamiento, sin proporcionar credenciales de autenticación S3, para determinar si el nodo de almacenamiento está disponible. Puede usar esta solicitud para supervisar o para permitir que los equilibradores de carga externos identifiquen cuando un nodo de almacenamiento esté inactivo.

Operaciones en bloques

El sistema StorageGRID admite un máximo de 5,000 bloques para cada cuenta de inquilino de S3.

Cada rejilla puede tener un máximo de 100.000 cubos.

Para admitir 5.000 buckets, cada nodo de almacenamiento del grid debe tener un mínimo de 64 GB de RAM.

Las restricciones de nombre de bloque siguen las restricciones de región estándar de AWS EE.UU., pero debe restringirlas a las convenciones de nomenclatura DNS para admitir solicitudes virtuales de estilo hospedado de S3.

En la siguiente sección, se ofrece más información:

- ["Guía del usuario de Amazon Simple Storage Service: Cuotas de buckets, restricciones y limitaciones"](#)
- ["Configure los nombres de dominio de punto final S3"](#)

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

Puede comprobar si las actualizaciones a la hora del último acceso están habilitadas o deshabilitadas para grupos individuales. Consulte ["GET Bucket última hora de acceso"](#).

En la siguiente tabla se describe cómo StorageGRID implementa operaciones de bloque de API DE REST de S3. Para realizar alguna de estas operaciones, se deben proporcionar las credenciales de acceso necesarias para la cuenta.

Funcionamiento	Implementación
CreateBucket	<p>Crea un nuevo cucharón. Al crear la cuchara, se convierte en el propietario de la cuchara.</p> <ul style="list-style-type: none"> Los nombres de los bloques deben cumplir con las siguientes reglas: <ul style="list-style-type: none"> Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino). Debe ser compatible con DNS. Debe contener al menos 3 y no más de 63 caracteres. Puede ser una serie de una o más etiquetas, con etiquetas adyacentes separadas por un punto. Cada etiqueta debe comenzar y terminar con una letra minúscula o un número y solo puede utilizar letras minúsculas, números y guiones. No debe ser una dirección IP con formato de texto. No debe utilizar períodos en solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor. Por defecto, los cubos se crean en la <code>us-east-1</code> región; sin embargo, puede utilizar el <code>LocationConstraint</code> elemento de solicitud en el cuerpo de la solicitud para especificar una región diferente. Al utilizar el <code>LocationConstraint</code> elemento, debe especificar el nombre exacto de una región que se ha definido mediante Grid Manager o la API de gestión de grid. Póngase en contacto con el administrador del sistema si no conoce el nombre de región que debe utilizar. <p>Nota: Se producirá un error si su solicitud de CreateBucket utiliza una región que no se ha definido en StorageGRID.</p> <ul style="list-style-type: none"> Puede incluir <code>x-amz-bucket-object-lock-enabled</code> el encabezado de solicitud para crear un depósito con S3 Object Lock activado. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3". <p>Debe habilitar S3 Object Lock cuando crea el bloque. No puede agregar o deshabilitar S3 Object Lock después de crear un bucket. S3 Object Lock requiere el control de versiones de bloques, que se habilita automáticamente al crear el bloque.</p>
DeleteBucket	Elimina el cucharón.
DeleteBucketCors	Elimina la configuración de CORS para el cucharón.
DeleteBucketEncryption	Elimina el cifrado predeterminado del depósito. Los objetos cifrados existentes permanecen cifrados, pero todos los objetos nuevos agregados al depósito no están cifrados.
DeleteBucketLifecycle	Elimina la configuración del ciclo de vida del depósito. Consulte " Cree una configuración del ciclo de vida de S3 ".

Funcionamiento	Implementación
DeleteBucketPolicy	Suprime la política asociada al depósito.
DeleteBucketReplication	Suprime la configuración de replicación asociada al depósito.
DeleteBucketTagging	Utiliza el <code>tagging</code> subrecurso para eliminar todas las etiquetas de un depósito. Precaución: Si se establece una etiqueta de política de ILM no predeterminada para este cubo, habrá una <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de cubo con un valor asignado. No emita una solicitud <code>DeleteBucketTagging</code> si hay una <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de depósito. En su lugar, emita una solicitud <code>PutBucketTagging</code> con solo la <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta y su valor asignado para eliminar todas las demás etiquetas del depósito. No modifique ni elimine la <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta del depósito.
GetBucketAcl	Devuelve una respuesta positiva y el ID, DisplayName y el permiso del propietario del depósito, lo que indica que el propietario tiene acceso completo al depósito.
GetBucketCors	Devuelve la <code>cors</code> configuración del cucharón.
GetBucketEncryption	Devuelve la configuración de cifrado predeterminada para el depósito.
GetBucketLifecycleConfiguration (Anteriormente llamado GET Bucket Lifecycle)	Devuelve la configuración del ciclo de vida del cucharón. Consulte " Cree una configuración del ciclo de vida de S3 ".
GetBucketLocation	Devuelve la región que se estableció utilizando el <code>LocationConstraint</code> elemento en la solicitud <code>CreateBucket</code> . Si la región del bloque es <code>us-east-1</code> , se devuelve una cadena vacía para la región.
GetBucketNotificationConfiguration (Anteriormente denominado notificación GET Bucket)	Devuelve la configuración de notificación adjunta al depósito.
GetBucketPolicy	Devuelve la política adjunta al depósito.
GetBucketReplication	Devuelve la configuración de replicación asociada al bloque.

Funcionamiento	Implementación
Etiquetado de GetBucketTagging	<p>Utiliza tagging el subrecurso para devolver todas las etiquetas de un depósito.</p> <p>Precaución: Si se establece una etiqueta de política de ILM no predeterminada para este cubo, habrá una NTAP-SG-ILM-BUCKET-TAG etiqueta de cubo con un valor asignado. No modifique ni elimine esta etiqueta.</p>
GetBucketVersioning	<p>Esta implantación utiliza el versioning subrecurso para devolver el estado de control de versiones de un depósito.</p> <ul style="list-style-type: none"> • <i>BLANK</i>: El control de versiones nunca se ha activado (el bloque no está versionado) • Activado: El control de versiones está activado • Suspendido: El control de versiones se ha habilitado anteriormente y se ha suspendido
GetObjectLockConfiguration	<p>Devuelve el modo de retención predeterminado del depósito y el período de retención predeterminado, si está configurado.</p> <p>Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".</p>
Segmento de cabeza	<p>Determina si existe un bloque y tiene permiso para acceder a él.</p> <p>Esta operación devuelve:</p> <ul style="list-style-type: none"> • <i>x-ntap-sg-bucket-id</i>: El UUID del bucket en formato UUID. • <i>x-ntap-sg-trace-id</i>: El identificador de rastreo único de la solicitud asociada.

Funcionamiento	Implementación
ListObjects y ListObjectsV2 (Anteriormente denominado GET Bucket)	<p>Devuelve algunos o todos (hasta 1.000) de los objetos de un cubo. La clase de almacenamiento para los objetos puede tener cualquiera de dos valores, incluso si el objeto se ingirió con REDUCED_REDUNDANCY la opción de clase storage:</p> <ul style="list-style-type: none"> • STANDARD, Que indica que el objeto se almacena en un pool de almacenamiento que consta de nodos de almacenamiento. • GLACIER, Que indica que el objeto se ha movido al depósito externo especificado por Cloud Storage Pool. <p>Si el depósito contiene un gran número de claves eliminadas que tienen el mismo prefijo, la respuesta puede incluir algunas CommonPrefixes que no contienen claves.</p> <p>Para las solicitudes HeadObject y ListObject, StorageGRID devuelve las marcas de tiempo de LastModified con diferente precisión, mientras que AWS devuelve las marcas de tiempo con la misma precisión, como se muestra en los siguientes ejemplos:</p> <ul style="list-style-type: none"> • Objeto principal de StorageGRID : "Última modificación": "2024-09-26T16:43:24+00:00" • Objeto de lista StorageGRID : "Última modificación": "2024-09-26T16:43:24.931000+00:00" • Objeto principal de AWS: "Última modificación": "2023-10-17T00:19:54+00:00" • AWS ListObject: "Última modificación": "2023-10-17T00:19:54+00:00"
ListObjectVersions (Versiones de objeto GET Bucket con nombre anterior)	Con acceso DE LECTURA en un bloque, mediante esta operación con versions el subrecurso, se enumeran los metadatos de todas las versiones de objetos del bloque.
A cargo de PutBucketCors	Establece la configuración de CORS para un depósito para que éste pueda atender solicitudes de origen cruzado. El uso compartido de recursos de origen cruzado (CORS) es un mecanismo de seguridad que permite a las aplicaciones web de cliente de un dominio acceder a los recursos de un dominio diferente. Por ejemplo, supongamos que utiliza un depósito S3 denominado images para almacenar gráficos. Al establecer la configuración de CORS para el images depósito, puede permitir que las imágenes de ese depósito se muestren en el sitio web http://www.example.com .

Funcionamiento	Implementación
PutBucketEncryption	<p>Establece el estado de cifrado predeterminado de un depósito existente. Cuando se habilita el cifrado a nivel de bloque, se cifran todos los objetos nuevos que se añadan al bloque. StorageGRID admite el cifrado en el lado del servidor con claves gestionadas por StorageGRID. Al especificar la regla de configuración de cifrado del servidor, establezca el SSEAlgorithm parámetro en AES256 y no utilice el KMSMasterKeyID parámetro.</p> <p>La configuración de cifrado por defecto de bucket se ignora si la solicitud de carga de objeto ya especifica el cifrado (es decir, si la solicitud incluye el x-amz-server-side-encryption-* encabezado de solicitud).</p>
<p>PutBucketLifecycleConfiguration (Anteriormente llamado PUT Bucket Lifecycle)</p>	<p>Crea una nueva configuración de ciclo de vida para el bloque o sustituye a una configuración de ciclo de vida existente. StorageGRID admite hasta 1,000 reglas de ciclo de vida en una configuración del ciclo de vida. Cada regla puede incluir los siguientes elementos XML:</p> <ul style="list-style-type: none"> • Caducidad (días, fecha, ExpiredObjectDeleteMarker) • Caducidad de versiones sin corriente (NewerNoncurrentVersions, NoncurrentDays) • Filtro (prefijo, etiqueta) • Estado • ID <p>StorageGRID no admite estas acciones:</p> <ul style="list-style-type: none"> • AbortIncompleteMultipartUpload • Transición <p>Consulte "Cree una configuración del ciclo de vida de S3". Para comprender cómo la acción de caducidad en un ciclo de vida de un depósito interactúa con las instrucciones de ubicación de ILM, consulte "Cómo funciona ILM a lo largo de la vida de un objeto".</p> <p>Nota: La configuración del ciclo de vida de la cuchara se puede utilizar con cucharones que tengan habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida de la cuchara no es compatible con cucharones legados compatibles.</p>

Funcionamiento	Implementación
PutBucketNotificationConfiguration (Anteriormente denominado notificación PUT Bucket)	<p>Configura las notificaciones para el depósito mediante el XML de configuración de notificación incluido en el cuerpo de la solicitud. Debe tener en cuenta los siguientes detalles de implementación:</p> <ul style="list-style-type: none"> StorageGRID admite temas de Amazon Simple Notification Service (Amazon SNS), temas de Kafka o puntos finales de webhook como destinos. No se admiten los puntos finales de Simple Queue Service (SQS) ni de AWS Lambda. El destino de las notificaciones debe especificarse como URN de un extremo de StorageGRID. Se pueden crear extremos con el administrador de inquilinos o la API de gestión de inquilinos. <p>El extremo debe existir para que la configuración de la notificación se realice correctamente. Si el punto final no existe, se devuelve un 400 Bad Request error con el código InvalidArgument.</p> <ul style="list-style-type: none"> No puede configurar una notificación para los siguientes tipos de evento. Estos tipos de evento no son compatibles. <ul style="list-style-type: none"> s3:ReducedRedundancyLostObject s3:ObjectRestore:Completed Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar, excepto que no incluyen algunas claves y utilizan valores específicos para otros, como se muestra en la lista siguiente: <ul style="list-style-type: none"> EventSource <ul style="list-style-type: none"> sgws:s3 * AwsRegion* no incluido x-amz-id-2 no incluido arn urn:sgws:s3:::bucket_name
Política de PutBucketPolicy	Establece la política asociada al depósito. Ver " Utilice las políticas de acceso de bloques y grupos " .

Funcionamiento	Implementación
PutBucketReplication	<p>Configura "Replicación de CloudMirror de StorageGRID" el depósito mediante el XML de configuración de replicación proporcionado en el cuerpo de la solicitud. Para la replicación de CloudMirror, debe tener en cuenta los siguientes detalles de la implementación:</p> <ul style="list-style-type: none"> StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso <code>Filter</code> del elemento para reglas y sigue las convenciones de V1 para eliminar versiones de objetos. Para obtener más información, consulte "Guía del usuario de Amazon Simple Storage Service: Configuración de replicación". La replicación de bloques se puede configurar en bloques con versiones o sin versiones. Puede especificar un segmento de destino diferente en cada regla del XML de configuración de replicación. Un bloque de origen puede replicar en más de un bloque de destino. Los bloques de destino se deben especificar como URN de extremos StorageGRID tal y como se especifica en el administrador de inquilinos o la API de gestión de inquilinos. Consulte "Configure la replicación de CloudMirror". <p>El extremo debe existir para que la configuración de replicación se complete correctamente. Si el punto final no existe, la solicitud falla como 400 Bad Request . El mensaje de error indica: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code></p> <ul style="list-style-type: none"> No es necesario especificar un <code>Role</code> en el XML de configuración. StorageGRID no utiliza este valor y se ignorará si se envía. Si omite la clase <code>storage</code> del XML de configuración, StorageGRID utiliza la <code>STANDARD</code> clase <code>storage</code> de forma predeterminada. Si elimina un objeto del bloque de origen o elimina el propio bloque de origen, el comportamiento de replicación entre regiones es el siguiente: <ul style="list-style-type: none"> Si elimina el objeto o bloque antes de que se haya replicado, el objeto o bloque no se replicará y no se le notificará. Si elimina el objeto o bloque después de haber sido replicado, StorageGRID sigue el comportamiento estándar de eliminación de Amazon S3 para V1 de replicación entre regiones.

