



Operaciones y limitaciones compatibles con la API REST de S3

StorageGRID

NetApp
April 10, 2024

This PDF was generated from <https://docs.netapp.com/es-es/storagegrid-116/s3/authenticating-requests.html> on April 10, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Operaciones y limitaciones compatibles con la API REST de S3 1
 - Gestión de fechas 1
 - Encabezados de solicitud comunes 1
 - Encabezados de respuesta comunes 1
 - Autenticar solicitudes 2
 - Operaciones en el servicio 2
 - Operaciones en bloques 3
 - Operaciones en objetos 19
 - Operaciones para cargas de varias partes 47
 - Respuestas de error 55

Operaciones y limitaciones compatibles con la API REST de S3

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

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

Gestión de fechas

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

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

Encabezados de solicitud comunes

El sistema StorageGRID admite encabezados de solicitud comunes definidos por la ["Documentación de Amazon Web Services \(AWS\): Referencia de API de Amazon simple Storage Service"](#), con una excepción.

Solicite el encabezado	Implementación
Autorización	Compatibilidad completa con la firma AWS Versión 2 Compatibilidad con la versión 4 de la firma de AWS, con las siguientes excepciones: <ul style="list-style-type: none">El valor SHA256 no se calcula para el cuerpo de la solicitud. El valor enviado por el usuario se acepta sin validación, como si fuera el valor <code>UNSIGNED-PAYLOAD</code> se había proporcionado para el <code>x-amz-content-sha256</code> encabezado.
x-amz-token de seguridad	No implementada. Retornos <code>XNotImplemented</code> .

Encabezados de respuesta comunes

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

Encabezado de respuesta	Implementación
x-amz-id-2	No se utiliza

Autenticar solicitudes

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

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

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

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

Utilice el encabezado autorización HTTP

`HTTP Authorization` Todas las operaciones de la API de S3 utilizan el encabezado excepto las solicitudes anónimas, donde lo permite la directiva de bloques. La `Authorization` encabezado contiene toda la información de firma necesaria para autenticar una solicitud.

Utilice los parámetros de consulta

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

Operaciones en el servicio

El sistema StorageGRID admite las siguientes operaciones en el servicio.

Funcionamiento	Implementación
OBTENER servicio	Se implementa con todo el comportamiento de la API DE REST de Amazon S3.
Obtenga el uso del almacenamiento	La solicitud GET Storage Usage le indica la cantidad total de almacenamiento que está usando una cuenta y por cada bloque asociado con la cuenta. Se trata de una operación en el servicio con una ruta de / y un parámetro de consulta personalizado (<code>?x-ntap-sg-usage</code>) agregado.

Funcionamiento	Implementación
OPCIONES /	Las aplicaciones cliente pueden emitir OPTIONS / Se solicita al puerto S3 en un nodo de almacenamiento, sin proporcionar credenciales de autenticación S3, para determinar si el nodo de almacenamiento está disponible. Puede usar esta solicitud para supervisar o para permitir que los equilibradores de carga externos identifiquen cuando un nodo de almacenamiento esté inactivo.

Información relacionada

[OBTENGA la solicitud de uso del almacenamiento](#)

Operaciones en bloques

El sistema StorageGRID admite un máximo de 1,000 bloques para cada cuenta de inquilino de S3.

Las restricciones de nombres de bloque siguen las restricciones de región del estándar estadounidense de AWS, pero debe restringirlas a convenciones de nomenclatura de DNS para admitir solicitudes de estilo hospedado virtual de S3.

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

[Configure los nombres de dominio de extremo API de S3](#)

Las operaciones GET Bucket (List Objects) Y GET Bucket admiten los controles de coherencia de StorageGRID.

Puede comprobar si las actualizaciones a la hora del último acceso están habilitadas o deshabilitadas para grupos individuales.

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

Funcionamiento	Implementación
ELIMINAR bloque	Se implementa con todo el comportamiento de la API DE REST de Amazon S3.
ELIMINAR los cors de cucharón	Esta operación elimina la configuración de CORS para el cucharón.
DELETE Bucket Encryption	Esta operación elimina el cifrado predeterminado del bloque. Los objetos cifrados existentes permanecen cifrados, pero los nuevos objetos agregados al bloque no están cifrados.
ELIMINAR ciclo de vida de bloque	Esta operación elimina la configuración del ciclo de vida del bloque.

Funcionamiento	Implementación
ELIMINE la política de bloques	Esta operación elimina la política asociada al bloque.
DELETE Bucket replicación	Esta operación elimina la configuración de replicación conectada al bloque.
DELETE Bucket tagging	Esta operación utiliza <code>tagging</code> subrecurso para quitar todas las etiquetas de un bloque.
GET Bucket (List Objects), versión 1 y versión 2	<p>Esta operación devuelve algunos o todos (hasta 1,000) de los objetos de un bloque. La clase de almacenamiento para los objetos puede tener cualquiera de dos valores, incluso si el objeto se ingirió con la <code>REDUCED_REDUNDANCY</code> opción de clase de almacenamiento:</p> <ul style="list-style-type: none"> • <code>STANDARD</code>, Que indica que el objeto se almacena en una agrupación de almacenamiento que consta de nodos de almacenamiento. • <code>GLACIER</code>, Que indica que el objeto se ha movido al bloque externo especificado por el grupo de almacenamiento en la nube. <p>Si el bloque contiene un gran número de claves eliminadas que tienen el mismo prefijo, la respuesta podría incluir algunas <code>CommonPrefixes</code> que no contienen claves.</p>
GET Bucket acl	Esta operación devuelve una respuesta positiva y el ID, <code>DisplayName</code> y permiso del propietario del bloque, lo que indica que el propietario tiene acceso completo al bloque.
OBTENGA los cors del cucharón	Esta operación devuelve el <code>cors</code> configuración del bloque.
OBTENGA el cifrado de bloque	Esta operación devuelve la configuración de cifrado determinada del bloque.
OBTENGA el ciclo de vida de la cuchara	Esta operación devuelve la configuración del ciclo de vida del bloque.
OBTENER ubicación de bloque	Esta operación devuelve la región que se estableció mediante el <code>LocationConstraint</code> Elemento de la solicitud PUT Bucket. Si la región del cucharón es <code>us-east-1</code> , se devuelve una cadena vacía para la región.
OBTENGA la notificación DE BUCKET	Esta operación devuelve la configuración de notificación asociada al bloque.
OBTENGA las versiones DE objeto Bucket	Con el acceso DE LECTURA en un bloque, esta operación con el <code>versions</code> subrecurso enumera los metadatos de todas las versiones de objetos del bloque.

Funcionamiento	Implementación
OBTENGA la política de bloques	Esta operación devuelve la política asociada al bloque.
OBTENGA la replicación de Bucket	Esta operación devuelve la configuración de replicación asociada al bloque.
GET Bucket tagging	Esta operación utiliza <code>tagging</code> subrecurso para devolver todas las etiquetas de un bloque.
OBTENGA el control de versiones de Bucket	<p>Esta implementación usa la <code>versioning</code> subrecurso para devolver el estado de control de versiones de un bloque.</p> <ul style="list-style-type: none"> • <i>Blank</i>: Nunca se ha activado el control de versiones (el cucharón es <code>"unversioned"</code>) • Activado: El control de versiones está activado • Suspendido: El control de versiones se ha habilitado anteriormente y se ha suspendido
OBTENER configuración de bloqueo de objeto	<p>Esta operación devuelve el modo de retención predeterminado de bloque y el período de retención predeterminado, si está configurado.</p> <p>Consulte OBTENER configuración de bloqueo de objeto para obtener información detallada.</p>
Cubo DE CABEZA	<p>Esta operación determina si existe un bloque y tiene permiso para acceder a él.</p> <p>Esta operación devuelve:</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: El UUID del bloque en formato UUID. • <code>x-ntap-sg-trace-id</code>: El ID de traza único de la solicitud asociada.

