



Operaciones sobre objetos

StorageGRID software

NetApp

December 03, 2025

Tabla de contenidos

Operaciones sobre objetos	1
Operaciones sobre objetos	1
Utilice S3 Select	5
Cláusulas	5
Tipos de datos	5
Operadores	5
Funciones agregadas	6
Funciones condicionales	6
Funciones de conversión	6
Funciones de fecha	7
Funciones de cadena	7
Utilice cifrado del lado del servidor	7
Utilice SSE	7
Utilice SSE-C	8
Consideraciones para el uso del cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C)	8
Copiar objeto	9
Resolver conflictos	9
Tamaño del objeto	9
Caracteres UTF-8 en metadatos de usuario	9
Encabezados de solicitud admitidos	10
Encabezados de solicitud no admitidos	11
Opciones de clase de almacenamiento	11
Uso de x-amz-copy-source en CopyObject	12
Encabezados de solicitud para el cifrado del lado del servidor	12
Control de versiones	13
Obtener objeto	13
GetObject y objetos multipart	13
Caracteres UTF-8 en metadatos de usuario	13
Encabezado de solicitud compatible	13
Encabezado de solicitud no compatible	14
Control de versiones	14
Encabezados de solicitud para cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)	14
Comportamiento de GetObject para objetos del grupo de almacenamiento en la nube	14
GetObject y replicación entre cuadrículas	15
Objeto principal	16
Objetos HeadObject y multipart	16
Caracteres UTF-8 en metadatos de usuario	16
Encabezado de solicitud compatible	16
Encabezado de solicitud no compatible	16
Control de versiones	16
Encabezados de solicitud para cifrado del lado del servidor con claves de cifrado proporcionadas por	

el cliente (SSE-C)	16
Respuestas de HeadObject para objetos de Cloud Storage Pool	17
Replicación de HeadObject y entre cuadrículas	19
PonerObjeto	19
Resolver conflictos	19
Tamaño del objeto	19
Tamaño de los metadatos del usuario	19
Caracteres UTF-8 en metadatos de usuario	20
Límites de etiquetas de objetos	20
Propiedad de los objetos	20
Encabezados de solicitud admitidos	20
Encabezados de solicitud no admitidos	21
Opciones de clase de almacenamiento	22
Encabezados de solicitud para el cifrado del lado del servidor	23
Control de versiones	23
Cálculos de firma para el encabezado de autorización	24
Restaurar objeto	24
Tipo de solicitud admitido	24
Control de versiones	24
Comportamiento de RestoreObject en objetos del grupo de almacenamiento en la nube	24
Seleccionar contenido del objeto	25
Ejemplo de sintaxis de solicitud CSV	26
Ejemplo de sintaxis de solicitud de Parquet	27
Ejemplo de consulta SQL	28
Ejemplo de uso de AWS-CLI (CSV)	29
Ejemplo de uso de AWS-CLI (Parquet)	30