Funcionamiento	Implementación
PutBucketTagging	<p>Utiliza el <code>tagging</code> subrecurso para agregar o actualizar un juego de etiquetas para un depósito. Al añadir etiquetas de bloque, tenga en cuenta las siguientes limitaciones:</p> <ul style="list-style-type: none"> • Tanto StorageGRID como Amazon S3 admiten hasta 50 etiquetas por cada bloque. • Las etiquetas asociadas con un bloque deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode de longitud. • Los valores de etiqueta pueden tener una longitud máxima de 256 caracteres Unicode. • La clave y los valores distinguen entre mayúsculas y minúsculas. <p>Precaución: Si se establece una etiqueta de política de ILM no predeterminada para este cubo, habrá una <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de cubo con un valor asignado. Asegúrese de que la <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de cubo está incluida con el valor asignado en todas las solicitudes de PutBucketTagging. No modifique ni elimine esta etiqueta.</p> <p>Nota: Esta operación sobrescribirá cualquier etiqueta actual que el cubo ya tenga. Si se omite alguna etiqueta existente del conjunto, esas etiquetas se eliminarán para el cucharón.</p>
PutBucketVersioning	<p>Utiliza <code>versioning</code> el subrecurso para definir el estado de control de versiones de un bloque existente. Puede establecer el estado de control de versiones con uno de los siguientes valores:</p> <ul style="list-style-type: none"> • Enabled: Activa el control de versiones de los objetos del bloque. Todos los objetos que se agregan al bloque reciben un ID de versión único. • Suspended: Desactiva el control de versiones de los objetos del bloque. Todos los objetos agregados al depósito reciben el ID de versión <code>null</code>.
PutObjectLockConfiguration	<p>Configura o elimina el modo de retención predeterminado y el período de retención predeterminado.</p> <p>Si se modifica el período de retención predeterminado, la fecha de retención hasta la de las versiones de objeto existentes seguirá siendo la misma y no se volverá a calcular utilizando el nuevo período de retención predeterminado.</p> <p>Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" para obtener información detallada.</p>

Operaciones en objetos

Operaciones en objetos

En esta sección se describe cómo el sistema StorageGRID implementa operaciones de la API DE REST de S3 para objetos.

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

- StorageGRID "valores de coherencia" son compatibles con todas las operaciones sobre objetos, con excepción de las siguientes:
 - GetObjectAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetention
 - SelectObjectContent
- Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.
- Todos los objetos de un bloque StorageGRID son propiedad del propietario del bloque, incluidos los objetos creados por un usuario anónimo o por otra cuenta.

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

Funcionamiento	Implementación
DeleteObject DeleteObjects (Anteriormente denominado DELETE Múltiples Objetos)	<p>La autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles.</p> <p>Al procesar una solicitud DeleteObject, StorageGRID intenta eliminar inmediatamente todas las copias del objeto de todas las ubicaciones almacenadas. Si se realiza correctamente, StorageGRID devuelve una respuesta al cliente inmediatamente. Si no se pueden eliminar todas las copias en 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y, a continuación, indica que se ha realizado correctamente al cliente.</p> <p>Creación de versiones</p> <p>Para eliminar una versión específica, el solicitante debe ser el propietario del depósito y utilizar el <code>versionId</code> subrecurso. El uso de este subrecurso elimina permanentemente la versión. Si el <code>versionId</code> corresponde a un marcador de borrado, la cabecera de respuesta <code>x-amz-delete-marker</code> se devuelve establecida en <code>true</code>.</p> <ul style="list-style-type: none"> Si se suprime un objeto sin el <code>versionId</code> subrecurso de un depósito con el control de versiones activado, se genera un marcador de supresión. El <code>versionId</code> para el marcador de supresión se devuelve mediante <code>x-amz-version-id</code> la cabecera de respuesta y la <code>x-amz-delete-marker</code> cabecera de respuesta se devuelve establecida en <code>true</code>. Si se suprime un objeto sin el <code>versionId</code> subrecurso de un depósito con control de versiones suspendido, se suprime permanentemente una versión 'nula' ya existente o un marcador de supresión 'nulo' y se genera un nuevo marcador de supresión 'nulo'. <code>x-amz-delete-marker</code> La cabecera de respuesta se devuelve definida en <code>true</code>. <p>Nota: En algunos casos, pueden existir varios marcadores de borrado para un objeto.</p> <p>Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" para obtener más información sobre cómo eliminar versiones de objetos en el modo de GOBIERNO.</p>
	<p>La autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles.</p> <p>Se pueden eliminar varios objetos en el mismo mensaje de solicitud.</p> <p>Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" para obtener más información sobre cómo eliminar versiones de objetos en el modo de GOBIERNO.</p>

Funcionamiento	Implementación
DeleteObjectTagging	<p>Utiliza el <code>tagging</code> subrecurso para eliminar todas las etiquetas de un objeto.</p> <p>Creación de versiones</p> <p>Si el <code>versionId</code> parámetro de consulta no se especifica en la solicitud, la operación suprime todas las etiquetas de la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado <code>MethodNotAllowed</code> con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.</p>
GetObject	" GetObject "
GetObjectAcl	Si se proporcionan las credenciales de acceso necesarias para la cuenta, la operación devuelve una respuesta positiva y el ID, <code>DisplayName</code> y permiso del propietario del objeto, lo que indica que el propietario tiene acceso completo al objeto.
GetObjectLegalHold	" Use la API REST DE S3 para configurar el bloqueo de objetos de S3 "
GetObjectRetention	" Use la API REST DE S3 para configurar el bloqueo de objetos de S3 "
GetObjectEtiquetado	<p>Utiliza el <code>tagging</code> subrecurso para devolver todas las etiquetas de un objeto.</p> <p>Creación de versiones</p> <p>Si el <code>versionId</code> parámetro de consulta no se especifica en la solicitud, la operación devuelve todas las etiquetas de la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado <code>MethodNotAllowed</code> con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.</p>
Objeto principal	" Objeto principal "
RestoreObject	" RestoreObject "
Objeto de puta	" Objeto de puta "
CopyObject (Anteriormente denominado Objeto PUT - Copiar)	" CopyObject "
PutObjectLegalHold	" Use la API REST DE S3 para configurar el bloqueo de objetos de S3 "

Funcionamiento	Implementación
PutObjectRetention	<p>"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"</p>
PutObjectEtiquetado	<p>Utiliza el <code>tagging</code> subrecurso para agregar un juego de etiquetas a un objeto existente.</p> <p>Límites de etiqueta de objeto</p> <p>Puede agregar etiquetas a nuevos objetos cuando los cargue o puede agregarlos a objetos existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas por cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode de longitud y los valores de etiqueta pueden tener hasta 256 caracteres Unicode de longitud. La clave y los valores distinguen entre mayúsculas y minúsculas.</p> <p>Comportamiento de ingestión y actualizaciones de etiquetas</p> <p>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 ingestión especificada en la regla de ILM que coincide. Cualquier cambio en la ubicación del objeto que se active por la actualización se realice cuando los procesos de ILM normales se reevalúan el ILM en segundo plano.</p> <p>Esto significa que si la regla ILM utiliza la opción estricta para el comportamiento de ingestión, no se realiza ninguna acción si no se pueden realizar las ubicaciones de objetos necesarias (por ejemplo, porque una nueva ubicación requerida no está disponible). El objeto actualizado conserva su ubicación actual hasta que sea posible la colocación requerida.</p> <p>Resolución de conflictos</p> <p>Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.</p> <p>Creación de versiones</p> <p>Si el <code>versionId</code> parámetro de consulta no se especifica en la solicitud, la operación agrega etiquetas a la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado <code>MethodNotAllowed</code> con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.</p>
SelectObjectContent	<p>"SelectObjectContent"</p>

Utilice S3 Select

StorageGRID admite las siguientes cláusulas, tipos de datos y operadores de selección de Amazon S3 para el "["SelectObjectContent"](#)".



No se admiten los elementos que no aparecen en la lista.

Para obtener la sintaxis, consulte "["SelectObjectContent"](#)". Para obtener más información acerca de S3 Select, consulte la ["Documentación de AWS para S3 Select"](#).

Solo las cuentas de inquilino con S3 Select habilitado pueden emitir consultas de SelectObjectContent. Consulte la ["Consideraciones y requisitos para usar S3 Select"](#).

Cláusulas

- SELECCIONAR lista
- CLÁUSULA FROM
- Cláusula WHERE
- Cláusula LIMIT

Tipos de datos

- bool
- entero
- cadena
- flotante
- decimal, numérico
- fecha/hora

Operadores

Operadores lógicos

- Y..
- NO
- O..

Operadores de comparación

- <
- >
- ⇐
- >=
- =
- =
- <>

- !=
- ENTRE
- PULG

Operadores de comparación de patrones

- COMO
- _
- %

Operadores unitarios

- ES NULL
- NO ES NULL

Operadores de matemáticas

- +
- -
- *
- /
- %

StorageGRID sigue la prioridad del operador de Amazon S3 Select.

Funciones de agregados

- MEDIA()
- RECUENTO (*)
- MÁX.()
- MIN()
- SUMA()

Funciones condicionales

- CASO
- COALCE
- NULLIF

Funciones de conversión

- CAST (para tipo de datos compatible)

Funciones de fecha

- FECHA_AÑADIR
- DIF_FECHA

- EXTRAER
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

Funciones de cadena

- CHAR_LENGTH, CHARACTER_LENGTH
- INFERIOR
- SUBCADENA
- RECORTE
- SUPERIOR

Usar cifrado del servidor

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

Si desea utilizar el cifrado en el servidor, puede elegir una de las dos opciones mutuamente excluyentes, basándose en cómo se administran las claves de cifrado:

- **SSE (cifrado del lado del servidor con claves administradas por StorageGRID)**: Cuando se emite una solicitud de S3 para almacenar un objeto, StorageGRID cifra el objeto con una clave única. Cuando emite una solicitud S3 para recuperar el objeto, StorageGRID utiliza la clave almacenada para descifrar el objeto.
- **SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente)**: Cuando se emite una solicitud S3 para almacenar un objeto, se proporciona su propia clave de cifrado. Cuando recupera un objeto, proporciona la misma clave de cifrado que parte de la solicitud. Si las dos claves de cifrado coinciden, el objeto se descifra y se devuelven los datos del objeto.

Mientras que StorageGRID gestiona todas las operaciones de cifrado y descifrado de objetos, debe gestionar las claves de cifrado que proporcione.



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente.



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

Utilice SSE

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

`x-amz-server-side-encryption`

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

- "["Objeto de puta"](#)
- "["CopyObject"](#)
- "["CreateMultipartUpload"](#)

Utilice SSE-C

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

Solicite el encabezado	Descripción
x-amz-server-side -encryption-customer -algorithm	Especifique el algoritmo de cifrado. El valor de la cabecera debe ser AES256.
x-amz-server-side -encryption-customer-key	Especifique la clave de cifrado que se utilizará para cifrar o descifrar el objeto. El valor de la clave debe estar codificado en base64 de 256 bits.
x-amz-server-side -encryption-customer-key -MD5	Especifique el resumen MD5 de la clave de cifrado según RFC 1321, que se utiliza para garantizar que la clave de cifrado se haya transmitido sin errores. El valor del resumen MD5 debe estar codificado en base64 de 128 bits.

Las siguientes operaciones de objeto admiten los encabezados de solicitud de SSE-C:

- "["GetObject"](#)
- "["Objeto principal"](#)
- "["Objeto de puta"](#)
- "["CopyObject"](#)
- "["CreateMultipartUpload"](#)
- "["UploadPart"](#)
- "["UploadPartCopy"](#)

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

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

- Debe usar https.



StorageGRID rechaza cualquier solicitud hecha a través de http Cuando se utiliza SSE-C. Para consideraciones de seguridad, debe considerar cualquier clave que envíe accidentalmente usando http para ser comprometida. Deseche la llave y gírela según corresponda.

- La ETag en la respuesta no es la MD5 de los datos del objeto.
- Debe gestionar la asignación de claves de cifrado a objetos. StorageGRID no almacena claves de cifrado. Usted es responsable del seguimiento de la clave de cifrado que usted proporciona para cada objeto.
- Si su bloque está habilitado para versionado, cada versión de objeto debe tener su propia clave de cifrado. Usted es responsable del seguimiento de la clave de cifrado utilizada para cada versión del objeto.

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



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente.

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

Información relacionada

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

CopyObject

Puede utilizar la solicitud S3 CopyObject para crear una copia de un objeto que ya está almacenado en S3. Una operación CopyObject es la misma que realizarGetObject seguido de PutObject.

Resolver conflictos

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Tamaño del objeto

El tamaño máximo de *recommended* para una sola operación PutObject es de 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice su "[carga de varias partes](#)" lugar.

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



Si actualizó desde StorageGRID 11,6 o una versión anterior, se activará la alerta S3 PUT Object size too large si intenta cargar un objeto que supere los 5 GiB. Si tiene una instalación nueva de StorageGRID 11,7 o 11,8, la alerta no se activará en este caso. Sin embargo, para alinearse con el estándar AWS S3, las versiones futuras de StorageGRID no admitirán cargas de objetos de más de 5 GiB.

Caracteres UTF-8 en los metadatos de usuario

Si una solicitud incluye (no escapadas) valores UTF-8 en el nombre de clave o el valor de los metadatos definidos por el usuario, el comportamiento de StorageGRID no está definido.

StorageGRID no analiza ni interpreta los caracteres UTF-8 escapados incluidos en el nombre de clave o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 que se han escapado se tratan como caracteres ASCII:

- Las solicitudes se realizan correctamente si los metadatos definidos por el usuario incluyen caracteres UTF-8 que se han escapado.
- StorageGRID no devuelve x-amz-missing-meta el encabezado si el valor interpretado del nombre o valor de la clave incluye caracteres no imprimibles.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

Puede REPLACE especificar que sobrescriba los metadatos existentes al copiar el objeto o que actualice los metadatos de los objetos.

- x-amz-storage-class
- x-amz-tagging-directive: El valor por defecto es COPY, que permite copiar el objeto y todas las etiquetas.