Funcionamiento	Implementación
COLOQUE el cucharón	<p>Esta operación crea un nuevo bloque. Al crear la cuchara, se convierte en el propietario de la cuchara.</p> <ul style="list-style-type: none"> • Los nombres de los bloques deben cumplir con las siguientes reglas: <ul style="list-style-type: none"> ◦ Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino). ◦ Debe ser compatible con DNS. ◦ Debe incluir al menos 3 y no más de 63 caracteres. ◦ Puede ser una serie de una o más etiquetas, con etiquetas adyacentes separadas por un punto. Cada etiqueta debe comenzar y terminar con una letra minúscula o un número y solo puede utilizar letras minúsculas, números y guiones. ◦ No debe ser una dirección IP con formato de texto. ◦ No debe utilizar periodos en solicitudes de estilo alojadas virtuales. Los periodos provocarán problemas en la verificación del certificado comodín del servidor. • De forma predeterminada, los bloques se crean en la <code>us-east-1</code> región; sin embargo, puede utilizar la <code>LocationConstraint</code> elemento de solicitud en el cuerpo de solicitud para especificar una región diferente. Cuando utilice la <code>LocationConstraint</code> Elemento, debe especificar el nombre exacto de una región que se ha definido mediante el Administrador de grid o la API de gestión de grid. Póngase en contacto con el administrador del sistema si no conoce el nombre de región que debe utilizar. <p>Nota: Se producirá un error si la solicitud PUT Bucket utiliza una región que no se ha definido en StorageGRID.</p> <ul style="list-style-type: none"> • Puede incluir el <code>x-amz-bucket-object-lock-enabled</code> Solicite el encabezado para crear un bucket con el bloqueo de objetos S3 habilitado. Consulte Utilice el bloqueo de objetos de S3. <p>Debe habilitar S3 Object Lock cuando crea el bloque. No se puede añadir o deshabilitar el bloqueo de objetos de S3 después de crear un bloque. S3 Object Lock requiere el control de versiones de bloques, que se habilita automáticamente al crear el bloque.</p>
COLOQUE los cors del cucharón	<p>Esta operación establece la configuración de CORS para un cucharón para que éste pueda atender solicitudes de origen cruzado. El uso compartido de recursos de origen cruzado (CORS) es un mecanismo de seguridad que permite a las aplicaciones web de cliente de un dominio acceder a los recursos de un dominio diferente. Por ejemplo, supongamos que se utiliza un bloque de S3 llamado <code>images</code> para almacenar gráficos. Mediante el ajuste de la configuración de CORS para <code>images</code> bloque, puede permitir que las imágenes de ese bloque se muestren en el sitio web <code>http://www.example.com</code>.</p>

Funcionamiento	Implementación
PUT Bucket Encryption	<p>Esta operación establece el estado de cifrado predeterminado de un bloque existente. Cuando se habilita el cifrado a nivel de bloque, se cifran todos los objetos nuevos que se añadan al bloque. StorageGRID admite el cifrado en el lado del servidor con claves gestionadas por StorageGRID. Al especificar la regla de configuración de cifrado del servidor, defina la <code>SSEAlgorithm</code> parámetro a. <code>AES256</code>, y no utilice <code>KMSMasterKeyID</code> parámetro.</p> <p>La configuración de cifrado predeterminada de bloque se omite si la solicitud de carga de objeto ya especifica cifrado (es decir, si la solicitud incluye la <code>x-amz-server-side-encryption-*</code> encabezado de solicitud).</p>
CICLO de vida DE la cuchara	<p>Esta operación crea una nueva configuración del ciclo de vida para el bloque o reemplaza una configuración de ciclo de vida existente. StorageGRID admite hasta 1,000 reglas de ciclo de vida en una configuración del ciclo de vida. Cada regla puede incluir los siguientes elementos XML:</p> <ul style="list-style-type: none"> • Caducidad (días, fecha) • <code>NoncurrentVersionExpiración</code> (<code>NoncurrentDays</code>) • Filtro (prefijo, etiqueta) • Estado • ID <p>StorageGRID no admite estas acciones:</p> <ul style="list-style-type: none"> • <code>AbortEncompleteMultipartUpload</code> • <code>ExpiredObjectDeleteMarker</code> • Transición <p>Para comprender cómo la acción de caducidad en el ciclo de vida de un bloque interactúa con las instrucciones de colocación de ILM, consulte "Cómo funciona ILM durante la vida de un objeto" en las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.</p> <p>Nota: La configuración del ciclo de vida de la cuchara se puede utilizar con cucharones que tengan habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida de la cuchara no es compatible con cucharones legados compatibles.</p>

Funcionamiento	Implementación
NOTIFICACIÓN DE PUT Bucket	<p>Esta operación configura notificaciones para el bloque mediante el XML de configuración de notificación incluido en el cuerpo de la solicitud. Debe tener en cuenta los siguientes detalles de implementación:</p> <ul style="list-style-type: none"> StorageGRID admite temas como destinos el Servicio de notificación simple (SNS). No se admiten extremos de simple Queue Service (SQS) o Amazon Lambda. El destino de las notificaciones debe especificarse como URN de un extremo de StorageGRID. Se pueden crear extremos con el administrador de inquilinos o la API de gestión de inquilinos. <p>El extremo debe existir para que la configuración de la notificación se realice correctamente. Si el extremo no existe, un <code>400 Bad Request</code> se devuelve un error con el código <code>InvalidArgument</code>.</p> <ul style="list-style-type: none"> No es posible configurar una notificación para los siguientes tipos de eventos. Estos tipos de evento no son compatibles. <ul style="list-style-type: none"> <code>s3:ReducedRedundancyLostObject</code> <code>s3:ObjectRestore:Completed</code> Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar excepto que no incluyen algunas claves y utilizan valores específicos para otros, como se muestra en el siguiente listado: <ul style="list-style-type: none"> EventSource <p><code>sgws:s3</code></p> * AwsRegion* <p>no incluido</p> x-amz-id-2 <p>no incluido</p> arn <p><code>urn:sgws:s3:::bucket_name</code></p>
POLÍTICA DE PUT Bucket	Esta operación establece la política asociada al bloque.

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

Funcionamiento	Implementación
PUT Bucket etiquetaje	<p>Esta operación utiliza <code>tagging</code> subrecurso para agregar o actualizar un conjunto de etiquetas para un bloque. Al añadir etiquetas de bloque, tenga en cuenta las siguientes limitaciones:</p> <ul style="list-style-type: none"> • Tanto StorageGRID como Amazon S3 admiten hasta 50 etiquetas por cada bloque. • Las etiquetas asociadas con un bloque deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode de longitud. • Los valores de etiqueta pueden tener una longitud máxima de 256 caracteres Unicode. • La clave y los valores distinguen entre mayúsculas y minúsculas.
PONER creación de versiones de bloques	<p>Esta implementación usa la <code>versioning</code> subrecurso para establecer el estado de control de versiones de un bloque existente. Puede establecer el estado de control de versiones con uno de los siguientes valores:</p> <ul style="list-style-type: none"> • Enabled: Activa el control de versiones de los objetos del bloque. Todos los objetos que se agregan al bloque reciben un ID de versión único. • Suspendido: Desactiva el control de versiones de los objetos del bloque. Todos los objetos agregados al bloque reciben el ID de versión <code>null</code>.
PONER configuración de bloqueo de objeto	<p>Esta operación configura o elimina el modo de retención predeterminado de bloque y el período de retención predeterminado.</p> <p>Si se modifica el período de retención predeterminado, la fecha de retención hasta la de las versiones de objeto existentes seguirá siendo la misma y no se volverá a calcular utilizando el nuevo período de retención predeterminado.</p> <p>Consulte PONER configuración de bloqueo de objeto para obtener información detallada.</p>

Información relacionada

[Controles de consistencia](#)

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

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

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

[Gestión de objetos con ILM](#)

[Usar cuenta de inquilino](#)

Cree una configuración del ciclo de vida de S3

Puede crear una configuración del ciclo de vida de S3 para controlar cuándo se eliminan

objetos específicos del sistema StorageGRID.

