Compatibilidad con la API REST de Amazon S3

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Compatibilidad con la API REST de Amazon S3

Detalles de implementación de la API REST de S3

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

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

Manejo de fechas

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

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

Encabezados de solicitud comunes

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

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

Encabezados de respuesta comunes

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

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

Autenticar solicitudes

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

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

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

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

Utilice el encabezado de autorización HTTP

El HTTP `Authorization` El encabezado lo utilizan todas las operaciones de API de S3, excepto las solicitudes anónimas cuando lo permite la política del bucket. El `Authorization` El encabezado contiene toda la información de firma necesaria para autenticar una solicitud.

Utilizar parámetros de consulta

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

Operaciones en el servicio

El sistema StorageGRID admite las siguientes operaciones en el servicio.

Operación	Implementación
Lista de cubos (anteriormente llamado Servicio GET)	Implementado con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.
Uso de almacenamiento GET	El StorageGRID"Uso de almacenamiento GET" La solicitud le indica la cantidad total de almacenamiento en uso por una cuenta y para cada depósito asociado con la cuenta. Esta es una operación en el servicio con una ruta de / y un parámetro de consulta personalizado(`?x-ntap-sg-usage`) agregado.

Operación	Implementación
OPCIONES /	Las aplicaciones cliente pueden emitir `OPTIONS /` solicitudes al puerto S3 en un nodo de almacenamiento, sin proporcionar credenciales de autenticación S3, para determinar si el nodo de almacenamiento está disponible. Puede utilizar esta solicitud para realizar monitoreo o para permitir que los balanceadores de carga externos identifiquen cuando un nodo de almacenamiento está inactivo.

Operaciones en buckets

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

Cada cuadrícula puede tener un máximo de 100.000 contenedores.

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

Las restricciones de nombre de depósito siguen las restricciones de la región estándar de AWS EE. UU., pero debe restringirlas aún más a las convenciones de nombres de DNS para admitir solicitudes de estilo alojado virtualmente S3.

Para obtener más información, consulte lo siguiente:

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

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

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

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

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

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

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

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

Operación	Implementación

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

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

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

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

Operaciones sobre objetos

Operaciones sobre objetos

Esta sección describe cómo el sistema StorageGRID implementa operaciones de API

REST S3 para objetos.

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

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

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

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

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

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

Utilice S3 Select

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

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

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

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

Cláusulas

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

Tipos de datos

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

Operadores

Operadores lógicos

- Y
- NO
- O

Operadores de comparación

- <
- >
- ⇐
- >=
- =
- =
- <>

- !=
- ENTRE
- EN

Operadores de coincidencia de patrones

- COMO
- _
- %

Operadores unitarios

- ES NULO
- NO ES NULO

Operadores matemáticos

- +
- -
- *
- /
- %

StorageGRID sigue la precedencia del operador Amazon S3 Select.

Funciones agregadas

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

Funciones condicionales

- CASO
- JUNTARSE
- NULLIF

Funciones de conversión

- CAST (para tipos de datos admitidos)

Funciones de fecha

- FECHA_AÑADIR
- FECHA_DIFF

- EXTRACTO
- A_CADENA
- HASTA_LA_MARCA_DE_TIEMPO
- UTCNOW

Funciones de cadena

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

Utilice cifrado del lado del servidor

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

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

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

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

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

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

Utilice SSE

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

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

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

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

Utilice SSE-C

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

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

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

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

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

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

- Debes utilizar https.

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

- La ETag en la respuesta no es el MD5 de los datos del objeto.
- Debe administrar la asignación de claves de cifrado a los objetos. StorageGRID no almacena claves de cifrado. Usted es responsable de rastrear la clave de cifrado que proporciona para cada objeto.

- Si su depósito tiene habilitada la gestión de versiones, cada versión del objeto debe tener su propia clave de cifrado. Usted es responsable de realizar el seguimiento de la clave de cifrado utilizada para cada versión del objeto.
- Dado que administra las claves de cifrado en el lado del cliente, también debe administrar cualquier protección adicional, como la rotación de claves, en el lado del cliente.

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

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

Información relacionada

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

Copiar objeto

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

Resolver conflictos

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

Tamaño del objeto

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

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

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

Caracteres UTF-8 en metadatos de usuario

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

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

- Las solicitudes tienen éxito si los metadatos definidos por el usuario incluyen caracteres UTF-8 escapados.