Puede especificar REPLACE que sobrescriba las etiquetas existentes al copiar el objeto o que actualice las etiquetas.

- Encabezados de solicitud de bloqueo de objetos S3:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

Si se realiza una solicitud sin estas cabeceras, se utiliza la configuración de retención por defecto del depósito para calcular el modo de versión del objeto y retener hasta la fecha. Consulte "["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)".

- Encabezados de solicitud SSE:

- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

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

Encabezados de solicitud no compatibles

No se admiten las siguientes cabeceras de solicitud:

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

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

- x-amz-website-redirect-location

Opciones para clase de almacenamiento

El x-amz-storage-class encabezado de solicitud está soportado y afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente utiliza la confirmación doble o equilibrada "[opción de ingestión](#)".

- STANDARD

(Predeterminado) especifica una operación de procesamiento de confirmación doble cuando la regla ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.

- REDUCED_REDUNDANCY

Especifica una operación de procesamiento de confirmación única cuando la regla de ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.



Si está ingiriendo un objeto en un depósito con S3 Object Lock activado, la REDUCED_REDUNDANCY opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, la REDUCED_REDUNDANCY opción devuelve un error. StorageGRID siempre realizará una ingestión con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Uso de x-amz-copy-source en CopyObject

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

Si el origen y el destino coinciden y la x-amz-metadata-directive cabecera se especifica como REPLACE, los metadatos del objeto se actualizan con los valores de metadatos proporcionados en la solicitud. En este caso, StorageGRID no vuelve a procesar el objeto. Esto tiene dos consecuencias importantes:

- No puede utilizar CopyObject para cifrar un objeto existente en su lugar, o para cambiar el cifrado de un objeto existente en su lugar. Si proporciona el x-amz-server-side-encryption encabezado o x-

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

- No se utiliza la opción de comportamiento de procesamiento especificado en la regla de ILM que coincida. Cualquier cambio en la ubicación del objeto que se active por la actualización se realice cuando los procesos de ILM normales se reevalúan el ILM en segundo plano.

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

Solicitar encabezados para el cifrado del servidor

Si ["usar cifrado del lado del servidor"](#), las cabeceras de solicitud que proporcione dependen de si el objeto de origen está cifrado y de si planea cifrar el objeto de destino.

- Si el objeto de origen se cifra mediante una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud CopyObject, para que el objeto se pueda descifrar y copiar:
 - x-amz-copy-source-server-side-encryption-customer-algorithm: Especificar AES256.
 - x-amz-copy-source-server-side-encryption-customer-key: Especifique la clave de cifrado que proporcionó al crear el objeto de origen.
 - x-amz-copy-source-server-side-encryption-customer-key-MD5: Especifique el resumen MD5 que proporcionó cuando creó el objeto de origen.
- Si desea cifrar el objeto de destino (la copia) con una clave única que proporciona y administra, incluya los tres encabezados siguientes:
 - x-amz-server-side-encryption-customer-algorithm: Especificar AES256.
 - x-amz-server-side-encryption-customer-key: Especifique una nueva clave de cifrado para el objeto de destino.
 - x-amz-server-side-encryption-customer-key-MD5: Especifique el resumen MD5 de la nueva clave de cifrado.



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones para ["utilizando cifrado del lado del servidor"](#).

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

- x-amz-server-side-encryption



server-side-encryption`El valor del objeto no se puede actualizar. En su lugar, realice una copia con un nuevo `server-side-encryption valor mediante x-amz-metadata-directive: REPLACE.

Creación de versiones

Si el depósito de origen está versionado, puede utilizar x-amz-copy-source la cabecera para copiar la

versión más reciente de un objeto. Para copiar una versión específica de un objeto, debe especificar explícitamente la versión que se va a copiar mediante el `versionId` subrecurso. Si el bloque de destino está versionado, la versión generada se devuelve en `x-amz-version-id` la cabecera de respuesta. Si se suspende el control de versiones para el depósito de destino, `x-amz-version-id` devuelve un valor nulo.

GetObject

Puede usar la solicitud GetObject S3 para recuperar un objeto de un bucket S3.

Objetos GetObject y multipart

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

Se puede establecer `partNumber` en 1 para objetos segmentados/multiparte y objetos no segmentados/no multiparte; sin embargo, el `x-amz-mp-parts-count` elemento de respuesta sólo se devuelve para objetos segmentados o multiparte.

Caracteres UTF-8 en los metadatos de usuario

StorageGRID no analiza ni interpreta caracteres UTF-8 escapados en los metadatos definidos por el usuario. Las solicitudes GET para un objeto con caracteres UTF-8 que se han escapado en los metadatos definidos por el usuario no devuelven `x-amz-missing-meta` el encabezado si el nombre o el valor de la clave incluyen caracteres no imprimibles.

Cabecera de solicitud admitida

Se admite el siguiente encabezado de solicitud:

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

`Range` La cabecera no está soportada con `x-amz-checksum-mode` para GetObject. Si se incluye `Range` en la solicitud con `x-amz-checksum-mode` Enabled, StorageGRID no devuelve un valor de suma de comprobación en la respuesta.

Encabezado de solicitud no compatible

La siguiente cabecera de solicitud no está soportada y devuelve XNotImplemented:

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

Creación de versiones

Si no se especifica un `versionId` subrecurso, la operación recupera la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de supresión, se devuelve un estado de no encontrado con la `x-amz-delete-marker` cabecera de respuesta establecida en `true`.

Solicitar encabezados para el cifrado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utilice los tres encabezados si el objeto está cifrado con una clave única que ha proporcionado.

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



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en "["Usar cifrado del servidor"](#)".

Comportamiento de los objetos GetObject para Cloud Storage Pool

Si se ha almacenado un objeto en un "[Pool de almacenamiento en cloud](#)", el comportamiento de una solicitud GetObject depende del estado del objeto. Consulte "["Objeto principal"](#)" para obtener más información.



Si un objeto está almacenado en un Pool de almacenamiento en la nube y una o más copias del objeto también existen en la cuadrícula, las solicitudes de GetObject intentarán recuperar los datos de la cuadrícula, antes de recuperarlo del Pool de almacenamiento en la nube.

Estado del objeto	Comportamiento de GetObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un pool de almacenamiento tradicional o utilizando código de borrado	200 OK Se recupera una copia del objeto.
Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	200 OK Se recupera una copia del objeto.
Objeto que ha pasado a un estado no recuperable	403 Forbidden, InvalidObjectState Utilice una " "RestoreObject" " solicitud para restaurar el objeto a un estado recuperable.
Objeto en proceso de restauración a partir de un estado no recuperable	403 Forbidden, InvalidObjectState Espere a que finalice la solicitud RestoreObject.
Objeto completamente restaurado en el pool de almacenamiento en cloud	200 OK Se recupera una copia del objeto.

Objetos de varias partes o segmentados en un pool de almacenamiento en nube

Si cargó un objeto con varias partes o StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el pool de almacenamiento en cloud al muestrear un subconjunto de

las partes o segmentos del objeto. En algunos casos, una solicitudGetObject podría regresar incorrectamente 200 OK cuando algunas partes del objeto ya se han trasladado a un estado no recuperable o cuando algunas partes del objeto aún no se han restaurado.

En estos casos:

- Es posible que la solicitudGetObject devuelva algunos datos, pero se detenga a mitad de la transferencia.
- Es posible que se devuelva una solicitudGetObject posterior 403 Forbidden .

GetObject y replicación entre grid

Si está utilizando "federación de grid" y "replicación entre grid" está habilitado para un depósito, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitudGetObject. La respuesta incluye el encabezado de respuesta específico de StorageGRID x-ntap-sg-cgr-replication-status, que tendrá uno de los siguientes valores:

Cuadrícula	Estado de replicación
Origen	<ul style="list-style-type: none">• COMPLETADO: La replicación fue exitosa.• PENDIENTE: El objeto aún no ha sido replicado.• FALLO: La replicación falló con un fallo permanente. Un usuario debe resolver el error.
Destino	REPLICA : El objeto fue replicado desde la cuadrícula de origen.



StorageGRID no admite x-amz-replication-status el encabezado.

Objeto principal

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

HeadObject y objetos multiparte

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

Se puede establecer partNumber en 1 para objetos segmentados/multiparte y objetos no segmentados/no multiparte; sin embargo, el x-amz-mp-parts-count elemento de respuesta sólo se devuelve para objetos segmentados o multiparte.

Caracteres UTF-8 en los metadatos de usuario

StorageGRID no analiza ni interpreta caracteres UTF-8 escapados en los metadatos definidos por el usuario. Las solicitudes de CABECERA para un objeto con caracteres UTF-8 que se han escapado en los metadatos definidos por el usuario no devuelven x-amz-missing-meta la cabecera si el nombre o el valor de la clave incluyen caracteres no imprimibles.

Cabecera de solicitud admitida

Se admite el siguiente encabezado de solicitud:

- `x-amz-checksum-mode`

El `partNumber` parámetro y `Range` el encabezado no son compatibles con `x-amz-checksum-mode` para `HeadObject`. Cuando se incluyen en la solicitud con `x-amz-checksum-mode Enabled`, StorageGRID no devuelve un valor de suma de comprobación en la respuesta.

Encabezado de solicitud no compatible

La siguiente cabecera de solicitud no está soportada y devuelve `XNotImplemented`:

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

Creación de versiones

Si no se especifica un `versionId` subrecurso, la operación recupera la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de supresión, se devuelve un estado de no encontrado con la `x-amz-delete-marker` cabecera de respuesta establecida en `true`.

Solicitar encabezados para el cifrado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utilice los tres encabezados si el objeto está cifrado con una clave única que ha proporcionado.

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

 Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en "["Usar cifrado del servidor"](#)".

Respuestas HeadObject para objetos de Cloud Storage Pool

Si el objeto se almacena en un "[Pool de almacenamiento en cloud](#)", se devuelven las siguientes cabeceras de respuesta:

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

Los encabezados de respuesta proporcionan información sobre el estado de un objeto a medida que se mueve a un pool de almacenamiento en cloud, y que, opcionalmente, se realiza la transición a un estado no recuperable y se restaura.

Estado del objeto	Respuesta a HeadObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un pool de almacenamiento tradicional o utilizando código de borrado	200 OK (No se devuelve ninguna cabecera de respuesta especial).
Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Hasta que el objeto se convierte en un estado no recuperable, el valor para expiry-date se establece en un tiempo lejano en el futuro. El sistema StorageGRID no controla la hora exacta de la transición.</p>
El objeto ha pasado a estar en estado no recuperable, pero también existe al menos una copia en la cuadrícula	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>El valor para expiry-date se establece en algún tiempo lejano en el futuro.</p> <p>Nota: Si la copia en la cuadrícula no está disponible (por ejemplo, un nodo de almacenamiento está caído), debe emitir una "RestoreObject" solicitud para restaurar la copia del grupo de almacenamiento en la nube antes de poder recuperar el objeto con éxito.</p>
El objeto ha pasado a un estado que no se puede recuperar y no existe ninguna copia en la cuadrícula	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
Objeto en proceso de restauración a partir de un estado no recuperable	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>

Estado del objeto	Respuesta a HeadObject
Objeto completamente restaurado en el pool de almacenamiento en cloud	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 2018 00:00:00 GMT"</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>`expiry-date` Indica cuándo el objeto del pool de almacenamiento en la nube volverá a un estado no recuperable.</p> </div>

Objetos de varias partes o segmentos en el pool de almacenamiento en cloud

Si cargó un objeto con varias partes o StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el pool de almacenamiento en cloud al muestrear un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud HeadObject podría regresar incorrectamente x-amz-restore: ongoing-request="false" cuando algunas partes del objeto ya se han trasladado a un estado no recuperable o cuando algunas partes del objeto aún no se han restaurado.

HeadObject y replicación entre grid

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

Cuadrícula	Estado de replicación
Origen	<ul style="list-style-type: none"> COMPLETADO: La replicación fue exitosa. PENDIENTE: El objeto aún no ha sido replicado. FALLO: La replicación falló con un fallo permanente. Un usuario debe resolver el error.
Destino	REPLICA : El objeto fue replicado desde la cuadrícula de origen.



StorageGRID no admite x-amz-replication-status el encabezado.

Objeto de puta

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

Resolver conflictos

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Tamaño del objeto

El tamaño máximo de *recommended* para una sola operación PutObject es de 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice su "[carga de varias partes](#)" lugar.

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

 Si actualizó desde StorageGRID 11,6 o una versión anterior, se activará la alerta S3 PUT Object size too large si intenta cargar un objeto que supere los 5 GiB. Si tiene una instalación nueva de StorageGRID 11,7 o 11,8, la alerta no se activará en este caso. Sin embargo, para alinearse con el estándar AWS S3, las versiones futuras de StorageGRID no admitirán cargas de objetos de más de 5 GiB.

Tamaño de los metadatos del usuario

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

Caracteres UTF-8 en los metadatos de usuario

Si una solicitud incluye (no escapadas) valores UTF-8 en el nombre de clave o el valor de los metadatos definidos por el usuario, el comportamiento de StorageGRID no está definido.

StorageGRID no analiza ni interpreta los caracteres UTF-8 escapados incluidos en el nombre de clave o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 que se han escapado se tratan como caracteres ASCII:

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

Límites de etiqueta de objeto

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

Propiedad del objeto

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

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- Cache-Control
- Content-Disposition
- Content-Encoding

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

- StorageGRID no verifica el chunk-signature con respecto a los datos del fragmento.
- StorageGRID no verifica el valor proporcionado para x-amz-decoded-content-length respecto al objeto.
- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

La codificación de transferencia fragmentada se admite si aws-chunked también se utiliza la firma de carga útil.

- x-amz-checksum-sha256
- x-amz-meta-, seguido de un par nombre-valor que contiene metadatos definidos por el usuario.

Cuando especifique la pareja nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

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

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

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

El valor para creation-time se evalúa como segundos desde el 1 de enero de 1970.



Una regla de ILM no puede usar un **Tiempo de creación definido por el usuario** para el Tiempo de referencia y la opción de ingestión equilibrada o estricta. Se devuelve un error cuando se crea la regla de ILM.