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

Qué es la configuración del ciclo de vida

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

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

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

Si aplica una configuración del ciclo de vida a un bloque, la configuración del ciclo de vida del bloque siempre anula la configuración de ILM de StorageGRID. StorageGRID utiliza la configuración de caducidad del bloque, no de ILM, para determinar si se deben eliminar o conservar objetos específicos.

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



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

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

- ELIMINAR ciclo de vida de bloque
- OBTENGA el ciclo de vida de la cuchara
- CICLO de vida DE la cuchara

Cree la configuración del ciclo de vida

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

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



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

3. La regla 3 sólo se aplica a los objetos que coinciden con el prefijo `category3/`. La `Expiration` parámetro especifica que cualquier versión no actual de objetos coincidentes caducará 50 días después de que se conviertan en no actualizados.

```

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

```

Aplicar la configuración del ciclo de vida al bloque

Después de crear el archivo de configuración del ciclo de vida, se aplica a un bloque emitiendo una solicitud PUT Bucket Lifecycle.

Esta solicitud aplica la configuración del ciclo de vida del archivo de ejemplo a los objetos de un bloque denominado `testbucket`.

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

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

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

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

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

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



Dado que el ciclo de vida de los bloques anula la gestión del ciclo de vida de `expiry-date` se muestra la fecha real en la que se eliminará el objeto. Para obtener más información, consulte [Cómo se determina la retención de objetos](#).

Por ejemplo, esta solicitud PUT Object fue emitida el 22 de junio de 2020 y coloca un objeto en el `testbucket` cucharón.

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

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


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

Por ejemplo, esta solicitud DE OBJETO HEAD se utilizó para obtener metadatos para el mismo objeto en el bloque testbucket.

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

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

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

Use la retención de bloque predeterminedada de Object Lock de S3

Si un bloque tiene habilitado el bloqueo de objetos S3, puede especificar un modo de retención predeterminedado y el período de retención predeterminedado que se aplicará a cada objeto que se agregue al bloque.

- El bloqueo de objetos de S3 se puede habilitar o deshabilitar para un bloque durante la creación de bloques.
- Si se habilita el bloqueo de objetos S3 para un bloque, puede configurar la retención predeterminedada para el bloque.
- La configuración de retención predeterminedada especifica:
 - Modo de retención predeterminedado: StorageGRID sólo admite el modo de "CUMPLIMIENTO".
 - Período de retención predeterminedado en días o años.

OBTENER configuración de bloqueo de objeto

La solicitud GET Object Lock Configuration (OBTENER configuración de bloqueo de objeto) permite determinar si el bloqueo de objeto está habilitado para un bloque y, si está habilitado, ver si hay un modo de

retención predeterminado y un período de retención configurado para el segmento.

Cuando se ingieren nuevas versiones de objetos en el bloque, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` no se ha especificado. El período de retención predeterminado se utiliza para calcular el valor de retener hasta la fecha if `x-amz-object-lock-retain-until-date` no se ha especificado.

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

Ejemplo de solicitud

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

Ejemplo de respuesta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB70XXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

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

PONER configuración de bloqueo de objeto

La solicitud DE CONFIGURACIÓN DE PUT Object Lock permite modificar el modo de retención predeterminado y el período de retención predeterminado para un bloque que tiene el bloqueo de objetos

activado. También es posible eliminar los ajustes de retención predeterminados previamente configurados.

Cuando se ingieren nuevas versiones de objetos en el bloque, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` no se ha especificado. El período de retención predeterminado se utiliza para calcular el valor de retener hasta la fecha if `x-amz-object-lock-retain-until-date` no se ha especificado.

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

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

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

Ejemplo de solicitud

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

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

Operaciones personalizadas en bloques

El sistema StorageGRID admite operaciones de bloques personalizadas que se añaden a la API DE REST de S3 y son específicas del sistema.

En la siguiente tabla, se enumeran las operaciones de bloque personalizadas que admite StorageGRID.

Funcionamiento	Descripción	Si quiere más información
OBTENGA coherencia de bloques	Devuelve el nivel de coherencia que se aplica a un bloque determinado.	OBTENGA la solicitud de consistencia de bloque
PONGA la consistencia del cucharón	Establece el nivel de consistencia aplicado a un bloque determinado.	PONER solicitud de consistencia de bloque
HORA de último acceso al bloque DE GET	Devuelve si las actualizaciones del último tiempo de acceso están habilitadas o deshabilitadas para un bloque en particular.	GET Bucket última solicitud de tiempo de acceso
PUT Bucket última hora de acceso	Permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para un bloque en particular.	PUT Bucket última solicitud de tiempo de acceso
DELETE bucket metadata notification Configuration	Elimina el XML de configuración de notificación de metadatos asociado a un bloque en particular.	DELETE bucket metadata notification Configuration
OBTENGA la configuración de notificación de metadatos del bloque de datos	Devuelve el XML de configuración de notificación de metadatos asociado a un bloque determinado.	OBTENGA la solicitud de configuración de notificación de metadatos del bloque
PUT bucket metadata notification Configuration	Configura el servicio de notificación de metadatos para un bloque.	PUT bucket metadata notification Configuration
COLOQUE el cucharón con la configuración de cumplimiento	Obsoleto y no compatible: Ya no puede crear nuevos bloques con el cumplimiento de normativas habilitado.	Obsoleto: COLOQUE el cucharón con la configuración de cumplimiento
Obtenga el cumplimiento de normativas de Bucket	Obsoleto pero compatible: Devuelve la configuración de cumplimiento vigente para un bloque compatible existente.	Obsoleto: GET Bucket Compliance Request
CUMPLIR con la normativa de los bloques	Obsoleto pero compatible: Permite modificar la configuración de cumplimiento de un bloque compatible heredado.	Obsoleto: PUT Bucket Compliance Request

Información relacionada

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

Operaciones en objetos

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

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

- StorageGRID [controles de consistencia](#) son compatibles con todas las operaciones de los objetos, con la excepción de lo siguiente:
 - OBTENER ACL de objeto
 - OPTIONS /
 - PONER objeto legal
 - PUT Object retention
 - SELECCIONE Contenido de objeto
- Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes S3 comienzan una operación.
- Todos los objetos de un bloque StorageGRID son propiedad del propietario del bloque, incluidos los objetos creados por un usuario anónimo o por otra cuenta.
- No se puede acceder a los objetos de datos procesados en el sistema StorageGRID a través de Swift a través de S3.

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

Funcionamiento	Implementación
ELIMINAR objeto	<p data-bbox="589 163 1481 226">Autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles.</p> <p data-bbox="589 268 1481 541">Al procesar una solicitud DE ELIMINACIÓN de objeto, StorageGRID intenta eliminar inmediatamente todas las copias del objeto de todas las ubicaciones almacenadas. Si se realiza correctamente, StorageGRID devuelve una respuesta al cliente inmediatamente. Si no se pueden eliminar todas las copias en un plazo de 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y luego indica que el cliente se ha realizado correctamente.</p> <p data-bbox="589 573 732 604">Versioning</p> <p data-bbox="589 636 1481 814">Para eliminar una versión específica, el solicitante debe ser el propietario del bloque y utilizar el <code>versionId</code> subrecurso. El uso de este subrecurso elimina permanentemente la versión. Si la <code>versionId</code> corresponde a un marcador de borrado, el encabezado de respuesta <code>x-amz-delete-marker</code> se devuelve establecido en <code>true</code>.</p> <ul data-bbox="613 846 1481 1287" style="list-style-type: none"> • Si se elimina un objeto sin el <code>versionId</code> subrecurso en un bloque habilitado para la versión, da como resultado la generación de un marcador de borrado. La <code>versionId</code> para el marcador de borrado se devuelve mediante <code>x-amz-version-id</code> encabezado de respuesta, y el <code>x-amz-delete-marker</code> el encabezado de la respuesta se devuelve establecido en <code>true</code>. • Si se elimina un objeto sin el <code>versionId</code> subrecurso en un bloque suspendido de la versión, se produce la eliminación permanente de una versión "nula" ya existente o un marcador de borrado "nula" y la generación de un nuevo marcador de borrado "nulo". La <code>x-amz-delete-marker</code> el encabezado de la respuesta se devuelve establecido en <code>true</code>. <p data-bbox="589 1329 1481 1392">Nota: En algunos casos, pueden existir varios marcadores de borrado para un objeto.</p>
ELIMINAR varios objetos	<p data-bbox="589 1451 1481 1514">Autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles.</p> <p data-bbox="589 1556 1433 1587">Se pueden eliminar varios objetos en el mismo mensaje de solicitud.</p>