- StorageGRID no devuelve el `x-amz-missing-meta` encabezado si el valor interpretado del nombre o valor de la clave incluye caracteres no imprimibles.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

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

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

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

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

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

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

- `x-amz-server-side-encryption-customer-algorithm`

  VerEncabezados de solicitud para el cifrado del lado del servidor

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

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

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

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

Opciones de clase de almacenamiento

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

Uso de x-amz-copy-source en CopyObject

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

Si el origen y el destino coinciden, y el `x-amz-metadata-directive` El encabezado se especifica como

`REPLACE` , los metadatos del objeto se actualizan con los valores de metadatos proporcionados en la solicitud. En este caso, StorageGRID no vuelve a ingerir el objeto. Esto tiene dos consecuencias importantes:

- No se puede utilizar CopyObject para cifrar un objeto existente en un lugar, ni para cambiar el cifrado de un objeto existente en un lugar. Si usted suministra el `x-amz-server-side-encryption` encabezado o el `x-amz-server-side-encryption-customer-algorithm` encabezado, StorageGRID rechaza la solicitud y devuelve `XNotImplemented` .
- No se utiliza la opción de Comportamiento de ingestión especificada en la regla ILM correspondiente. Cualquier cambio en la ubicación de objetos que se active mediante la actualización se realiza cuando ILM se vuelve a evaluar mediante procesos de fondo normales de ILM.

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

Encabezados de solicitud para el cifrado del lado del servidor

Si usted"utilizar cifrado del lado del servidor" Los encabezados de solicitud que proporcione dependerán de si el objeto de origen está cifrado y de si planea cifrar el objeto de destino.

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

  > Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de los objetos, revise las consideraciones para"utilizando cifrado del lado del servidor" .
- Si desea cifrar el objeto de destino (la copia) con una clave única administrada por StorageGRID (SSE), incluya este encabezado en la solicitud CopyObject:
  - `x-amz-server-side-encryption`

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

Control de versiones

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

Obtener objeto

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

GetObject y objetos multipart

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

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

Caracteres UTF-8 en metadatos de usuario

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

Encabezado de solicitud compatible

Se admite el siguiente encabezado de solicitud:

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

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

Encabezado de solicitud no compatible

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

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

Control de versiones

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

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

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

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

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

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

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

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

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

Estado del objeto	Comportamiento de GetObject
Objeto completamente restaurado al grupo de almacenamiento en la nube	`200 OK` Se recupera una copia del objeto.

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

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

En estos casos:

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

GetObject y replicación entre cuadrículas

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

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

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

Objeto principal

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

Objetos HeadObject y multipart

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

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

Caracteres UTF-8 en metadatos de usuario

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

Encabezado de solicitud compatible

Se admite el siguiente encabezado de solicitud:

- `x-amz-checksum-mode`

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

Encabezado de solicitud no compatible

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

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

Control de versiones

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

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

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

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

> ⚠ Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de los objetos, revise las consideraciones en"Utilice cifrado del lado del servidor" .

Respuestas de HeadObject para objetos de Cloud Storage Pool

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

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

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

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

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

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

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

Estado del objeto	Respuesta a HeadObject

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

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

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

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

Replicación de HeadObject y entre cuadrículas

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

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

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

PonerObjeto

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

Resolver conflictos

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

Tamaño del objeto

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

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

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

Tamaño de los metadatos del usuario

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

Caracteres UTF-8 en metadatos de usuario

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

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

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

Límites de etiquetas de objetos

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

Propiedad de los objetos

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

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

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

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

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

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

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

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

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

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

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

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

    Si se realiza una solicitud sin estos encabezados, se utilizan las configuraciones de retención predeterminadas del depósito para calcular el modo de versión del objeto y la fecha de retención. Ver "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" .
- Encabezados de solicitud SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    VerEncabezados de solicitud para el cifrado del lado del servidor

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

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

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

Opciones de clase de almacenamiento

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

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

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

- `STANDARD`(Por defecto)

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

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

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

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

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

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

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

Encabezados de solicitud para el cifrado del lado del servidor

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

- **SSE**: utilice el siguiente encabezado si desea cifrar el objeto con una clave única administrada por

StorageGRID.

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

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

- **SSE-C**: utilice estos tres encabezados si desea cifrar el objeto con una clave única que usted proporcione y administre.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256` .
  - `x-amz-server-side-encryption-customer-key`:Especifique su clave de cifrado para el nuevo objeto.
  - `x-amz-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.

> Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de los objetos, revise las consideraciones para"utilizando cifrado del lado del servidor" .

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

Control de versiones

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

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

Cálculos de firma para el encabezado de autorización

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

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

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

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

Información relacionada

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

Restaurar objeto

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

Tipo de solicitud admitido

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

Control de versiones

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

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

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

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

Estado del objeto	Comportamiento de RestoreObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, o el objeto no está en un grupo de almacenamiento en la nube	`403 Forbidden` , `InvalidObjectState`
Objeto en el grupo de almacenamiento en la nube pero que aún no ha pasado a un estado no recuperable	`200 OK`No se realizan cambios **Nota**: Antes de que un objeto pase a un estado no recuperable, no se puede cambiar su `expiry-date` .