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

Si se realiza una solicitud sin estas cabeceras, se utiliza la configuración de retención por defecto del depósito para calcular el modo de versión del objeto y retener hasta la fecha. Consulte ["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#).

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

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

Encabezados de solicitud no compatibles

No se admiten las siguientes cabeceras de solicitud:

- `If-Match`
- `If-None-Match`
- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

El `x-amz-website-redirect-location` cabezal devuelve `XNotImplemented`.

Opciones para clase de almacenamiento

`'x-amz-storage-class'` Se admite el encabezado de solicitud. El valor enviado para `'x-amz-storage-class'` afecta a la forma en que StorageGRID protege los datos de los objetos durante la ingestión y no al número de copias persistentes del objeto que se almacenan en el sistema StorageGRID (que viene determinado por ILM) .

Si la regla de ILM que coincide con un objeto ingerido utiliza la opción `strict ingest`, el `x-amz-storage-class` encabezado no tiene efecto.

Se pueden utilizar los siguientes valores para `x-amz-storage-class`:

- STANDARD (Predeterminado)

- **Commit doble:** Si la regla ILM especifica la opción COMMIT doble para el comportamiento de procesamiento, tan pronto como un objeto se ingiere una segunda copia de ese objeto se crea y se distribuye a un nodo de almacenamiento diferente (COMMIT doble). Cuando se evalúa el ciclo de vida de la información, StorageGRID determina si estas copias provisionales iniciales cumplen las instrucciones de colocación que se indican en la regla. Si no es así, es posible que deban realizarse copias de objetos nuevas en ubicaciones diferentes y es posible que las copias provisionales iniciales deban eliminarse.
- **Equilibrado:** Si la regla de ILM especifica la opción Equilibrada y StorageGRID no puede hacer inmediatamente todas las copias especificadas en la regla, StorageGRID hace dos copias provisionales en diferentes nodos de almacenamiento.

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

- REDUCED_REDUNDANCY

- **Commit doble:** Si la regla ILM especifica la opción COMMIT doble para el comportamiento de la ingestión, StorageGRID crea una única copia provisional mientras se ingiere el objeto (COMMIT único).
- **Equilibrado:** Si la regla de ILM especifica la opción Equilibrada, StorageGRID hace una sola copia provisional solo si el sistema no puede hacer inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación síncrona, este encabezado no tiene ningún efecto. REDUCED_REDUNDANCY La opción se usa mejor cuando la regla de ILM que coincide con el objeto crea una copia replicada única. En este caso, utilizar REDUCED_REDUNDANCY elimina la creación y la eliminación innecesarias de una copia de objeto adicional para cada operación de ingestión.

En otras circunstancias, no se recomienda utilizar REDUCED_REDUNDANCY la opción.

REDUCED_REDUNDANCY aumenta el riesgo de pérdida de datos de objetos durante la ingestión. Por ejemplo, puede perder datos si la única copia se almacena inicialmente en un nodo de almacenamiento que falla antes de que se pueda realizar la evaluación de ILM.

 Tener solo una copia replicada durante un periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

La especificación REDUCED_REDUNDANCY solo afecta al número de copias que se crean cuando se procesa un objeto por primera vez. No afecta a cuántas copias del objeto se realizan cuando el objeto se evalúa mediante las políticas de ILM activas y no da lugar a que los datos se almacenen en niveles más bajos de redundancia del sistema StorageGRID.

 Si está ingiriendo un objeto en un depósito con S3 Object Lock activado, la REDUCED_REDUNDANCY opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, la REDUCED_REDUNDANCY opción devuelve un error. StorageGRID siempre realizará una ingestión con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Solicitar encabezados para el cifrado del servidor

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

- **SSE:** Utilice el siguiente encabezado si desea cifrar el objeto con una clave única gestionada por StorageGRID.

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

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

- **SSE-C:** Utilice los tres encabezados si desea cifrar el objeto con una clave única que proporciona y administra.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256.

- `x-amz-server-side-encryption-customer-key`: Especifique su clave de cifrado para el nuevo objeto.

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



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones para "[utilizando cifrado del lado del servidor](#)".



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

Creación de versiones

Si se activa el control de versiones para un depósito, se genera automáticamente una única `versionId` para la versión del objeto que se está almacenando. Esto `versionId` también se devuelve en la respuesta utilizando `x-amz-version-id` la cabecera de respuesta.

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

Cálculos de firma para la cabecera de autorización

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

- StorageGRID no requiere que `host` se incluyan encabezados en `CanonicalHeaders`.
- StorageGRID no requiere `Content-Type` ser incluido dentro de `CanonicalHeaders`.
- StorageGRID no requiere que `x-amz-*` se incluyan encabezados en `CanonicalHeaders`.



Como práctica recomendada general, incluya siempre estos encabezados en `CanonicalHeaders` para asegurarse de que están verificados; sin embargo, si excluye estos encabezados, StorageGRID no devuelve un error.

Para obtener más información, consulte "[Cálculos de firma para la cabecera de autorización: Transferencia de carga útil en un solo fragmento \(AWS Signature versión 4\)](#)" .

Información relacionada

- "[Gestión de objetos con ILM](#)"
- "[Referencia de API de Amazon Simple Storage Service: PutObject](#)"

RestoreObject

Puede utilizar la solicitud S3 RestoreObject para restaurar un objeto almacenado en un Cloud Storage Pool.

Tipo de solicitud admitido

StorageGRID solo admite solicitudes RestoreObject para restaurar un objeto. No apoya el SELECT tipo de restauración. Seleccione Solicitudes devueltas XNotImplemented.

Creación de versiones

De forma opcional, especifique si desea `versionId` restaurar una versión específica de un objeto en un bloque con versiones. Si no especifica `versionId`, se restaurará la versión más reciente del objeto

Comportamiento de RestoreObject en objetos de Cloud Storage Pool

Si se ha almacenado un objeto en un "[Pool de almacenamiento en cloud](#)", una solicitud RestoreObject tiene el siguiente comportamiento, según el estado del objeto. Consulte "[Objeto principal](#)" para obtener más información.



Si un objeto se almacena en un pool de almacenamiento en la nube y una o más copias del objeto también existen en la cuadrícula, no es necesario restaurar el objeto emitiendo una solicitud RestoreObject. En su lugar, la copia local se puede recuperar directamente mediante una solicitud GetObject.

Estado del objeto	Comportamiento de RestoreObject
El objeto se ingiere en StorageGRID pero aún no se ha evaluado por ILM, o el objeto no está en un pool de almacenamiento cloud	403 Forbidden, InvalidObjectState
Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	200 OK No se realizan cambios. Nota: Antes de que un objeto haya sido trasladado a un estado no recuperable, no puede cambiar su estado expiry-date.

Estado del objeto	Comportamiento de RestoreObject
Objeto que ha pasado a un estado no recuperable	<p>202 Accepted Restaura una copia recuperable del objeto en Cloud Storage Pool durante el Núm. De días especificado en el cuerpo de la solicitud. Al final de este período, el objeto se devuelve a un estado no recuperable.</p> <p>De forma opcional, utilice el <code>Tier</code> elemento request para determinar cuánto tiempo tardará el trabajo de restauración en finalizar (Expedited, Standard o Bulk). Si no especifica <code>Tier</code>, se utilizará el Standard nivel.</p> <p>Importante: Si un objeto ha sido trasladado a S3 Glacier Deep Archive o el Cloud Storage Pool usa almacenamiento de Azure Blob, no puede restaurarlo usando el Expedited nivel. Se devuelve el siguiente error 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.</p>
Objeto en proceso de restauración a partir de un estado no recuperable	409 Conflict, RestoreAlreadyInProgress
Objeto completamente restaurado en el pool de almacenamiento en cloud	<p>200 OK</p> <p>Nota: Si un objeto ha sido restaurado a un estado recuperable, puede cambiarlo <code>expiry-date</code> volviendo a emitir la solicitud <code>RestoreObject</code> con un nuevo valor para <code>Days</code>. La fecha de restauración se actualiza en relación con la hora de la solicitud.</p>

SelectObjectContent

Puede utilizar la solicitud S3 `SelectObjectContent` para filtrar el contenido de un objeto S3 en función de una simple instrucción SQL.

Para obtener más información, consulte "[Referencia de API de Amazon Simple Storage Service: SelectObjectContent](#)".

Antes de empezar

- La cuenta de inquilino tiene el permiso de S3 `Select`.
- Tiene `s3:GetObject` permiso para el objeto que desea consultar.
- El objeto que desea consultar debe tener uno de los siguientes formatos:
 - **CSV.** Se puede utilizar tal cual o comprimir en archivos GZIP o bzip2.
 - **Parquet.** Requisitos adicionales para objetos de parquet:
 - S3 Select solo admite la compresión en columnas usando GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos de parquet.
 - S3 La selección no es compatible con la salida de parquet. Debe especificar el formato de salida como CSV o JSON.
 - El tamaño máximo del grupo de filas sin comprimir es de 512 MB.

- Debe utilizar los tipos de dato especificados en el esquema del objeto.
- No puede utilizar los tipos lógicos INTERVAL, JSON, LIST, TIME o UUID.
- La expresión SQL tiene una longitud máxima de 256 KB.
- Cualquier registro de la entrada o de los resultados tiene una longitud máxima de 1 MIB.

Ejemplo de sintaxis de solicitud CSV

```

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

```

Ejemplo de sintaxis de solicitud de parquet

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

Ejemplo de consulta SQL

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

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

Las primeras líneas del archivo que se va a consultar, SUB-EST2020_ALL.csv, se ven así:

```

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

```

Ejemplo de uso de AWS-CLI (CSV)

```

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

```

Las primeras líneas del archivo de salida, changes.csv, tienen el siguiente aspecto:

```

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

```

Ejemplo de uso AWS-CLI (Parquet)

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

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

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

Operaciones para cargas de varias partes

Operaciones para cargas de varias partes

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

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

- No debe superar las 1.000 cargas simultáneas de varias partes en un solo bloque porque los resultados de las consultas ListMultipartUploads de ese bloque podrían devolver resultados incompletos.
- StorageGRID aplica los límites de tamaño de AWS para piezas multipartes. Los clientes de S3 deben seguir estas directrices:
 - Cada parte de una carga de varias partes debe estar entre 5 MIB (5,242,880 bytes) y 5 GIB (5,368,709,120 bytes).
 - La última parte puede ser más pequeña que 5 MIB (5,242,880 bytes).
 - En general, los tamaños de las piezas deben ser lo más grandes posible. Por ejemplo, utilice tamaños de parte de 5 GIB para un objeto de 100 GIB. Debido a que cada parte se considera un objeto único, el uso de piezas de gran tamaño reduce la sobrecarga de metadatos de StorageGRID.
 - En el caso de objetos de menor tamaño de 5 GIB, considere usar la carga sin varias partes.
- ILM se evalúa para cada parte de un objeto de varias partes a medida que se ingiere y para el objeto como un todo cuando se completa la carga de varias partes, si la regla de ILM utiliza el equilibrado o estricto "[opción de ingestión](#)". Debe saber cómo afecta esto a la ubicación de objetos y piezas:
 - Si el ILM cambia mientras se realiza una carga de varias partes de S3 GB, es posible que algunas partes del objeto no cumplan los requisitos del ILM actuales cuando se complete la carga de varias partes. Cualquier pieza que no se coloque correctamente se pondrá en cola para volver a evaluarla y

posteriormente se moverá a la ubicación correcta.

- Al evaluar ILM para una pieza, StorageGRID filtra el tamaño de la pieza, no el tamaño del objeto. Esto significa que las partes de un objeto se pueden almacenar en ubicaciones que no cumplen con los requisitos de ILM para el objeto como un todo. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan a DC1 mientras que todos los objetos más pequeños se almacenan a DC2, cada parte de 1 GB de una carga de varias partes de 10 partes se almacena a DC2 en el momento de la ingestión. Sin embargo, cuando se evalúa ILM para el objeto como un todo, todas las partes del objeto se mueven a DC1.
- Todas las operaciones de carga multiparte son compatibles con StorageGRID "valores de coherencia".
- Cuando se ingiere un objeto mediante la carga de varias partes, no se aplica el "Umbral de segmentación de objetos (1 GiB)".
- Según sea necesario, puede utilizar "cifrado del lado del servidor" con cargas de varias partes. Para utilizar SSE (cifrado del lado del servidor con claves administradas por StorageGRID), debe incluir `x-amz-server-side-encryption` el encabezado de solicitud solo en la solicitud `CreateMultipartUpload`. Para utilizar SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente), debe especificar los mismos tres encabezados de solicitud de clave de cifrado en la solicitud `CreateMultipartUpload` y en cada solicitud subsiguiente `UploadPart`.
- Un objeto cargado de varias partes se incluye en un "cubo de rama" si la ingestión se inició antes de la marca de tiempo Antes del depósito base, independientemente de cuándo se complete la carga.

Funcionamiento	Implementación
<code>AbortMultipartUpload</code>	Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones.
<code>CompleteMultipartUpload</code>	Consulte " CompleteMultipartUpload "
<code>CreateMultipartUpload</code> (Anteriormente denominado Iniciar carga de varias partes)	Consulte " CreateMultipartUpload "
<code>ListCargas multipartitas</code>	Consulte " ListCargas multipartitas "
<code>ListParts</code>	Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones.
<code>UploadPart</code>	Consulte " UploadPart "
<code>UploadPartCopy</code>	Consulte " UploadPartCopy "

CompleteMultipartUpload

La operación `CompleteMultipartUpload` completa una carga de varias partes de un objeto mediante el ensamblaje de las piezas cargadas anteriormente.



StorageGRID soporta valores no consecutivos en orden ascendente para el `partNumber` parámetro `request` con `CompleteMultipartUpload`. El parámetro puede comenzar con cualquier valor.

Resolver conflictos

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

``x-amz-storage-class`` El encabezado afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente especifica el `xref:{relative_path}.../ilm/data-protection-options-for-ingest.html` ["Opción de registro doble o ingestión equilibrada"] .

- STANDARD

(Predeterminado) especifica una operación de procesamiento de confirmación doble cuando la regla ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.

- REDUCED_REDUNDANCY

Especifica una operación de procesamiento de confirmación única cuando la regla de ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.