Funcionamiento	Implementación
ELIMINAR etiquetado de objetos	<p>Utiliza la <code>tagging</code> subrecurso para quitar todas las etiquetas de un objeto. Se implementa con todo el comportamiento de la API DE REST de Amazon S3.</p> <p>Versioning</p> <p>Si la <code>versionId</code> el parámetro de consulta no se especifica en la solicitud, la operación elimina todas las etiquetas de la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de borrado, se devuelve el estado "MetodNotAllowed" con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.</p>
OBTENER objeto	OBTENER objeto
OBTENER ACL de objeto	Si se proporcionan las credenciales de acceso necesarias para la cuenta, la operación devuelve una respuesta positiva y el ID, DisplayName y permiso del propietario del objeto, lo que indica que el propietario tiene acceso completo al objeto.
OBTENER retención legal de objetos	Utilice el bloqueo de objetos de S3
OBTENGA retención de objetos	Utilice el bloqueo de objetos de S3
GET Object tagging	<p>Utiliza la <code>tagging</code> subrecurso para devolver todas las etiquetas de un objeto. Se implementa con todo el comportamiento de la API DE REST de Amazon S3</p> <p>Versioning</p> <p>Si la <code>versionId</code> el parámetro de consulta no se especifica en la solicitud, la operación devuelve todas las etiquetas de la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de borrado, se devuelve el estado "MetodNotAllowed" con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.</p>
OBJETO HEAD	OBJETO HEAD
Restauración DE objetos posterior	Restauración DE objetos posterior
OBJETO PUT	OBJETO PUT
PONER objeto: Copiar	PONER objeto: Copiar
PONER objeto legal	Utilice el bloqueo de objetos de S3

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

Información relacionada

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

Utilice el bloqueo de objetos de S3

Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, puede crear bloques con la función S3 Object Lock habilitada y, a continuación, especificar los periodos de retención predeterminados para cada bloque o la configuración específica de retención hasta la fecha y la conservación legal para cada versión de objeto que añada a ese bloque.

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

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

Habilite S3 Object Lock para bloque

Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, también puede habilitar el bloqueo de objetos S3 al crear cada bloque. Es posible usar cualquiera de estos métodos:

- Cree el bloque con el Administrador de arrendatarios.

[Usar cuenta de inquilino](#)

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

[Operaciones en bloques](#)

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

Un bloque con S3 Object Lock habilitado puede contener una combinación de objetos con y sin la configuración de S3 Object Lock. StorageGRID admite periodos de retención predeterminados para los objetos en bloques de bloqueo de objetos de S3 y admite la operación DE bloque de configuración PUT Object Lock. La `s3:object-lock-remaining-retention-days` la clave de condición de política establece los periodos de retención mínimos y máximos permitidos para los objetos.

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

Para determinar si la opción S3 Object Lock está habilitada, use [OBTENER configuración de bloqueo de objeto](#) solicitud.

Crear objeto con la configuración de Object Lock de S3

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



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

- `x-amz-object-lock-mode`, Que debe ser DE CUMPLIMIENTO (distingue entre mayúsculas y minúsculas).



Si especifica `x-amz-object-lock-mode`, también debe especificar `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
 - El valor retener hasta la fecha debe tener el formato `2020-08-10T21:46:00Z`. Se permiten segundos fraccionarios, pero sólo se conservan 3 dígitos decimales (precisión de milisegundos). No se admiten otros formatos ISO 8601.
 - La fecha de retención debe ser futura.
- `x-amz-object-lock-legal-hold`

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

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

- La `Content-MD5` la cabecera de la solicitud es necesaria si la hay `x-amz-object-lock-*` El encabezado de la solicitud está presente en LA solicitud PUT Object. `Content-MD5` No es necesario PARA PONER objeto: Copiar o iniciar carga de varias partes.
- Si el bloque no tiene habilitado el bloqueo de objetos S3 y un `x-amz-object-lock-*` El encabezado de la solicitud está presente, se devuelve un error de solicitud incorrecta 400 (InvalidRequest).
- La solicitud PUT Object admite el uso de `x-amz-storage-class: REDUCED_REDUNDANCY` Para igualar el comportamiento de AWS. Sin embargo, cuando un objeto se procesa en un bucket con el bloqueo de objetos S3 habilitado, StorageGRID siempre ejecuta un procesamiento de compromiso doble.
- Una respuesta posterior A LA versión GET o HEAD Object incluirá los encabezados `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, y `x-amz-object-lock-legal-hold`, si está configurado y si el remitente de la solicitud tiene el correcto `s3:Get*` permisos.
- Una solicitud de ELIMINACIÓN de versión de objeto o ELIMINACIÓN de objetos no se realizará correctamente si se encuentra antes de la fecha de retención o si la retención legal está activada.

Actualice la configuración de bloqueo de objetos S3

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

- PUT Object legal-hold

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

- PUT Object retention
 - El valor del modo debe ser DE CUMPLIMIENTO (distingue entre mayúsculas y minúsculas).

- El valor retener hasta la fecha debe tener el formato 2020-08-10T21:46:00Z. Se permiten segundos fraccionarios, pero sólo se conservan 3 dígitos decimales (precisión de milisegundos). No se admiten otros formatos ISO 8601.
- Si una versión de objeto tiene una fecha de retención existente, sólo puede aumentarla. El nuevo valor debe ser el futuro.

Información relacionada

[Gestión de objetos con ILM](#)

[Usar cuenta de inquilino](#)

[OBJETO PUT](#)

[PONER objeto: Copiar](#)

[Inicie la carga de varias partes](#)

[Control de versiones de objetos](#)

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

Utilice S3 Select

StorageGRID admite las siguientes cláusulas, los tipos de datos y los operadores de AWS S3 Select [SelectObjectContent](#).



No se admiten los elementos que no aparezcan.

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

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

Cláusulas

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

Tipos de datos

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

Operadores

Operadores lógicos

- Y..
- NO
- O.

Operadores de comparación

- <
- >
- ≤
- ≥
- =
- =
- <>
- !=
- ENTRE
- PULG

Operadores de comparación de patrones

- COMO
- _
- %

Operadores unitarios

- ES NULL
- NO ES NULL

Operadores de matemáticas

- +
- -
- *
- /
- %

StorageGRID sigue la prioridad del operador de AWS S3 Select.

Funciones de agregados

- MEDIA()
- RECUENTO (*)

- MÁX.()
- MIN()
- SUMA()

Funciones condicionales

- CASO
- COALCE
- NULLIF

Funciones de conversión

- CAST (para tipo de datos compatible)

Funciones de fecha

- FECHA_AÑADIR
- DIF_FECHA
- EXTRAER
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

Funciones de cadena

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

Usar cifrado del servidor

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

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

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

coinciden, el objeto se descifra y se devuelven los datos del objeto.

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



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



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

Utilice SSE

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

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

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

- OBJETO PUT
- PONER objeto: Copiar
- Inicie la carga de varias partes

Utilice SSE-C

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

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

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

- OBTENER objeto
- OBJETO HEAD
- OBJETO PUT
- PONER objeto: Copiar

- Inicie la carga de varias partes
- Cargar artículo
- Cargar pieza: Copiar

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

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

- Debe usar https.