Estado del objeto	Comportamiento de RestoreObject
Objeto en transición a un estado no recuperable	`202 Accepted`Restaura una copia recuperable del objeto en el grupo de almacenamiento en la nube durante la cantidad de días especificada en el cuerpo de la solicitud. Al final de este período, el objeto vuelve a un estado no recuperable. Opcionalmente, utilice el `Tier` Elemento de solicitud para determinar cuánto tiempo tardará en finalizar el trabajo de restauración(`Expedited` , `Standard` , o `Bulk`). Si no lo especifica `Tier` , el `Standard` Se utiliza el nivel. **Importante**: Si un objeto se ha transferido a S3 Glacier Deep Archive o el grupo de almacenamiento en la nube usa almacenamiento de blobs de Azure, no podrá restaurarlo mediante el `Expedited` nivel. Se devuelve el siguiente error `403 Forbidden` , `InvalidTier` : `Retrieval option is not supported by this storage class` .
Objeto en proceso de restauración desde un estado no recuperable	`409 Conflict` , `RestoreAlreadyInProgress`
Objeto completamente restaurado al grupo de almacenamiento en la nube	`200 OK` **Nota:** Si un objeto se ha restaurado a un estado recuperable, puede cambiar su `expiry-date` volviendo a emitir la solicitud RestoreObject con un nuevo valor para `Days` . La fecha de restauración se actualiza en relación con el momento de la solicitud.

Seleccionar contenido del objeto

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

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

Antes de empezar

- La cuenta de inquilino tiene el permiso S3 Select.
- Tienes `s3:GetObject` Permiso para el objeto que desea consultar.
- El objeto que desea consultar debe estar en uno de los siguientes formatos:
  - **CSV**. Se puede utilizar tal cual o comprimido en archivos GZIP o BZIP2.
  - **Parquet**. Requisitos adicionales para los objetos Parquet:
    - S3 Select solo admite la compresión en columnas mediante GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos Parquet.
    - S3 Select no admite la salida Parquet. Debe especificar el formato de salida como CSV o JSON.
    - El tamaño máximo del grupo de filas sin comprimir es 512 MB.

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

Ejemplo de sintaxis de solicitud CSV

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

Ejemplo de sintaxis de solicitud de Parquet

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

Ejemplo de consulta SQL

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

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

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

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

Ejemplo de uso de AWS-CLI (CSV)

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

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

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

Ejemplo de uso de AWS-CLI (Parquet)

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

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

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

Operaciones para cargas multiparte

Operaciones para cargas multiparte

Esta sección describe cómo StorageGRID admite operaciones para cargas multiparte.

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

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

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

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

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

Carga completa de varias partes

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

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

Resolver conflictos

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

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

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

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

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

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

Control de versiones

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

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

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

> Cuando el control de versiones está habilitado para un bucket, completar una carga multiparte siempre crea una nueva versión, incluso si hay cargas multiparte simultáneas completadas en la misma clave de objeto. Cuando el control de versiones no está habilitado para un bucket, es posible iniciar una carga multiparte y luego iniciar y completar primero otra carga multiparte en la misma clave de objeto. En los depósitos sin versiones, la carga multiparte que se completa en último lugar tiene prioridad.

Error de replicación, notificación o notificación de metadatos

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

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

Consulte "Solucionar problemas de servicios de la plataforma" .

Crear carga de varias partes

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

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

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

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

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

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

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

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

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

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

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

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

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

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

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

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

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

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

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

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

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

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

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

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

    Encabezados de solicitud para el cifrado del lado del servidor

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

Encabezados de solicitud para el cifrado del lado del servidor

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

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

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

> Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de los objetos, revise las consideraciones para"utilizando cifrado del lado del servidor" .

Encabezados de solicitud no admitidos

El siguiente encabezado de solicitud no es compatible:

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

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

Control de versiones

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

Lista de cargas de varias partes

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

Se admiten los siguientes parámetros de solicitud:

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

Control de versiones

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

Subir parte

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

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

Encabezados de solicitud para el cifrado del lado del servidor

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

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

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

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

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

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

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

Control de versiones

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

Subir copia parcial

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

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

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

Se admiten los siguientes encabezados de solicitud:

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

Encabezados de solicitud para el cifrado del lado del servidor

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

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

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

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

> ⚠ Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de los objetos, revise las consideraciones en"Utilice cifrado del lado del servidor" .

Control de versiones

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

Respuestas de error

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

Códigos de error de la API de S3 compatibles

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

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

Códigos de error personalizados de StorageGRID

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

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