Si está ingiriendo un objeto en un depósito con S3 Object Lock activado, la `REDUCED_REDUNDANCY` opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, la `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingestión con doble confirmación para garantizar que se cumplen los requisitos de cumplimiento.



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



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

Encabezados de solicitud no compatibles

No se admiten las siguientes cabeceras de solicitud:

- If-Match
- If-None-Match
- x-amz-sdk-checksum-algorithm
- x-amz-trailer

Creación de versiones

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

Si se activa el control de versiones para un depósito, se genera automáticamente una única `versionId` para la versión del objeto que se está almacenando. Esto `versionId` también se devuelve en la respuesta utilizando `x-amz-version-id` la cabecera de respuesta.

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

 Cuando se habilita el control de versiones para un bloque, al completar una carga de varias partes siempre se crea una versión nueva, incluso si hay cargas simultáneas de varias partes completadas en la misma clave de objeto. Cuando el control de versiones no está habilitado para un bloque, es posible iniciar una carga de varias partes y, a continuación, hacer que se inicie y finalice otra carga de varias partes primero en la misma clave de objeto. En cubos sin versiones, la carga de varias partes que finaliza por última vez tiene prioridad.

Error en la replicación, notificación o notificación de metadatos

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

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

Consulte "[Solucione problemas de servicios de plataforma](#)".

CreateMultipartUpload

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

`x-amz-storage-class` Se admite el encabezado de solicitud. El valor enviado para `x-amz-storage-class` afecta a la forma en que StorageGRID protege los datos de los objetos durante la ingestión y no al número de copias persistentes del objeto que se almacenan en el sistema StorageGRID (que viene determinado por ILM).

Si la regla de ILM que coincide con un objeto ingerido utiliza el estricto "[opción de ingestión](#)", `x-amz-storage-class` la cabecera no tiene ningún efecto.

Se pueden utilizar los siguientes valores para `x-amz-storage-class`:

- STANDARD (Predeterminado)

- **Confirmación doble:** Si la regla ILM especifica la opción de ingestión de confirmación doble, tan pronto como se ingiere un objeto, se crea una segunda copia de ese objeto y se distribuye a un nodo de almacenamiento diferente (confirmación doble). Cuando se evalúa el ciclo de vida de la información, StorageGRID determina si estas copias provisionales iniciales cumplen las instrucciones de colocación que se indican en la regla. Si no es así, es posible que deban realizarse copias de objetos nuevas en ubicaciones diferentes y es posible que las copias provisionales iniciales deban eliminarse.
- **Equilibrado:** Si la regla de ILM especifica la opción Equilibrada y StorageGRID no puede hacer inmediatamente todas las copias especificadas en la regla, StorageGRID hace dos copias provisionales en diferentes nodos de almacenamiento.

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

- REDUCED_REDUNDANCY

- **Confirmación doble:** Si la regla de ILM especifica la opción Confirmación doble, StorageGRID crea una sola copia provisional a medida que se ingiere el objeto (confirmación única).
- **Equilibrado:** Si la regla de ILM especifica la opción Equilibrada, StorageGRID hace una sola copia provisional solo si el sistema no puede hacer inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación síncrona, este encabezado no tiene ningún efecto. REDUCED_REDUNDANCY La opción se usa mejor cuando la regla de ILM que coincide con el objeto crea una copia replicada única. En este caso, utilizar REDUCED_REDUNDANCY elimina la creación y la eliminación innecesarias de una copia de objeto adicional para cada operación de ingestión.

En otras circunstancias, no se recomienda utilizar REDUCED_REDUNDANCY la opción.

REDUCED_REDUNDANCY aumenta el riesgo de pérdida de datos de objetos durante la ingestión. Por ejemplo, puede perder datos si la única copia se almacena inicialmente en un nodo de almacenamiento que falla antes de que se pueda realizar la evaluación de ILM.

 Tener solo una copia replicada durante un periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

La especificación REDUCED_REDUNDANCY solo afecta al número de copias que se crean cuando se procesa un objeto por primera vez. No afecta a cuántas copias del objeto se realizan cuando el objeto se evalúa mediante las políticas de ILM activas y no da lugar a que los datos se almacenen en niveles más bajos de redundancia del sistema StorageGRID.

 Si está ingiriendo un objeto en un depósito con S3 Object Lock activado, la REDUCED_REDUNDANCY opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, la REDUCED_REDUNDANCY opción devuelve un error. StorageGRID siempre realizará una ingestión con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

Actualmente, solo se admite el valor de SHA256 para x-amz-checksum-algorithm.

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

Cuando especifique la pareja nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

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

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

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

El valor para creation-time se evalúa como segundos desde el 1 de enero de 1970.



No se permite agregar creation-time como metadatos definidos por el usuario si está agregando un objeto a un depósito que tiene activada la conformidad heredada. Se devolverá un error.

- Encabezados de solicitud de bloqueo de objetos S3:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

Si se realiza una solicitud sin estos encabezados, la configuración de retención predeterminada del bloque se utiliza para calcular la versión del objeto mantener hasta la fecha.

["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)

- Encabezados de solicitud SSE:

- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

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



Para obtener más información sobre cómo StorageGRID trata los caracteres UTF-8, consulte ["Objeto de puta"](#).

Solicitar encabezados para el cifrado del servidor

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

- **SSE:** Utilice el siguiente encabezado en la solicitud CreateMultipartUpload si desea cifrar el objeto con una clave única gestionada por StorageGRID. No especifique esta cabecera en ninguna de las solicitudes de artículo de carga.
 - `x-amz-server-side-encryption`
- **SSE-C:** Utilice los tres encabezados en la solicitud CreateMultipartUpload (y en cada solicitud subsiguiente UploadPart) si desea cifrar el objeto con una clave única que proporcione y administre.
 - `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256.
 - `x-amz-server-side-encryption-customer-key`: Especifique su clave de cifrado para el nuevo objeto.
 - `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones para ["utilizando cifrado del lado del servidor"](#).

Encabezados de solicitud no compatibles

No se admite el siguiente encabezado de solicitud:

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

El `x-amz-website-redirect-location` cabezal devuelve XNotImplemented.

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

ListCargas multipartitas

La operación ListMultipartUploads muestra las cargas de varias partes en curso para un bloque.

Se admiten los siguientes parámetros de solicitud:

- `encoding-type`
- `key-marker`

- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

UploadPart

La operación UploadPart carga una pieza en una carga de varias partes para un objeto.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

Solicitar encabezados para el cifrado del servidor

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

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



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en "["Usar cifrado del servidor"](#)".

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

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

Encabezados de solicitud no compatibles

No se admiten las siguientes cabeceras de solicitud:

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

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación `CompleteMultipartUpload`.

UploadPartCopy

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

La operación `UploadPartCopy` se implementa con todo el comportamiento de la API DE REST DE Amazon S3. Reservado el derecho a realizar modificaciones.

Esta solicitud lee y escribe los datos de objetos especificados en `x-amz-copy-source-range` el sistema StorageGRID.

Se admiten los siguientes encabezados de solicitud:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Solicitar encabezados para el cifrado del servidor

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

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

Si el objeto de origen se cifra utilizando una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud `UploadPartCopy`, para que el objeto se pueda descifrar y copiar:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar AES256.
- `x-amz-copy-source-server-side-encryption-customer-key`: Especifique la clave de cifrado que proporcionó al crear el objeto de origen.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 que proporcionó cuando creó el objeto de origen.



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones en "["Usar cifrado del servidor"](#)".

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

Respuestas de error

El sistema StorageGRID es compatible con todas las respuestas de error estándar de la API DE REST de S3 que se aplican. Además, la implementación de StorageGRID añade varias respuestas personalizadas.

códigos de error API de S3 admitidos

Nombre	Estado de HTTP
ACCESSDENIED	403 Prohibido
BadDigest	400 solicitud incorrecta
BucketAlreadyExists	409 conflicto
BucketNotEmpty	409 conflicto
IncompleteBody	400 solicitud incorrecta
Internalerror	500 error de servidor interno
InvalidAccessKeyId	403 Prohibido
InvalidArgumentException	400 solicitud incorrecta
InvalidBucketName	400 solicitud incorrecta
InvalidBucketState	409 conflicto
InvalidDigest	400 solicitud incorrecta
InvalidEncryptionAlgorithmError	400 solicitud incorrecta
InvalidPart	400 solicitud incorrecta
InvalidPartOrder	400 solicitud incorrecta

Nombre	Estado de HTTP
InvalidRange	416 rango solicitado no utilizable
InvalidRequest	400 solicitud incorrecta
InvalidStorageClass	400 solicitud incorrecta
InvalidTag	400 solicitud incorrecta
InvalidURI	400 solicitud incorrecta
KeyTooLong	400 solicitud incorrecta
MalformedXML	400 solicitud incorrecta
MetadataTooLarge	400 solicitud incorrecta
MethodNotAllowed	405 método no permitido
MissingContentLength	411 longitud requerida
MissingRequestBodyError	400 solicitud incorrecta
MissingSecurityHeader	400 solicitud incorrecta
NoSuchBucket	404 no encontrado
NoSuchKey	404 no encontrado
NoSuchUpload	404 no encontrado
NotImplimed	501 no implementada
NoSuchBucketPolicy	404 no encontrado
ObjectLockConfigurationNotFoundError	404 no encontrado
Error de precondiciónError	Error de condición 412
RequestTimeTooSowed	403 Prohibido
ServiceUnavailable	503 Servicio no disponible
SignatureDoesNotMatch	403 Prohibido

Nombre	Estado de HTTP
Cucharones TooMany	400 solicitud incorrecta
UserKeyMustBeSpecified	400 solicitud incorrecta

códigos de error personalizados de StorageGRID

Nombre	Descripción	Estado de HTTP
XBucketLifecycleNotAllowed	No se permite la configuración del ciclo de vida de los bloques en un bloque compatible heredado	400 solicitud incorrecta
XBucketPolicyParseException	Error al analizar la política JSON de bloques recibidos.	400 solicitud incorrecta
XCondit. Cumplimiento	Operación denegada debido a la configuración de cumplimiento anterior.	403 Prohibido
XDSLA ReducedRedundancyForbidden	No se permite una redundancia reducida en el bloque compatible con la tecnología heredada	400 solicitud incorrecta
XMaxBucketPolicyLengthExceeded	Su política supera la longitud máxima permitida de la política de bloques.	400 solicitud incorrecta
XMissingInternalRequestHeader	Falta un encabezado de una solicitud interna.	400 solicitud incorrecta
Cumplimiento de XNoSuchBucketCompliance	El bloque especificado no tiene la conformidad heredada activada.	404 no encontrado
XNotAcceptable	La solicitud contiene uno o más encabezados de aceptación que no se han podido satisfacer.	406 no aceptable
XNotImplemed	La solicitud que ha proporcionado implica una funcionalidad que no se ha implementado.	501 no implementada

Operaciones personalizadas de StorageGRID

Operaciones personalizadas de StorageGRID

El sistema StorageGRID admite operaciones personalizadas que se añaden a la API DE REST DE la versión S3.

La siguiente tabla enumera las operaciones personalizadas que admite StorageGRID.

Funcionamiento	Descripción
"OBTENGA coherencia de bloques"	Devuelve la coherencia aplicada a un bloque determinado.
"PONGA la consistencia del cucharón"	Establece la coherencia aplicada a un bloque determinado.
"GET Bucket última hora de acceso"	Devuelve si las actualizaciones del último tiempo de acceso están habilitadas o deshabilitadas para un bloque en particular.
"PUT Bucket última hora de acceso"	Permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para un bloque en particular.
"Configuración de notificaciones de metadatos de DELETE Bucket"	Elimina el XML de configuración de notificación de metadatos asociado a un bloque en particular.
"OBTENGA la configuración de notificación de metadatos del bloque de datos"	Devuelve el XML de configuración de notificación de metadatos asociado a un bloque determinado.
"Configuración de notificaciones de metadatos de PUT Bucket"	Configura el servicio de notificación de metadatos para un bloque.
"Obtenga el uso del almacenamiento"	Indica la cantidad total de almacenamiento que utiliza una cuenta y para cada depósito asociado a la cuenta.
"Obsoleto: CreateBucket con configuración de cumplimiento"	Obsoleto y no compatible: Ya no puede crear nuevos bloques con el cumplimiento de normativas habilitado.
"En desuso: OBTENGA el cumplimiento de normativas de bloques"	Obsoleto pero compatible: Devuelve la configuración de cumplimiento vigente para un bloque compatible existente.
"Obsoleto: PUT Bucket Compliance"	Obsoleto pero compatible: Permite modificar la configuración de cumplimiento de un bloque compatible heredado.

OBTENGA coherencia de bloques

La solicitud OBTENER coherencia de bloques permite determinar la coherencia que se aplica a un bloque en particular.

La consistencia predeterminada se establece en garantía de lectura tras escritura para los objetos recién creados.