StorageGRID rechaza todas las solicitudes realizadas sobre http cuando se utilice SSE-C. Por cuestiones de seguridad, debe tener en cuenta cualquier clave que envíe accidentalmente mediante http para que se vea comprometida. Deseche la llave y gírela según corresponda.

- La ETag en la respuesta no es la MD5 de los datos del objeto.
- Debe gestionar la asignación de claves de cifrado a objetos. StorageGRID no almacena claves de cifrado. Usted es responsable del seguimiento de la clave de cifrado que usted proporciona para cada objeto.
- Si su bloque está habilitado para versionado, cada versión de objeto debe tener su propia clave de cifrado. Usted es responsable del seguimiento de la clave de cifrado utilizada para cada versión del objeto.
- Dado que gestiona las claves de cifrado en el cliente, también debe administrar cualquier protección adicional, como la rotación de claves, en el cliente.



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

- Si la replicación de CloudMirror está configurada para el bloque, no podrá procesar objetos SSE-C. La operación de ingesta fallará.

Información relacionada

[OBTENER objeto](#)

[OBJETO HEAD](#)

[OBJETO PUT](#)

[PONER objeto: Copiar](#)

[Inicie la carga de varias partes](#)

[Cargar artículo](#)

[Cargar pieza: Copiar](#)

["Guía para desarrolladores de Amazon S3: Protección de datos mediante cifrado en el lado del servidor con claves de cifrado proporcionadas por el cliente \(SSE-C\)"](#)

OBTENER objeto

Puede usar la solicitud GET Object de S3 para recuperar un objeto de un bloque de S3.

OBJETOS GET y objetos de varias partes

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

Puede ajustar `partNumber` a 1 para objetos segmentados/multipartes y no segmentados/no multipartes; sin embargo, la `x-amz-mp-parts-count` el elemento de respuesta sólo se devuelve para objetos segmentados o multipartes.

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

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

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



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones que se incluyen en el apartado «"usar cifrado en el servidor"».

Caracteres UTF-8 en los metadatos de usuario

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

Encabezado de solicitud no compatible

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

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

Creación de versiones

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

Comportamiento de OBTENER objeto para objetos de pool de almacenamiento en cloud

Si un objeto se ha almacenado en un Cloud Storage Pool (consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información), el comportamiento de una solicitud GET Object depende del estado del objeto. Consulte «'HEAD Object'» para obtener más información.



Si un objeto está almacenado en un Cloud Storage Pool y existen también una o varias copias del objeto en el grid, GET Object Requests intentará recuperar datos del grid, antes de recuperarlos del Cloud Storage Pool.

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

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

Si cargó un objeto con varias partes o StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el pool de almacenamiento en cloud al muestrear un subconjunto de las partes o segmentos del objeto. En algunos casos, es posible que UNA solicitud GET Object devuelva incorrectamente 200 OK cuando algunas partes del objeto ya se han trasladado a un estado no recuperable o cuando algunas partes del objeto aún no se han restaurado.

En estos casos:

- La solicitud GET Object puede devolver algunos datos pero detenerse a mitad de camino a través de la transferencia.
- Una petición GET Object posterior podría devolver 403 Forbidden.

Información relacionada

[Usar cifrado del servidor](#)

[Gestión de objetos con ILM](#)

[Restauración DE objetos posterior](#)

OBJETO HEAD

Puede usar la solicitud del ENCABEZADO Object de S3 para recuperar metadatos de un objeto sin devolver el objeto propiamente dicho. Si el objeto se almacena en un pool de almacenamiento en el cloud, puede usar HEAD Object para determinar el estado de transición del objeto.

OBJETO DE CABECERA y objetos de varias partes

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

Puede ajustar `partNumber` a 1 para objetos segmentados/multipartes y no segmentados/no multipartes; sin embargo, la `x-amz-mp-parts-count` el elemento de respuesta sólo se devuelve para objetos segmentados o multipartes.

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

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

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



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones que se incluyen en el apartado «"usar cifrado en el servidor"».

Caracteres UTF-8 en los metadatos de usuario

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

Encabezado de solicitud no compatible

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

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

Encabezados de respuesta para objetos de Cloud Storage Pool

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

respuesta:

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

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

Estado del objeto	Respuesta al OBJETO PRINCIPAL
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un pool de almacenamiento tradicional o utilizando código de borrado	200 OK (No se devuelve ningún encabezado de respuesta especial).
Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Hasta que el objeto se realice la transición a un estado no recuperable, el valor de <code>expiry-date</code> se configura a una hora distante en el futuro. El sistema StorageGRID no controla la hora exacta de la transición.
El objeto ha pasado a estar en estado no recuperable, pero también existe al menos una copia en la cuadrícula	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Valor para <code>expiry-date</code> se configura a una hora distante en el futuro. Nota: Si la copia de la cuadrícula no está disponible (por ejemplo, un nodo de almacenamiento está inactivo), debe emitir una solicitud DE restauración DE objetos POST para restaurar la copia desde el grupo de almacenamiento en la nube antes de poder recuperar el objeto correctamente.
El objeto ha pasado a un estado que no se puede recuperar y no existe ninguna copia en la cuadrícula	200 OK <code>x-amz-storage-class: GLACIER</code>

Estado del objeto	Respuesta al OBJETO PRINCIPAL
Objeto en proceso de restauración a partir de un estado no recuperable	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"
Objeto completamente restaurado en el pool de almacenamiento en cloud	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" La expiry-date Indica si el objeto del Cloud Storage Pool regresará a un estado no recuperable.

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

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

Creación de versiones

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

Información relacionada

[Usar cifrado del servidor](#)

[Gestión de objetos con ILM](#)

[Restauración DE objetos posterior](#)

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

Restauración DE objetos posterior

Puede usar la solicitud DE restauración DE objetos POST de S3 PARA restaurar un objeto almacenado en un pool de almacenamiento en cloud.

Tipo de solicitud admitido

StorageGRID solo admite solicitudes POSTERIORES a la restauración de objetos para restaurar un objeto. No admite la `SELECT` tipo de restauración. Seleccione solicitudes de devolución `XNotImplemented`.

Creación de versiones

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

Comportamiento de la restauración POSTERIOR de objetos en objetos de Pool de almacenamiento en cloud

Si un objeto se ha almacenado en un Cloud Storage Pool (consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información), una solicitud POSTERIOR de restauración de objetos tiene el siguiente comportamiento, en función del estado del objeto. Consulte «'HEAD Object'» para obtener más información.



Si un objeto se almacena en un Cloud Storage Pool y existen también una o varias copias del objeto en la cuadrícula, no es necesario restaurar el objeto mediante la emisión de una solicitud DE restauración DE objetos POSTERIOR. En su lugar, la copia local se puede recuperar directamente, utilizando UNA solicitud GET Object.

Estado del objeto	Comportamiento DE la restauración POSTERIOR de objetos
El objeto se ingiere en StorageGRID pero aún no se ha evaluado por ILM, o el objeto no está en un pool de almacenamiento cloud	403 Forbidden, InvalidObjectState
Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	200 OK No se han realizado cambios. Nota: Antes de que un objeto haya pasado a un estado no recuperable, no puede cambiar su <code>expiry-date</code> .
Objeto que ha pasado a un estado no recuperable	202 Accepted Restaura una copia recuperable del objeto en el Pool de almacenamiento en la nube durante la cantidad de días especificada en el cuerpo de la solicitud. Al final de este período, el objeto se devuelve a un estado no recuperable. Opcionalmente, utilice la <code>Tier</code> solicitar elemento para determinar cuánto tiempo tardará el trabajo de restauración en finalizar (<code>Expedited</code> , <code>Standard</code> , o. <code>Bulk</code>). Si no especifica <code>Tier</code> , la <code>Standard</code> se utiliza el nivel. Atención: Si se ha realizado la transición de un objeto a S3 Glacier Deep Archive o el Cloud Storage Pool utiliza Azure Blob Storage, no puede restaurarlo con el <code>Expedited</code> nivel. Se devuelve el siguiente error 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.