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

Ejemplo de solicitud

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

Respuesta

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

Coherencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.
fuerte en todo el mundo	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
sitio seguro	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
lectura-después-nueva-escritura	(Predeterminado) proporciona coherencia de lectura tras escritura para los nuevos objetos y coherencia final para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
disponible	Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Ejemplo de respuesta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-new-write</Consistency>
```

Información relacionada

["Coherencia"](#)

PONGA la consistencia del cucharón

La solicitud COLOCAR coherencia de bloques permite especificar la coherencia que se debe aplicar a las operaciones realizadas en un bloque.

La consistencia predeterminada se establece en garantía de lectura tras escritura para los objetos recién creados.

Antes de empezar

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

Solicitud

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

Coherencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.
fuerte en todo el mundo	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
sitio seguro	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
lectura-después-nueva-escritura	(Predeterminado) proporciona coherencia de lectura tras escritura para los nuevos objetos y coherencia final para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
disponible	Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Nota: En general, debes usar la consistencia de “Leer después de la nueva escritura”. Si las solicitudes no funcionan correctamente, cambie el comportamiento del cliente de aplicación si es posible. O bien, configure el cliente para especificar la consistencia de cada solicitud API. Defina la consistencia en el nivel del cucharón sólo como último recurso.

Ejemplo de solicitud

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

Información relacionada

["Coherencia"](#)

GET Bucket última hora de acceso

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

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

Ejemplo de solicitud

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

Ejemplo de respuesta

Este ejemplo muestra que las actualizaciones de la última hora de acceso están habilitadas para el bloque.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

PUT Bucket última hora de acceso

La solicitud DE la última hora de acceso al bloque DE PUT permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para bloques individuales. Al

deshabilitar las actualizaciones de la última hora de acceso, se mejora el rendimiento, y es la configuración predeterminada para todos los bloques creados con la versión 10.3.0 o posterior.

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

A partir de la versión 10.3 de StorageGRID, las actualizaciones de la última hora de acceso se deshabilitan de forma predeterminada para todos los bloques nuevos. Si tiene bloques que se crearon con una versión anterior de StorageGRID y desea coincidir con el nuevo comportamiento predeterminado, debe deshabilitar explícitamente las actualizaciones de la última hora de acceso para cada uno de esos bloques anteriores. Puede activar o desactivar las actualizaciones en la hora del último acceso mediante la solicitud de hora de último acceso de PUT Bucket o desde la página de detalles de un bucket en el gestor de inquilinos. Consulte ["Activar o desactivar las actualizaciones de la hora del último acceso"](#).

Si se desactivan las actualizaciones de la última hora de acceso para un bloque, se aplicará el siguiente comportamiento a las operaciones del bloque:

- Las solicitudesGetObject,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 solicitudesCopyObject y PutObjectTagging que actualizan solo los metadatos también actualizan la hora de último acceso. El objeto se agrega a las colas para la evaluación de ILM.
- Si las actualizaciones de la hora del último acceso están deshabilitadas para el bloque de origen, las solicitudes deCopyObject no actualizan la hora del último acceso para el bloque de origen. El objeto que se copió no se agrega a colas para la evaluación de ILM para el bloque de origen. Sin embargo, para el destino, las solicitudes deCopyObject siempre actualizan la hora del último acceso. La copia del objeto se agrega a las colas para la evaluación de ILM.
- Las solicitudes deCompleteMultipartUpload actualizan la hora del último acceso. El objeto completado se agrega a las colas para la evaluación de ILM.

Solicitar ejemplos

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

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

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

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

Configuración de notificaciones de metadatos de DELETE Bucket

La solicitud de configuración DE notificación DE metadatos DELETE Bucket permite deshabilitar el servicio de integración de búsqueda para bloques individuales al eliminar el XML de configuración.

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

Ejemplo de solicitud

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

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

OBTENGA la configuración de notificación de metadatos del bloque de datos

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

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

Ejemplo de solicitud

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

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

Respuesta

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

```

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

```

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

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	<p>Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos.</p> <p>Contiene uno o más elementos Regla.</p>	Sí
Regla	<p>Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado.</p> <p>Se rechazan las reglas con prefijos superpuestos.</p> <p>Incluido en el elemento MetadataNotificationConfiguration.</p>	Sí
ID	<p>Identificador único de la regla.</p> <p>Incluido en el elemento Regla.</p>	No
Estado	<p>El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas.</p> <p>Incluido en el elemento Regla.</p>	Sí

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

Ejemplo de respuesta

El XML incluido entre las

```
<MetadataNotificationConfiguration></MetadataNotificationConfiguration>
```

etiquetas muestra cómo se configura la integración con un punto final de integración de búsqueda para el bloque. En este ejemplo, los metadatos del objeto se envían a un índice de Elasticsearch denominado `current` y tipo denominado `2017` que se aloja en un dominio de AWS denominado `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Información relacionada

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

Configuración de notificaciones de metadatos de PUT Bucket

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

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

Solicitud

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

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, puede enviar metadatos para objetos con el prefijo /images a un destino y los objetos con el prefijo /videos a otro.

Las configuraciones que tienen prefijos superpuestos no son válidas y se rechazan cuando se envían. Por ejemplo, no se permitiría una configuración que incluyera una regla para objetos con el prefijo test y una segunda regla para objetos con el prefijo test2.

Los destinos se deben especificar con el URN de un extremo de StorageGRID. El punto final debe existir

cuando se ejecuta la configuración de notificación de metadatos o la solicitud falla como A. 400 Bad Request El mensaje de error indica: Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: *URN*.

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

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

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

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

Solicitar ejemplos

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

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

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

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

```

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

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

```

JSON generado por el servicio de integración de búsqueda

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

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

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

Metadatos de objetos incluidos en las notificaciones de metadatos

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

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

Tipo	Nombre del elemento	Descripción
Información sobre bloques y objetos	cucharón	Nombre del bloque
Información sobre bloques y objetos	clave	Nombre de clave de objeto
Información sobre bloques y objetos	ID de versión	Versión de objeto, para objetos en bloques con versiones
Información sobre bloques y objetos	región	Región de bloque, por ejemplo us-east-1
Metadatos del sistema	tamaño	Tamaño del objeto (en bytes) visible para un cliente HTTP
Metadatos del sistema	md5	Hash de objeto
Metadatos del usuario	metadatos <i>key:value</i>	Todos los metadatos de usuario del objeto, como pares clave-valor

Tipo	Nombre del elemento	Descripción
Etiquetas	etiquetas <i>key:value</i>	Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor



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

Información relacionada

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

OBTENGA la solicitud de uso del almacenamiento

La solicitud GET Storage Usage le indica la cantidad total de almacenamiento que está usando una cuenta y por cada bloque asociado con la cuenta.

La cantidad de almacenamiento utilizada por una cuenta y sus depósitos se puede obtener mediante una solicitud de ListBuckets modificada con el `x-ntap-sg-usage` parámetro de consulta. Se realiza un seguimiento del uso del almacenamiento en bloques de forma independiente de las solicitudes DE PUT y DELETE procesadas por el sistema. Es posible que haya algún retraso antes de que los valores de uso coincidan con los valores esperados en función del procesamiento de las solicitudes, especialmente si el sistema está sometido a cargas pesadas.

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

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

Ejemplo de solicitud

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

Ejemplo de respuesta

Este ejemplo muestra una cuenta que tiene cuatro objetos y 12 bytes de datos en dos bloques. Cada bloque contiene dos objetos y seis bytes de datos.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Creación de versiones

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

Información relacionada

["Coherencia"](#)

Solicitudes de bloque obsoletas para cumplimiento de normativas heredadas

Solicitudes de bloque obsoletas para cumplimiento de normativas heredadas

Es posible que deba utilizar la API DE REST de StorageGRID S3 para gestionar los bloques creados con la función de cumplimiento heredada.

Función de cumplimiento de normativas obsoleta

La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3.

Si anteriormente habilitó la configuración de cumplimiento global, la opción de bloqueo de objetos S3 global se habilita en StorageGRID 11.6. Ya no se pueden crear nuevos bloques con la función de cumplimiento habilitada; sin embargo, según sea necesario, se puede utilizar la API DE REST de StorageGRID S3 para gestionar bloques existentes que cumplen las normativas.

- ["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)
- ["Gestión de objetos con ILM"](#)
- ["Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"](#)

Solicitudes de cumplimiento de normativas obsoletas:

- ["Obsoleto: PONGA modificaciones de solicitud de cucharón para el cumplimiento"](#)

El elemento XML de SGCompliance está obsoleto. Anteriormente, podría incluir este elemento personalizado de StorageGRID en el cuerpo de solicitud XML opcional de SOLICITUDES PUT Bucket para crear un bloque compatible.

- ["Obsoleto: OBTENER cumplimiento de bloques"](#)

La solicitud de cumplimiento de normativas GET Bucket quedó obsoleta. Sin embargo, puede seguir utilizando esta solicitud para determinar la configuración de cumplimiento actual para un bloque compatible heredado existente.

- ["Obsoleto: Cumplimiento de PUT Bucket"](#)

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

Obsoleto: Modificaciones de la solicitud de CreateBucket para el cumplimiento

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

La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3. En la siguiente sección, se ofrecen más detalles:



- ["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)
- ["Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"](#)

Ya no se pueden crear bloques nuevos con el cumplimiento de normativas habilitado. Se devuelve el siguiente mensaje de error si intenta utilizar las modificaciones de solicitud de CreateBucket para la conformidad con el fin de crear un nuevo depósito compatible:

The Compliance feature is deprecated.

Contact your StorageGRID administrator if you need to create new Compliant buckets.

Obsoleto: OBTENER solicitud de cumplimiento de bloques

La solicitud de cumplimiento de normativas GET Bucket quedó obsoleta. Sin embargo, puede seguir utilizando esta solicitud para determinar la configuración de cumplimiento actual para un bloque compatible heredado existente.

 La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3. En la siguiente sección, se ofrecen más detalles:

- ["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)
- ["Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"](#)

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

Ejemplo de solicitud

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

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

Ejemplo de respuesta

En el XML de respuesta, <SGCompliance> muestra la configuración de cumplimiento vigente para el bloque. Esta respuesta de ejemplo muestra la configuración de cumplimiento de un bloque en el que se conservará cada objeto durante un año (525,600 minutos), a partir del momento en que el objeto se ingiere en la cuadrícula. Actualmente, no existe ningún derecho legal en este segmento. Cada objeto se eliminará automáticamente después de un año.

```

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

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

```

Nombre	Descripción
RetentionPeriodonMinutes	La duración del período de retención para los objetos que se añadió a este bloque, en minutos. El período de retención se inicia cuando el objeto se ingiere en la cuadrícula.
LegalHold	<ul style="list-style-type: none"> Cierto: Este segmento está actualmente bajo un control legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la conservación legal, incluso si ha caducado su período de retención. Falso: Este segmento no está actualmente bajo un derecho. Los objetos de este bloque se pueden eliminar cuando expire su período de retención.
Eliminación automática	<ul style="list-style-type: none"> True: Los objetos de este bloque se eliminarán automáticamente cuando expire su período de retención, a menos que el bloque se encuentre bajo una retención legal. False: Los objetos de este bloque no se eliminarán automáticamente cuando finalice el período de retención. Debe eliminar estos objetos manualmente si necesita eliminarlos.

Respuestas de error

Si el depósito no se ha creado para que sea compatible, el código de estado HTTP de la respuesta es 404 Not Found, con un código de error S3 XNoSuchBucketCompliance .

Obsoleto: Solicitud de cumplimiento de bloques PUT

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

 La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3. En la siguiente sección, se ofrecen más detalles:

- ["Use la API REST DE S3 para configurar el bloqueo de objetos de S3"](#)
- ["Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"](#)

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

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

Ejemplo de solicitud

Esta solicitud de ejemplo modifica la configuración de cumplimiento para el depósito denominado `mybucket`. En este ejemplo, los objetos de `mybucket` ahora se conservarán durante dos años (1.051.200 minutos) en lugar de un año, a partir del momento en que el objeto se ingiere en la cuadrícula. No existe ningún derecho legal en este segmento. Cada objeto se eliminará automáticamente después de dos años.

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

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

Nombre	Descripción
RetentionPeriodonMinutes	<p>La duración del período de retención para los objetos que se añadió a este bloque, en minutos. El período de retención se inicia cuando el objeto se ingiere en la cuadrícula.</p> <p>Importante Al especificar un nuevo valor para <code>RetentionPeriodMinutes</code>, debe especificar un valor que sea igual o mayor que el período de retención actual del bucket. Después de definir el período de retención del depósito, no puede disminuir ese valor; solo puede aumentarlo.</p>

Nombre	Descripción
LegalHold	<ul style="list-style-type: none"> • Ciento: Este segmento está actualmente bajo un control legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la conservación legal, incluso si ha caducado su período de retención. • Falso: Este segmento no está actualmente bajo un derecho. Los objetos de este bloque se pueden eliminar cuando expire su período de retención.
Eliminación automática	<ul style="list-style-type: none"> • True: Los objetos de este bloque se eliminarán automáticamente cuando expire su período de retención, a menos que el bloque se encuentre bajo una retención legal. • False: Los objetos de este bloque no se eliminarán automáticamente cuando finalice el período de retención. Debe eliminar estos objetos manualmente si necesita eliminarlos.

Consistencia para la configuración de cumplimiento

Cuando se actualiza la configuración de cumplimiento de normativas para un bloque de S3 con una solicitud DE cumplimiento PUT Bucket, StorageGRID intenta actualizar los metadatos del bloque en el grid. De forma predeterminada, StorageGRID utiliza la consistencia **strong-global** para garantizar que todos los sitios del centro de datos y todos los nodos de almacenamiento que contienen metadatos del depósito tengan consistencia de lectura tras escritura para los ajustes de cumplimiento modificados.

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

Si recibe esta respuesta, debe ponerse en contacto con el administrador de grid para garantizar que los servicios de almacenamiento requeridos estén disponibles en lo antes posible.. Si el administrador de grid no puede poner a disposición suficientes nodos de almacenamiento en cada sitio, el soporte técnico puede indicarle que vuelva a intentar la solicitud fallida forzando la consistencia del **sitio fuerte**.



Nunca fuerce la consistencia de **strong-site** para el cumplimiento de PUT bucket a menos que se le haya indicado hacerlo por el soporte técnico y a menos que comprenda las posibles consecuencias de usar este nivel.

Cuando la consistencia se reduce a **strong-site**, StorageGRID garantiza que la configuración de cumplimiento actualizada tendrá consistencia de lectura tras escritura solo para las solicitudes de los clientes dentro de un sitio. Esto significa que el sistema StorageGRID podría tener temporalmente varias configuraciones incoherentes para este bloque hasta que todos los sitios y nodos de almacenamiento estén disponibles. La configuración incoherente puede dar como resultado un comportamiento inesperado y no deseado. Por ejemplo, si va a colocar un bloque bajo una conservación legal y fuerza una menor coherencia, la configuración de cumplimiento anterior del bloque (es decir, la retención legal) puede seguir vigente en algunos sitios del centro de datos. Como resultado, los objetos que cree que están en retención legal se pueden eliminar cuando caduque su período de retención, ya sea por el usuario o por AutoDelete, si está activado.

Para forzar el uso de la consistencia **strong-site**, vuelva a emitir la solicitud de cumplimiento de PUT Bucket e incluya Consistency-Control el encabezado de solicitud HTTP, de la siguiente manera:

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

Respuestas de error

- Si el depósito no se ha creado para ser compatible, el código de estado HTTP para la respuesta es 404 Not Found.
- Si RetentionPeriodMinutes en la solicitud es inferior al período de retención actual del depósito, el código de estado HTTP es 400 Bad Request.

Información relacionada

"[Obsoleto: PONGA modificaciones de solicitud de cucharón para el cumplimiento](#)"

Administrar políticas de acceso

Utilizar políticas de acceso

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

Información general sobre las políticas de acceso

StorageGRID admite tres tipos de políticas de acceso:

- **Políticas de cubo**, que se administran mediante las operaciones de la API GetBucketPolicy, PutBucketPolicy y DeleteBucketPolicy S3 o el administrador de inquilinos o la API de administración de inquilinos. Las políticas de bloque se asocian a bloques, por lo que se configuran para controlar el acceso de los usuarios de la cuenta de propietario del bloque u otras cuentas al bloque y a los objetos en él. La política de bloques se aplica únicamente a un bloque y, posiblemente, a varios grupos.
- **Políticas de grupo**, que se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Las directivas de grupo se asocian a un grupo de la cuenta, por lo que se configuran para permitir que dicho grupo tenga acceso a recursos específicos propiedad de dicha cuenta. La política de grupo se aplica únicamente a un grupo y, posiblemente, a varios bloques.
- **Políticas de sesión**, que se incluyen como parte de la realización de una solicitud AssumeRole. Las políticas de sesión solo se aplican a la sesión determinada, definiendo además los permisos que tiene el usuario, además de aquellos otorgados por la política de grupo y de depósito.



No hay diferencia de prioridad entre las políticas de grupo, de depósito y de sesión.

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

- ID de sentencia (Sid) (opcional)

- Efecto
- Principal/NotPrincipal
- Recurso/NotResource
- Acción/NotAction
- Condición (opcional)

Las sentencias de directiva se crean utilizando esta estructura para especificar permisos: Conceda <Effect> para permitir/denegar que <Principal> ejecute <Action> en <Resource> cuando se aplique <Condition>.

Cada elemento de directiva se utiliza para una función específica:

Elemento	Descripción
SID	El elemento Sid es opcional. El Sid sólo se ha diseñado como una descripción para el usuario. El sistema StorageGRID lo almacena pero no lo interpreta.
Efecto	Utilice el elemento Effect para establecer si se permiten o deniegan las operaciones especificadas. Debe identificar las operaciones que permite (o deniega) en cubos u objetos utilizando las palabras clave del elemento Acción admitido.
Principal/NotPrincipal	Puede permitir a los usuarios, grupos y cuentas acceder a recursos específicos y realizar acciones específicas. Si no se incluye ninguna firma S3 en la solicitud, se permite el acceso anónimo especificando el carácter comodín (*) como principal. De forma predeterminada, sólo la raíz de la cuenta tiene acceso a los recursos que pertenecen a la cuenta. Sólo es necesario especificar el elemento Principal en una política de bloque. Para las directivas de grupo, el grupo al que se asocia la directiva es el elemento Principal implícito.
Recurso/NotResource	El elemento Resource identifica los bloques y los objetos. Puede permitir o denegar permisos para cubos y objetos utilizando el nombre de recurso de Amazon (ARN) para identificar el recurso.
Acción/NotAction	Los elementos Acción y efecto son los dos componentes de los permisos. Cuando un grupo solicita un recurso, se le concede o se le deniega el acceso al recurso. Se deniega el acceso a menos que asigne permisos de forma específica, pero puede utilizar Denegar explícito para anular un permiso otorgado por otra directiva.
Condición	El elemento Condition es opcional. Las condiciones permiten crear expresiones para determinar cuándo se debe aplicar una directiva.

En el elemento Action , puede utilizar el carácter comodín (*) para especificar todas las operaciones o un subconjunto de operaciones. Por ejemplo, esta acción coincide con permisos como s3:GetObject, s3:PutObject y s3:DeleteObject.