Estado del objeto	Comportamiento DE la restauración POSTERIOR de objetos
Objeto en proceso de restauración a partir de un estado no recuperable	409 Conflict, RestoreAlreadyInProgress
Objeto completamente restaurado en el pool de almacenamiento en cloud	200 OK Nota: Si un objeto ha sido restaurado a un estado recuperable, usted puede cambiar su <code>expiry-date</code> Volviendo a emitir la solicitud DE restauración DE objeto POSTERIOR con un nuevo valor para <code>Days</code> . La fecha de restauración se actualiza en relación con la hora de la solicitud.

Información relacionada

[Gestión de objetos con ILM](#)

OBJETO HEAD

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

OBJETO PUT

Puede usar la solicitud PUT Object de S3 para añadir un objeto a un bloque.

Resolver conflictos

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

Tamaño del objeto

El tamaño máximo *recomendado* para una única operación PUT Object es de 5 GiB (5,368,709,120 bytes). Si tiene objetos que sean mayores de 5 GiB, utilice la carga de varias partes en su lugar.



En StorageGRID 11.6, el tamaño máximo *admitido* para una única operación PUT Object es de 5 TiB (5,497,558,138,880 bytes). Sin embargo, la alerta * S3 PUT Object size demasiado grande* se activará si intenta cargar un objeto que supere los 5 GiB.

Tamaño de los metadatos del usuario

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

Caracteres UTF-8 en los metadatos de usuario

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

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

- LAS solicitudes PUT, PUT Object-Copy, GET y HEAD se realizan correctamente si los metadatos definidos por el usuario incluyen caracteres UTF-8 que se han escapado.
- StorageGRID no devuelve el `x-amz-missing-meta` encabezado si el valor interpretado del nombre o valor de clave incluye caracteres no imprimibles.

Límites de etiqueta de objeto

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

Propiedad del objeto

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

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

Al especificar `aws-chunked` para `Content-Encoding` StorageGRID no verifica los siguientes elementos:

- StorageGRID no verifica el `chunk-signature` contra los datos del fragmento.
- StorageGRID no verifica el valor indicado para `x-amz-decoded-content-length` contra el objeto.

- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

La codificación de transferencia con chunked es compatible si `aws-chunked` también se utiliza la firma de carga útil.

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

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

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

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

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

Valor para `creation-time` Se evalúa como segundos desde el 1 de enero de 1970.



Una regla de ILM no puede utilizar un **tiempo de creación definido por el usuario** para el tiempo de referencia y las opciones equilibradas o estrictas para el comportamiento de procesamiento. Se devuelve un error cuando se crea la regla de ILM.

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

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

Utilice el bloqueo de objetos de S3

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

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

Encabezados de solicitud no compatibles

No se admiten los siguientes encabezados de solicitud:

- La `x-amz-acl` no se admite el encabezado de la solicitud.
- La `x-amz-website-redirect-location` el encabezado de la solicitud no es compatible y devuelve `XNotImplemented`.

Opciones para clase de almacenamiento

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

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

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

- **STANDARD (Predeterminado)**
 - **Commit doble:** Si la regla ILM especifica la opción COMMIT doble para el comportamiento de procesamiento, tan pronto como un objeto se ingiere una segunda copia de ese objeto se crea y se distribuye a un nodo de almacenamiento diferente (COMMIT doble). Cuando se evalúa el ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de colocación en la regla. Si no lo hacen, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y que sea necesario eliminar las copias provisionales iniciales.
 - **Balanceado:** Si la regla ILM especifica la opción equilibrada y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en nodos de almacenamiento diferentes.

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

- **REDUCED_REDUNDANCY**
 - **Commit doble:** Si la regla ILM especifica la opción COMMIT doble para el comportamiento de la ingesta, StorageGRID crea una única copia provisional mientras se ingiere el objeto (COMMIT único).
 - **Balanceado:** Si la regla ILM especifica la opción equilibrada, StorageGRID realiza una única copia provisional sólo si el sistema no puede hacer inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación síncrona, este encabezado no tiene ningún efecto. La `REDUCED_REDUNDANCY` Se recomienda utilizar la opción cuando la regla de ILM que coincide con el objeto crea una única copia replicada. En este caso, utilizar `REDUCED_REDUNDANCY` elimina la creación y eliminación innecesarias de una copia de objetos adicional en cada operación de procesamiento.

Con el `REDUCED_REDUNDANCY` la opción no se recomienda en otras circunstancias.

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

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

Especificando `REDUCED_REDUNDANCY` sólo afecta al número de copias que se crean cuando un objeto se ingiere por primera vez. No afecta al número de copias del objeto que se realizan cuando el objeto se evalúa mediante la política de ILM activa y no provoca que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID.

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

REDUCED_REDUNDANCY opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el REDUCED_REDUNDANCY opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Solicitar encabezados para el cifrado del servidor

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

- **SSE:** Utilice el siguiente encabezado si desea cifrar el objeto con una clave única gestionada por StorageGRID.
 - `x-amz-server-side-encryption`
- **SSE-C:** Utilice los tres encabezados si desea cifrar el objeto con una clave única que proporciona y administra.
 - `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256.
 - `x-amz-server-side-encryption-customer-key`: Especifique la clave de cifrado para el nuevo objeto.
 - `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.

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

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

Creación de versiones

Si el control de versiones está habilitado para un bloque, un valor único `versionId` se genera automáticamente para la versión del objeto almacenado. Este `versionId` también se devuelve en la respuesta mediante el `x-amz-version-id` encabezado de respuesta.

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

Información relacionada

[Gestión de objetos con ILM](#)

[Operaciones en bloques](#)

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

[Usar cifrado del servidor](#)

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

PONER objeto: Copiar

Puede usar la solicitud PUT Object - Copy de S3 para crear una copia de un objeto que ya está almacenado en S3. UNA operación PONER objeto - copia es la misma que

realizar UNA GET y LUEGO UN PUT.

Resolver conflictos

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

Tamaño del objeto

El tamaño máximo *recomendado* para una única operación PUT Object es de 5 GIB (5,368,709,120 bytes). Si tiene objetos que sean mayores de 5 GIB, utilice la carga de varias partes en su lugar.



En StorageGRID 11.6, el tamaño máximo *admitido* para una única operación PUT Object es de 5 TIB (5,497,558,138,880 bytes). Sin embargo, la alerta * S3 PUT Object size demasiado grande* se activará si intenta cargar un objeto que supere los 5 GIB.

Caracteres UTF-8 en los metadatos de usuario

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

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

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

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

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

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

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

- Encabezados de solicitud de bloqueo de objetos S3:

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

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

[Utilice el bloqueo de objetos de S3](#)

- Encabezados de solicitud SSE:

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

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

Encabezados de solicitud no compatibles

No se admiten los siguientes encabezados de solicitud:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-website-redirect-location`

Opciones para clase de almacenamiento

La `x-amz-storage-class` Se admite el encabezado de la solicitud y afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente especifica un comportamiento de ingesta de `COMMIT` doble o de equilibrado.

- STANDARD

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

- REDUCED_REDUNDANCY

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



Si va a procesar un objeto en un bloque con el bloqueo de objetos S3 habilitado, el REDUCED_REDUNDANCY opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el REDUCED_REDUNDANCY opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Uso de x-amz-copy-source en PUT Object - Copy

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

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

- No se puede utilizar PONER objeto - Copiar para cifrar un objeto existente en su lugar ni para cambiar el cifrado de un objeto existente en su lugar. Si proporciona el `x-amz-server-side-encryption` cabecera o la `x-amz-server-side-encryption-customer-algorithm` Encabezamiento, StorageGRID rechaza la solicitud y devuelve XNotImplemented.
- No se utiliza la opción de comportamiento de procesamiento especificado en la regla de ILM que coincida. Cualquier cambio en la ubicación del objeto que se active por la actualización se realice cuando los procesos de ILM normales se reevalúan el ILM en segundo plano.