```
s3:*Object
```

En el elemento Resource , puede utilizar los caracteres comodín (*) y (?). Aunque el asterisco (*) coincide con 0 o más caracteres, el signo de interrogación (?) coincide con cualquier carácter.

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

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

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

En el ejemplo siguiente, la instrucción utiliza los elementos Effect, Principal, Acción y recurso. En este ejemplo se muestra una sentencia de política de bloque completa que utiliza el efecto Permitir para otorgar a los principales, al grupo de administración federated-group/admin y al grupo financiero federated-group/finance , permisos para realizar la acción s3>ListBucket en el bloque denominado mybucket y la acción s3GetObject en todos los objetos de ese bloque.

```
{  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": [  
          "arn:aws:iam::27233906934684427525:federated-group/admin",  
          "arn:aws:iam::27233906934684427525:federated-group/finance"  
        ]  
      },  
      "Action": [  
        "s3>ListBucket",  
        "s3GetObject"  
      ],  
      "Resource": [  
        "arn:aws:s3:::mybucket",  
        "arn:aws:s3:::mybucket/*"  
      ]  
    }  
  ]  
}
```

La política de bloque tiene un límite de tamaño de 20,480 bytes y la política de grupo tiene un límite de tamaño de 5,120 bytes.

Coherencia de las políticas

De forma predeterminada, cualquier actualización que realice a las directivas de grupo será consistente. Cuando una normativa de grupo es coherente, los cambios pueden tardar 15 minutos adicionales en aplicarse debido al almacenamiento en caché de la política. Por defecto, cualquier actualización que realice en las políticas de depósito es fuertemente coherente.

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

En este caso, puede establecer `Consistency-Control` el encabezado en la solicitud PutBucketPolicy, o puede utilizar la solicitud de consistencia PUT Bucket. Cuando una política de depósito es coherente, los cambios pueden tardar 8 segundos adicionales en aplicarse debido al almacenamiento en caché de la política.

 Si establece la consistencia en un valor diferente para resolver una situación temporal, asegúrese de volver a establecer el valor de nivel de cubo en su valor original cuando haya terminado. De lo contrario, todas las solicitudes de bloque futuras utilizarán la configuración modificada.

¿Qué es la política de sesión?

Una política de sesión es una política de acceso que restringe temporalmente los permisos disponibles durante una sesión específica, como cuando un usuario asume un grupo. Una política de sesión solo puede permitir un subconjunto de permisos y no puede otorgar permisos adicionales. El propio grupo podría tener permisos más amplios.

Utilice ARN en las declaraciones de política

En las declaraciones de política, el ARN se utiliza en los elementos Principal y Recursos.

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

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

- Utilice esta sintaxis para especificar el recurso de identidad ARN (usuarios y grupos):

```
arn:aws:iam::account_id:root  
arn:aws:iam::account_id:user/user_name  
arn:aws:iam::account_id:group/group_name  
arn:aws:iam::account_id:federated-user/user_name  
arn:aws:iam::account_id:federated-group/group_name
```

Otras consideraciones:

- Puede utilizar el asterisco (*) como comodín para que coincida con cero o más caracteres dentro de la clave de objeto.
- Los caracteres internacionales, que se pueden especificar en la clave de objeto, deben codificarse

mediante JSON UTF-8 o mediante secuencias de escape JSON \u. No se admite el porcentaje de codificación.

["Sintaxis de URN RFC 2141"](#)

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

Especifique recursos en una política

En las sentencias de directiva, puede utilizar el elemento Resource para especificar el bloque o el objeto para el que se permiten o deniegan los permisos.

- Cada instrucción de directiva requiere un elemento Resource. En una política, los recursos se indican con el elemento Resource, o alternativamente, NotResource para la exclusión.
- Se especifican recursos con un ARN de recurso S3. Por ejemplo:

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

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

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

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

Especifique los principales en una directiva

Utilice el elemento Principal para identificar al usuario, grupo o cuenta de arrendatario que la sentencia de directiva permite o deniega el acceso al recurso.

- Cada sentencia de política de una política de bloque debe incluir un elemento Principal. Las sentencias de política de una política de grupo no necesitan el elemento Principal porque se entiende que el grupo es el principal.
- En una política, los principales se denotan por el elemento Principal o, alternativamente, NotPrincipal para la exclusión.
- Las identidades basadas en cuentas se deben especificar mediante un ID o un ARN:

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

- En este ejemplo se utiliza el ID de cuenta de inquilino 27233906934684427525, que incluye la raíz de la cuenta y todos los usuarios de la cuenta:

```
"Principal": { "AWS": "27233906934684427525" }
```

- Puede especificar sólo la raíz de la cuenta:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Puede especificar un usuario federado específico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-user/Alex" }
```

- Puede especificar un grupo federado específico ("managers"):

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

- Puede especificar un principal anónimo:

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

- Para evitar ambigüedades, puede utilizar el UUID de usuario en lugar del nombre de usuario:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

Por ejemplo, supongamos que Alex abandona la organización y se elimina el nombre de usuario Alex. Si un nuevo Alex se une a la organización y se le asigna el mismo Alex nombre de usuario, el nuevo usuario podría heredar involuntariamente los permisos otorgados al usuario original.

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

Especificar permisos en una directiva

En una directiva, el elemento Acción se utiliza para permitir/denegar permisos a un recurso. Hay un conjunto de permisos que puede especificar en una directiva, que se indican mediante el elemento "Acción" o, alternativamente, "NotAction" para la exclusión. Cada uno de estos elementos se asigna a operaciones de API de REST de S3 específicas.

En las tablas se enumeran los permisos que se aplican a los bloques y los permisos que se aplican a los objetos.

 Amazon S3 ahora usa el permiso S3:PutReplicationConfiguration para las acciones PutBucketReplication y DeleteBucketReplication. StorageGRID utiliza permisos independientes para cada acción, que coinciden con la especificación original de Amazon S3.



Se realiza una supresión cuando se utiliza una PUT para sobrescribir un valor existente.

Permisos que se aplican a los bloques

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:CreateBucket	CreateBucket	Sí. Nota: Usar solo en la política de grupo.
s3:DeleteBucket	DeleteBucket	
s3:DeleteBucketMetadataNotification	Configuración de notificaciones de metadatos de DELETE Bucket	Sí
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBucketReplication	Sí, separe los permisos para PUT y DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	CUMPLIMIENTO de GET Bucket (obsoleto)	Sí
s3:GetBucketConsistency	OBTENGA coherencia de bloques	Sí
s3: GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	GET Bucket última hora de acceso	Sí
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	OBTENGA la configuración de notificación de metadatos del bloque de datos	Sí
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:GetBucketTagging	Etiquetado de GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3>ListAllMyBuckets	<ul style="list-style-type: none"> • ListCuchers • Obtenga el uso del almacenamiento 	Sí, para OBTENER uso de almacenamiento. Nota: Usar solo en la política de grupo.
s3>ListBucket	<ul style="list-style-type: none"> • ListObjects • Segmento de cabeza • RestoreObject 	
s3>ListBucketMultipartUploads	<ul style="list-style-type: none"> • ListCargas multipartitas • RestoreObject 	
s3>ListBucketVersions	OBTENGA las versiones DE Bucket	
s3:PutBucketCompliance	CUMPLIMIENTO de PUT Bucket (obsoleto)	Sí
s3:PutBucketConsistency	PONGA la consistencia del cucharón	Sí
s3: PutBucketCORS	<ul style="list-style-type: none"> • DeleteBucketCors† • A cargo de PutBucketCors 	
s3:PutEncryptionConfiguration	<ul style="list-style-type: none"> • DeleteBucketEncryption • PutBucketEncryption 	
s3:PutBucketLastAccessTime	PUT Bucket última hora de acceso	Sí
s3:PutBucketMetadataNotification	Configuración de notificaciones de metadatos de PUT Bucket	Sí
s3:PutBucketNotification	PutBucketNotificationConfiguration	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> CreateBucket con x-amz-bucket-object-lock-enabled: true en el encabezado de solicitud (también requiere el permiso S3:CreateBucket) PutObjectLockConfiguration 	
s3:PutBucketPolicy	Política de PutBucketPolicy	
s3:PutBucketEtiquetado	<ul style="list-style-type: none"> DeleteBucketTagging† PutBucketTagging 	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	<ul style="list-style-type: none"> DeleteBucketLifecycle† PutBucketLifecycleConfiguration 	
s3:PutReplicationConfiguration	PutBucketReplication	Sí, separe los permisos para PUT y DELETE

Permisos que se aplican a objetos

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:AbortMultipartUpload	<ul style="list-style-type: none"> AbortMultipartUpload RestoreObject 	
s3:BypassGovernanceRetention	<ul style="list-style-type: none"> DeleteObject DeleteObjects PutObjectRetention 	
s3:DeleteObject	<ul style="list-style-type: none"> DeleteObject DeleteObjects RestoreObject 	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (una versión específica del objeto)	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:DeleteObjectVersion	DeleteObject (una versión específica del objeto)	
s3:GetObject	<ul style="list-style-type: none"> • GetObject • Objeto principal • RestoreObject • SelectObjectContent 	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectEtiquetado	
s3:GetObjectVersionTagging	GetObjectTagging (una versión específica del objeto)	
s3:GetObjectVersion	GetObject (una versión específica del objeto)	
s3>ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	<ul style="list-style-type: none"> • Objeto de puta • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy 	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectEtiquetado	PutObjectEtiquetado	
s3:PutObjectVersionEtiquetado	PutObjectTagging (una versión específica del objeto)	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:PutOverwriteObject	<ul style="list-style-type: none"> • Objeto de puta • CopyObject • PutObjectEtiquetado • DeleteObjectTagging • CompleteMultipartUpload 	Sí
s3:RestoreObject	RestoreObject	

Utilice el permiso PutOverwriteObject

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

Entre los posibles ajustes para este permiso se incluyen:

- **Permitir:** El cliente puede sobrescribir un objeto. Esta es la configuración predeterminada.
- **Denegar:** El cliente no puede sobrescribir un objeto. Cuando se establece en Denegar, el permiso PutOverwriteObject funciona de la siguiente manera:
 - Si se encuentra un objeto existente en la misma ruta:
 - Los datos del objeto, los metadatos definidos por el usuario o el etiquetado de objetos S3 no se pueden sobrescribir.
 - Se cancela cualquier operación de ingestión en curso y se devuelve un error.
 - Si el control de versiones S3 está activado, la configuración Denegar impide que las operaciones PutObjectTagging o DeleteObjectTagging modifiquen el TagSet para un objeto y sus versiones no actuales.
 - Si no se encuentra un objeto existente, este permiso no tiene efecto.
- Cuando este permiso no está presente, el efecto es el mismo que si se estableció permitir.