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

Solicitar encabezados para el cifrado del servidor

Si utiliza cifrado del servidor, los encabezados de solicitud que proporcione dependerán de si el objeto de origen está cifrado y de si planea cifrar el objeto de destino.

- Si el objeto de origen se cifra utilizando una clave proporcionada por el cliente (SSE-C), debe incluir los tres encabezados siguientes en LA solicitud PUT Object - Copy, para que el objeto se pueda descifrar y copiar a continuación:
 - `x-amz-copy-source-server-side-encryption-customer-algorithm` Especifique AES256.
 - `x-amz-copy-source-server-side-encryption-customer-key` Especifique la clave de cifrado que proporcionó cuando creó el objeto de origen.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique el resumen

MD5 que proporcionó cuando creó el objeto de origen.

- Si desea cifrar el objeto de destino (la copia) con una clave única que proporciona y administra, incluya los tres encabezados siguientes:
 - `x-amz-server-side-encryption-customer-algorithm`: Especifique AES256.
 - `x-amz-server-side-encryption-customer-key`: Especifique una nueva clave de cifrado para el objeto de destino.
 - `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la nueva clave de cifrado.

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

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

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

Creación de versiones

Si se crea una versión del contenedor de origen, puede utilizar `x-amz-copy-source` encabezado para copiar la versión más reciente de un objeto. Para copiar una versión específica de un objeto, debe especificar explícitamente la versión que desea copiar mediante `versionId` subrecurso. Si se crea una versión del bloque de destino, la versión generada se devuelve en el `x-amz-version-id` encabezado de respuesta. Si se suspende el control de versiones para el bloque de destino, entonces `x-amz-version-id` devuelve un valor «'null'».

Información relacionada

[Gestión de objetos con ILM](#)

[Usar cifrado del servidor](#)

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

OBJETO PUT

SelectObjectContent

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

Para obtener más información, consulte ["Documentación de AWS para SelectObjectContent"](#).

Lo que necesitará

- La cuenta de inquilino tiene el permiso de S3 Select.
- Ya tienes `s3:GetObject` permiso para el objeto al que desea consultar.
- El objeto que desea consultar tiene el formato CSV o es un archivo comprimido GZIP o BZIP2 que contiene un archivo con formato CSV.

- La expresión SQL tiene una longitud máxima de 256 KB.
- Cualquier registro de la entrada o de los resultados tiene una longitud máxima de 1 MIB.

Ejemplo de sintaxis de solicitud

```
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 consulta SQL

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

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

Las primeras líneas del archivo a consultar, SUB-EST2020_ALL.csv, mire como esto:

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

Ejemplo de uso de AWS-CLI


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

Las primeras líneas del archivo de salida, `changes.csv`, mire como esto:

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

Operaciones para cargas de varias partes

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

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

- No debe exceder 1,000 cargas simultáneas de varias partes en un solo bloque, ya que los resultados de List Multipart cargan consultas para ese bloque pueden devolver resultados incompletos.
- StorageGRID aplica los límites de tamaño de AWS para piezas multiparte. Los clientes de S3 deben seguir estas directrices:
 - Cada parte de una carga de varias partes debe estar entre 5 MIB (5,242,880 bytes) y 5 GIB (5,368,709,120 bytes).
 - La última parte puede ser más pequeña que 5 MIB (5,242,880 bytes).
 - En general, los tamaños de las piezas deben ser lo más grandes posible. Por ejemplo, utilice tamaños de parte de 5 GIB para un objeto de 100 GIB. Dado que cada parte se considera un objeto único, el uso de tamaños de pieza grandes reduce la sobrecarga de metadatos de StorageGRID.
 - En el caso de objetos de menor tamaño de 5 GIB, considere usar la carga sin varias partes.
- ILM se evalúa para cada parte de un objeto de varias partes tal como se procesa y para el objeto como un todo cuando se completa la carga de varias partes, si la regla de ILM utiliza el comportamiento estricto o equilibrado del procesamiento. Debe saber cómo afecta esto a la ubicación de objetos y piezas:
 - Si ILM cambia mientras se carga varias partes de S3, es posible que cuando la carga de varias partes completa algunas partes del objeto no cumplan los requisitos actuales de ILM. Cualquier pieza que no

se haya colocado correctamente se coloca en la cola de reevaluación de ILM y se mueve posteriormente a la ubicación correcta.

- Al evaluar ILM para una pieza, StorageGRID filtra el tamaño de la pieza, no el tamaño del objeto. Esto significa que las partes de un objeto se pueden almacenar en ubicaciones que no cumplen los requisitos de ILM para el objeto como un todo. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan en DC1 mientras que todos los objetos más pequeños se almacenan en DC2, al ingerir cada parte de 1 GB de una carga multiparte de 10 partes se almacena en DC2. Cuando se evalúa ILM para el objeto como un todo, todas las partes del objeto se mueven a DC1.
- Todas las operaciones de carga de varias partes admiten controles de coherencia de StorageGRID.
- Según sea necesario, puede utilizar el cifrado del servidor con cargas en varias partes. Para usar SSE (cifrado en el servidor con claves gestionadas por StorageGRID), incluye el `x-amz-server-side-encryption`. Solicite el encabezado sólo en la solicitud Iniciar carga de varias partes. Para utilizar SSE-C (cifrado del servidor con claves proporcionadas por el cliente), debe especificar los mismos tres encabezados de solicitud de clave de cifrado en la solicitud de carga de varias partes iniciada y en cada solicitud de artículo de carga posterior.

Funcionamiento	Implementación
Enumerar cargas de varias partes	Consulte Enumerar cargas de varias partes
Inicie la carga de varias partes	Consulte Inicie la carga de varias partes
Cargar artículo	Consulte Cargar artículo
Cargar pieza: Copiar	Consulte Cargar pieza: Copiar
Completar carga de varias partes	Consulte Completar carga de varias partes
Cancelar carga de varias partes	Se implementa con todo el comportamiento de la API DE REST de Amazon S3
Enumerar piezas	Se implementa con todo el comportamiento de la API DE REST de Amazon S3

Información relacionada

- [Controles de consistencia](#)
- [Usar cifrado del servidor](#)

Enumerar cargas de varias partes

La operación List Multipart carga enumera las cargas de varias partes en curso para un bloque.

Se admiten los siguientes parámetros de solicitud:

- `encoding-type`
- `max-uploads`

- `key-marker`
- `prefix`
- `upload-id-marker`

La `delimiter` el parámetro `request` no es compatible.

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Cuando se realiza la operación de carga de varias partes completa, ese es el punto en el que se crean objetos (y se crean versiones si procede).

Inicie la carga de varias partes

La operación Iniciar carga de varias partes inicia una carga de varias partes para un objeto y devuelve un ID de carga.

La `x-amz-storage-class` se admite el encabezado de la solicitud. El valor enviado para `x-amz-storage-class` Afecta la forma en que StorageGRID protege los datos de objetos durante el procesamiento y no cuántas copias persistentes del objeto se almacenan en el sistema StorageGRID (determinado por ILM).

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

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

- **STANDARD (Predeterminado)**
 - **Commit doble:** Si la regla ILM especifica la opción COMMIT doble para el comportamiento de procesamiento, tan pronto como un objeto se ingiere una segunda copia de ese objeto se crea y se distribuye a un nodo de almacenamiento diferente (COMMIT doble). Cuando se evalúa el ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de colocación en la regla. Si no lo hacen, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y que sea necesario eliminar las copias provisionales iniciales.
 - **Balanceado:** Si la regla ILM especifica la opción equilibrada y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en nodos de almacenamiento diferentes.

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

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

procesamiento.

Con el `REDUCED_REDUNDANCY` la opción no se recomienda en otras circunstancias.

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

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

Especificando `REDUCED_REDUNDANCY` sólo afecta al número de copias que se crean cuando un objeto se ingiere por primera vez. No afecta al número de copias del objeto que se realizan cuando el objeto se evalúa mediante la política de ILM activa y no provoca que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID.

Nota: Si está ingiriendo un objeto en un cubo con el bloqueo de objetos S3 activado, el `REDUCED_REDUNDANCY` opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Se admiten los siguientes encabezados de solicitud:

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

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