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

Especificar condiciones en una política

Las condiciones definen cuándo estará en vigor una política. Las condiciones consisten en operadores y pares clave-valor.

Condiciones Utilice pares clave-valor para la evaluación. Un elemento Condition puede contener varias condiciones y cada condición puede contener varios pares clave-valor. El bloque Condition utiliza el siguiente formato:

```

Condition: {
    condition_type: {
        condition_key: condition_values
}

```

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

```

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

```

Operadores de condición admitidos

Los operadores de condición se categorizan de la siguiente manera:

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

Operadores de condición	Descripción
StringEquals	Compara una clave con un valor de cadena basado en la coincidencia exacta (distingue entre mayúsculas y minúsculas).
StringNotEquals	Compara una clave con un valor de cadena basado en la coincidencia negada (distingue entre mayúsculas y minúsculas).
StringEqualIgnoreCase	Compara una clave con un valor de cadena basado en la coincidencia exacta (omite Case).
StringNotEqualIgnoreCase	Compara una clave con un valor de cadena basado en la coincidencia negada (omite Case).
StringLike	Compara una clave con un valor de cadena basado en la coincidencia exacta (distingue entre mayúsculas y minúsculas). Puede incluir caracteres comodín * y ?.
StringNotLike	Compara una clave con un valor de cadena basado en la coincidencia negada (distingue entre mayúsculas y minúsculas). Puede incluir caracteres comodín * y ?.

Operadores de condición	Descripción
Valores numéricos	Compara una clave con un valor numérico basado en la coincidencia exacta.
NumericNotEquals	Compara una clave con un valor numérico basado en la coincidencia negada.
NumericGreaterthan	Compara una clave con un valor numérico basado en la coincidencia mayor que.
NumericGreaterThanOrEqualTo	Compara una clave con un valor numérico en función de la coincidencia mayor o igual que.
NumericLessThan	Compara una clave con un valor numérico basado en la coincidencia menor que.
NumericLessThanOrEqualTo	Compara una clave con un valor numérico en función de la coincidencia menor o igual que.
Bool	Compara una clave con un valor booleano basado en la coincidencia “true o false”.
IPAddress	Compara una clave con una dirección IP o un rango de direcciones IP.
NotIpAddress	Compara una clave con una dirección IP o un intervalo de direcciones IP basándose en la coincidencia negada.
Nulo	Comprueba si hay una clave de condición en el contexto actual de la solicitud.
Si existe	Se agrega a cualquier operador de condición, excepto la condición Nula, para verificar la ausencia de esa clave de condición. Devuelve VERDADERO si la clave de condición no está presente.

Teclas de condición compatibles

Teclas de condición	Acciones	Descripción
aws:SourceIp	Operadores IP	<p>Comparará con la dirección IP desde la que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos.</p> <p>Nota: Si la solicitud S3 se envió a través del servicio Load Balancer en nodos Admin y nodos de Gpuertas de enlace, se comparará con la dirección IP anterior al servicio Load Balancer.</p> <p>Nota: Si se utiliza un equilibrador de carga no transparente de terceros, se comparará con la dirección IP de ese equilibrador de carga. Cualquier X-Forwarded-For encabezado se ignorará porque no se puede determinar su validez.</p>
aws:nombre de usuario	Recurso/identidad	Comparará con el nombre de usuario del remitente desde el que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos.
s3:delimitador	s3>ListBucket y. s3>ListBucketVersions permisos	Se comparará con el parámetro delimitador especificado en una solicitud ListObjects o ListObjectVersions.
S3:ExistingObjectTag/<tag-key>	s3>DeleteObjectTagging s3>DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl s3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging S3:PutObjectAcl s3:PutObjectEtiquetado S3:PutObjectVersionAcl s3:PutObjectVersionEtiquetado	Requerirá que el objeto existente tenga la clave de etiqueta y el valor específicos.

Teclas de condición	Acciones	Descripción
s3:max-keys	s3>ListBucket y. s3>ListBucketVersions permisos	Se compara con el parámetro max-keys especificado en una solicitud ListObjects o ListObjectVersions.
s3: modo de bloqueo de objeto	s3:PutObject	Se compara con el object-lock-mode ampliado desde el encabezado de solicitud en la solicitud PutObject, CopyObject y CreateMultipartUpload.
s3: modo de bloqueo de objeto	s3:PutObjectRetention	Se compara con el object-lock-mode ampliado desde el cuerpo XML en la solicitud PutObjectRetention.
s3:retención-días restante del bloqueo de objetos	s3:PutObject	Se compara con la fecha de retención especificada en x-amz-object-lock-retain-until-date la cabecera de solicitud o calculada a partir del período de retención por defecto de período para asegurarse de que estos valores se encuentran dentro del rango permitido para las siguientes solicitudes: <ul style="list-style-type: none"> • Objeto de puta • CopyObject • CreateMultipartUpload
s3:retención-días restante del bloqueo de objetos	s3:PutObjectRetention	Se compara con la fecha de retención especificada en la solicitud PutObjectRetention para asegurarse de que se encuentra dentro del rango permitido.
s3:prefijo	s3>ListBucket y. s3>ListBucketVersions permisos	Se comparará con el parámetro PreFIX especificado en una solicitud ListObjects o ListObjectVersions.
S3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectEtiquetado s3:PutObjectVersionEtiquetado	Requerirá una clave y un valor de etiqueta específicos cuando la solicitud del objeto incluya el etiquetado.
algoritmo de cifrado del lado del servidor s3:x-amz para el cliente	s3:PutObject	Se compara con el sse-customer-algorithm o al copy-source-sse-customer-algorithm ampliado desde el encabezado de solicitud en la solicitud PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy y CompleteMultipartUpload.

Especifique las variables en una política

Las variables de las directivas se pueden utilizar para llenar la información de directivas cuando esté disponible. Puede utilizar variables de política en el `Resource` elemento y en comparaciones de cadenas en el `Condition` elemento.

En este ejemplo, la variable `#{aws:username}` forma parte del elemento `Resource`:

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

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

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

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

Crear directivas que requieran un manejo especial

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

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

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
Policy otorga a una cuenta no propietaria (incluidas las cuentas anónimas) permisos para colocar objetos.	Cucharón	Válido. Los objetos son propiedad de la cuenta creadora y la política de bucket no se aplica. La cuenta de creador debe otorgar permisos de acceso al objeto mediante ACL de objeto.	Válido. Los objetos son propiedad de la cuenta de propietario del bloque. Se aplica la política de bloques.

Protección WORM (escritura única lectura múltiple)

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

Para asegurarse de que las sobrescrituras se deniegan siempre, puede:

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



Si se configura DeleteObject como DENEGADO en una política de S3, ILM no impide que elimine objetos cuando existe una regla como «copias cero tras 30 días».



Incluso cuando se aplican todas estas reglas y políticas, no protegen frente a escrituras simultáneas (consulte la situación A). Protegen contra sobrescrituras completadas secuenciales (consulte la situación B).

Situación A: Escrituras simultáneas (no protegidas contra)

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

Situación B: Sobrescrituras completadas secuenciales (protegidas contra)

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

Información relacionada

- "Cómo gestionan las reglas de ILM de StorageGRID los objetos"
- "Ejemplo de políticas de bloque"
- "Ejemplo de políticas de grupo"
- "Ejemplo de política de sesión"
- "Gestión de objetos con ILM"
- "Usar una cuenta de inquilino"

Ejemplo de política de sesión

Utilice el siguiente ejemplo para crear una política de sesión StorageGRID .

Ejemplo: Configurar una política de sesión que permita la recuperación de objetos

En este ejemplo, al principal de la sesión solo se le permite recuperar objetos del bucket1. Todas las demás acciones se deniegan implícitamente, excepto las acciones específicas de StorageGRID, como el uso de "s3:PutOverwriteObject" permiso. La política de sesión se puede proporcionar como un archivo JSON al llamar a la API AssumeRole.

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

Ejemplo de políticas de bloque

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

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

- "Administrador de inquilinos".
- CLI de AWS con este comando (consulte "[Operaciones en bloques](#)"):

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

Ejemplo: Permitir que todos tengan acceso de solo lectura a un bloque

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

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

Ejemplo: Permitir que todos en una cuenta tengan acceso total y que todas las personas de otra cuenta tengan acceso de solo lectura a un bloque

En este ejemplo, todos los usuarios de una cuenta especificada tienen acceso completo a un depósito, mientras que todos los usuarios de otra cuenta especificada solo pueden listar el depósito y realizar operaciones GetObject en objetos del depósito empezando por el `shared/` prefijo de clave de objeto.



En StorageGRID, los objetos creados por una cuenta que no es propietaria (incluidas las cuentas anónimas) son propiedad de la cuenta de propietario del bloque. La política de bloque se aplica a estos objetos.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3>ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}

```

Ejemplo: Permitir que todo el mundo tenga acceso de solo lectura a un bloque y acceso completo por un grupo especificado

En este ejemplo, todos, incluidos los anónimos, pueden enumerar el depósito y realizar operaciones GetObject en todos los objetos del depósito, mientras que solo los usuarios que pertenecen al grupo Marketing en la cuenta especificada tienen acceso completo.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3>ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Ejemplo: Permitir que todo el mundo tenga acceso de lectura y escritura a un bloque si un cliente se encuentra en el rango de IP

En este ejemplo, todos, incluido el anónimo, pueden enumerar el bloque y realizar cualquier operación Object en todos los objetos del bloque, siempre que las solicitudes provengan de un intervalo IP especificado (54.240.143.0 a 54.240.143.255, excepto 54.240.143.188). Se denegarán todas las demás operaciones y se denegarán todas las solicitudes que estén fuera del rango de IP.

```
{  
  "Statement": [  
    {  
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": [ "s3:*Object", "s3>ListBucket" ],  
      "Resource":  
        ["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"],  
      "Condition": {  
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},  
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}  
      }  
    }  
  ]  
}
```

Ejemplo: Permitir el acceso completo a un bloque exclusivamente por un usuario federado especificado

En este ejemplo, al usuario federado Alex se le permite el acceso completo al examplebucket bucket y sus objetos. A todos los demás usuarios, incluido "root", se les deniega explícitamente todas las operaciones. Tenga en cuenta, sin embargo, que "root" nunca se le deniegan los permisos para poner/obtener/DeleteBucketPolicy.

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

Ejemplo: Permiso PutOverwriteObject

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

```

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

```

Ejemplo de políticas de grupo

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

Las directivas de grupo especifican los permisos de acceso para el grupo al que está asociada la directiva. No hay Principal ningún elemento en la política porque está implícito. Las políticas de grupo se configuran con el administrador de inquilinos o la API.

Ejemplo: Establecer la directiva de grupo mediante el Administrador de inquilinos

Al agregar o editar un grupo en el Gestor de inquilinos, puede seleccionar una política de grupo para determinar qué permisos de acceso S3 tendrán los miembros de este grupo. Consulte ["Cree grupos para un inquilino de S3"](#).

- **Sin acceso S3:** Opción predeterminada. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que el acceso se conceda con una política de bloque. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3.
- **Acceso de sólo lectura:** Los usuarios de este grupo tienen acceso de sólo lectura a los recursos S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de sólo lectura aparece en el cuadro de texto. No puede editar esta cadena.
- **Acceso completo:** Los usuarios de este grupo tienen acceso completo a los recursos S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena.
- **Ransomware Mitigation:** Esta política de muestra se aplica a todos los cubos para este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden suprimir de forma permanente objetos de los bloques que tienen activado el control de versiones de objetos.

Los usuarios del gestor de inquilinos que tengan el permiso Gestionar todos los bloques pueden sustituir esta política de grupo. Limite el permiso Gestionar todos los buckets a usuarios de confianza y use la autenticación multifactor (MFA) cuando esté disponible.

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

Ejemplo: Permite el acceso total de grupos a todos los bloques

En este ejemplo, a todos los miembros del grupo se les permite el acceso completo a todos los segmentos que pertenecen a la cuenta de inquilino, a menos que la política de bloque lo deniegue explícitamente.

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

Ejemplo: Permitir el acceso de solo lectura de grupo a todos los bloques

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

```
{  
  "Statement": [  
    {  
      "Sid": "AllowGroupReadOnlyAccess",  
      "Effect": "Allow",  
      "Action": [  
        "s3>ListAllMyBuckets",  
        "s3>ListBucket",  
        "s3>ListBucketVersions",  
        "s3GetObject",  
        "s3GetObjectTagging",  
        "s3GetObjectVersion",  
        "s3GetObjectVersionTagging"  
      ],  
      "Resource": "arn:aws:s3:::*"  
    }  
  ]  
}
```

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

En este ejemplo, sólo se permite a los miembros del grupo que enumeren y tengan acceso a su carpeta específica (prefijo de clave) en el bloque especificado. Tenga en cuenta que los permisos de acceso de otras políticas de grupo y la directiva de bloque deben tenerse en cuenta al determinar la privacidad de estas carpetas.

```

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

```

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

Los servicios de StorageGRID generan los mensajes de auditoría y se almacenan en archivos de registro de texto. Es posible revisar los mensajes de auditoría específicos de S3 en el registro de auditoría para obtener detalles sobre las operaciones de bloques y objetos.

Se realizó un seguimiento de las operaciones de bloque en los registros de auditoría

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- Etiquetado de GetBucketTagging
- Segmento de cabeza
- ListObjects
- ListObjectVersions
- CUMPLIR con la normativa de los bloques

- PutBucketTagging
- PutBucketVersioning

Se realizó un seguimiento de las operaciones de objetos en los registros de auditoría

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- Objeto principal
- Objeto de puta
- RestoreObject
- Seleccionar objeto
- UploadPart (cuando una regla de ILM utiliza una ingestión equilibrada o estricta)
- UploadPartCopy (cuando una regla de ILM utiliza una ingestión equilibrada o estricta)

Información relacionada

- "[Acceda al archivo de registro de auditoría](#)"
- "[El cliente escribe mensajes de auditoría](#)"
- "[El cliente lee los mensajes de auditoría](#)"

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.