```
x-amz-meta-__name__: `value`
```

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

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

Valor para `creation-time` Se evalúa como segundos desde el 1 de enero de 1970.



Adición `creation-time` Como metadatos definidos por el usuario no se permite si va a agregar un objeto a un bloque que tiene la conformidad heredada habilitada. Se devolverá un error.

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

- `x-amz-object-lock-legal-hold`

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

Uso del bloqueo de objetos de S3

- Encabezados de solicitud SSE:

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

Solicitar encabezados para el cifrado del servidor



Para obtener información acerca de cómo StorageGRID maneja los caracteres UTF-8, consulte la documentación de PUT Object.

Solicitar encabezados para el cifrado del servidor

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

- **SSE:** Utilice el siguiente encabezado en la solicitud Iniciar carga de varias partes si desea cifrar el objeto con una clave única gestionada por StorageGRID. No especifique este encabezado en ninguna de las solicitudes de artículo de carga.
 - `x-amz-server-side-encryption`
- **SSE-C:** Utilice los tres encabezados de la solicitud de carga de varias partes iniciada (y en cada solicitud de artículo de carga posterior) si desea cifrar el objeto con una clave única que proporciona y gestiona.
 - `x-amz-server-side-encryption-customer-algorithm`: Especifique AES256.
 - `x-amz-server-side-encryption-customer-key`: Especifique la clave de cifrado para el nuevo objeto.
 - `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.

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

Encabezados de solicitud no compatibles

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

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

Creación de versiones

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

Información relacionada

[Gestión de objetos con ILM](#)

[Usar cifrado del servidor](#)

OBJETO PUT

Cargar artículo

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

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- Content-Length
- Content-MD5

Solicitar encabezados para el cifrado del servidor

Si ha especificado el cifrado SSE-C para la solicitud de carga de varias partes iniciada, también debe incluir los siguientes encabezados de solicitud en cada solicitud de artículo de carga:

- x-amz-server-side-encryption-customer-algorithm: Especificar AES256.
- x-amz-server-side-encryption-customer-key: Especifique la misma clave de cifrado que proporcionó en la solicitud Iniciar carga de varias partes.
- x-amz-server-side-encryption-customer-key-MD5: Especifique el mismo resumen MD5 que ha proporcionado en la solicitud Iniciar carga de varias partes.



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones que se incluyen en el apartado «"usar cifrado en el servidor"».

Creación de versiones

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

Información relacionada

[Usar cifrado del servidor](#)

Cargar pieza: Copiar

La operación cargar pieza - Copiar carga una parte de un objeto copiando datos de un objeto existente como origen de datos.

La operación cargar pieza - copia se implementa con todo el comportamiento de la API DE REST de Amazon S3.

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

Se admiten los siguientes encabezados de solicitud:

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

Solicitar encabezados para el cifrado del servidor

Si ha especificado el cifrado SSE-C para la solicitud de carga de varias partes iniciada, también debe incluir los siguientes encabezados de solicitud en cada parte de carga - solicitud de copia:

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

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

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



Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones que se incluyen en el apartado «"usar cifrado en el servidor"».

Creación de versiones

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

Completar carga de varias partes

La operación de carga de varias partes completa completa finaliza una carga de varias partes de un objeto mediante el montaje de las piezas previamente cargadas.

Resolver conflictos

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

Solicitar encabezados

La `x-amz-storage-class` Se admite el encabezado de la solicitud y afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente especifica un comportamiento de ingesta de COMMIT doble o de equilibrado.

- STANDARD

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

- REDUCED_REDUNDANCY

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



Si va a procesar un objeto en un bloque con el bloqueo de objetos S3 habilitado, el REDUCED_REDUNDANCY opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el REDUCED_REDUNDANCY opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.



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



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

Creación de versiones

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

Si el control de versiones está habilitado para un bloque, un valor único `versionId` se genera automáticamente para la versión del objeto almacenado. Este `versionId` también se devuelve en la respuesta mediante el `x-amz-version-id` encabezado de respuesta.

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



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

Error en la replicación, notificación o notificación de metadatos

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

Si esto ocurre, se genera una alarma en el administrador de grid en eventos totales (SMTT). El mensaje Last Event muestra "error al publicar notificaciones para la clave de objeto de nombre de bloque" del último objeto cuya notificación ha fallado. (Para ver este mensaje, seleccione **NODES > Storage Node > Events**. Ver último evento en la parte superior de la tabla). Los mensajes de eventos también se muestran en la `/var/local/log/bycast-err.log`.

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

Información relacionada

[Gestión de objetos con ILM](#)

Respuestas de error

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

códigos de error API de S3 admitidos

Nombre	Estado de HTTP
ACCESSDENIED	403 Prohibido
BadDigest	400 solicitud incorrecta
BucketAlreadyExists	409 conflicto
BucketNotEmpty	409 conflicto
IncompleteBody	400 solicitud incorrecta
Internalerror	500 error de servidor interno
InvalidAccessKeyId	403 Prohibido

Nombre	Estado de HTTP
InvalidArgument	400 solicitud incorrecta
InvalidBucketName	400 solicitud incorrecta
InvalidBucketState	409 conflicto
InvalidDigest	400 solicitud incorrecta
InvalidEncryptionAlgorithmError	400 solicitud incorrecta
InvalidPart	400 solicitud incorrecta
InvalidPartOrder	400 solicitud incorrecta
InvalidRange	416 rango solicitado no utilizable
InvalidRequest	400 solicitud incorrecta
InvalidStorageClass	400 solicitud incorrecta
InvalidTag	400 solicitud incorrecta
InvalidURI	400 solicitud incorrecta
KeyTooLong	400 solicitud incorrecta
MalformedXML	400 solicitud incorrecta
MetadataTooLarge	400 solicitud incorrecta
MethodNotAllowed	405 método no permitido
MissingContentLength	411 longitud requerida
MissingRequestBodyError	400 solicitud incorrecta
MissingSecurityHeader	400 solicitud incorrecta
NoSuchBucket	404 no encontrado
NoSuchKey	404 no encontrado
NoSuchUpload	404 no encontrado

Nombre	Estado de HTTP
NotImplimed	501 no implementada
NoSuchBucketPolicy	404 no encontrado
ObjectLockConfigurationNotFound	404 no encontrado
Error de preconditionError	Error de condición 412
RequestTimeTooSowed	403 Prohibido
ServiceUnavailable	503 Servicio no disponible
SignatureDoesNotMatch	403 Prohibido
Cucharones TooMany	400 solicitud incorrecta
UserKeyMustBeSpecified	400 solicitud incorrecta

códigos de error personalizados de StorageGRID

Nombre	Descripción	Estado de HTTP
XBucketLifecycleNotAllowed	No se permite la configuración del ciclo de vida de los bloques en un bloque compatible heredado	400 solicitud incorrecta
XBucketPolicyParseException	Error al analizar la política JSON de bloques recibidos.	400 solicitud incorrecta
XCondit. Cumplimiento	Operación denegada debido a la configuración de cumplimiento anterior.	403 Prohibido
XDSLAReducedRedundancyForbidden	No se permite una redundancia reducida en el bloque compatible con la tecnología heredada	400 solicitud incorrecta
XMaxBucketPolicyLengthExceeded	Su política supera la longitud máxima permitida de la política de bloques.	400 solicitud incorrecta
XMissingInternalRequestHeader	Falta un encabezado de una solicitud interna.	400 solicitud incorrecta

Nombre	Descripción	Estado de HTTP
Cumplimiento de XNoSuchBucketCompliance	El bloque especificado no tiene la conformidad heredada activada.	404 no encontrado
XNotAcceptable	La solicitud contiene uno o más encabezados de aceptación que no se han podido satisfacer.	406 no aceptable
XNotImplemed	La solicitud que ha proporcionado implica una funcionalidad que no se ha implementado.	501 no implementada

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.