Operaciones sobre objetos

Operaciones sobre objetos

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

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

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

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

Operación	Implementación
Eliminar objeto	<p data-bbox="591 163 1481 233">Autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles</p> <p data-bbox="591 268 1481 506">Al procesar una solicitud <code>DeleteObject</code>, StorageGRID intenta eliminar inmediatamente todas las copias del objeto de todas las ubicaciones almacenadas. Si tiene éxito, StorageGRID devuelve una respuesta al cliente inmediatamente. Si no se pueden eliminar todas las copias en 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y luego indica el éxito al cliente.</p> <p data-bbox="591 541 867 569">Control de versiones</p> <p data-bbox="631 583 1481 789">Para eliminar una versión específica, el solicitante debe ser el propietario del depósito y utilizar el <code>versionId</code> subrecurso. El uso de este subrecurso elimina permanentemente la versión. Si el <code>versionId</code> corresponde a un marcador de eliminación, el encabezado de respuesta <code>x-amz-delete-marker</code> se devuelve establecido en <code>true</code>.</p> <ul data-bbox="656 825 1481 1304" style="list-style-type: none"> • Si se elimina un objeto sin el <code>versionId</code> subrecurso en un bucket con control de versiones habilitado, esto genera un marcador de eliminación. El <code>versionId</code> para el marcador de eliminación se devuelve utilizando el <code>x-amz-version-id</code> encabezado de respuesta y el <code>x-amz-delete-marker</code> El encabezado de respuesta se devuelve configurado en <code>true</code>. • Si se elimina un objeto sin el <code>versionId</code> subrecurso en un bucket con control de versiones suspendido, esto da como resultado una eliminación permanente de una versión 'nula' ya existente o un marcador de eliminación 'nulo' y la generación de un nuevo marcador de eliminación 'nulo'. El <code>x-amz-delete-marker</code> El encabezado de respuesta se devuelve configurado en <code>true</code>. <p data-bbox="680 1339 1481 1402">Nota: En ciertos casos, pueden existir múltiples marcadores de eliminación para un objeto.</p> <p data-bbox="591 1455 1481 1556">Ver"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" para aprender cómo eliminar versiones de objetos en el modo GOBERNANZA.</p>
Eliminar objetos (anteriormente llamado ELIMINAR Múltiples Objetos)	<p data-bbox="591 1606 1481 1675">Autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles</p> <p data-bbox="591 1711 1435 1745">Se pueden eliminar varios objetos en el mismo mensaje de solicitud.</p> <p data-bbox="591 1780 1481 1881">Ver"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" para aprender cómo eliminar versiones de objetos en el modo GOBERNANZA.</p>

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

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

Utilice S3 Select

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



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

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

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

Cláusulas

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

Tipos de datos

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

Operadores

Operadores lógicos

- Y
- NO
- O

Operadores de comparación

- <
- >
- <=
- >=
- =
- =

- <>
- !=
- ENTRE
- EN

Operadores de coincidencia de patrones

- COMO
- _
- %

Operadores unitarios

- ES NULO
- NO ES NULO

Operadores matemáticos

- +
- -
- *
- /
- %

StorageGRID sigue la precedencia del operador Amazon S3 Select.

Funciones agregadas

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

Funciones condicionales

- CASO
- JUNTARSE
- NULLIF

Funciones de conversión

- CAST (para tipos de datos admitidos)

Funciones de fecha

- FECHA_AÑADIR
- FECHA_DIFF
- EXTRACTO
- A_CADENA
- HASTA_LA_MARCA_DE_TIEMPO
- UTCNOW

Funciones de cadena

- LONGITUD_CHARACTER, LONGITUD_CHARACTER
- MÁS BAJO
- SUBCADENA
- RECORTAR
- SUPERIOR

Utilice cifrado del lado del servidor

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

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

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

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



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



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

Utilice SSE

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

x-amz-server-side-encryption

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

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

Utilice SSE-C

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

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

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

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

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

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

- Debes utilizar https.



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

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



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

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

Información relacionada

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

Copiar objeto

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

Resolver conflictos

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

Tamaño del objeto

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

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



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

Caracteres UTF-8 en metadatos de usuario

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

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

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

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

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

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

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

- Encabezados de solicitud de bloqueo de objetos S3:

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

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

- Encabezados de solicitud SSE:

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

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

Ver [Encabezados de solicitud para el cifrado del lado del servidor](#)

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

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

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

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

Opciones de clase de almacenamiento

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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



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

Uso de x-amz-copy-source en CopyObject

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

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

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

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

Encabezados de solicitud para el cifrado del lado del servidor

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

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



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

- Si desea cifrar el objeto de destino (la copia) con una clave única administrada por StorageGRID (SSE),

incluya este encabezado en la solicitud CopyObject:

◦ `x-amz-server-side-encryption`



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

Control de versiones

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

Obtener objeto

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

GetObject y objetos multipart

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

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

Caracteres UTF-8 en metadatos de usuario

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

Encabezado de solicitud compatible

Se admite el siguiente encabezado de solicitud:

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

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

Encabezado de solicitud no compatible

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

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

Control de versiones

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

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

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

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



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

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

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



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

Estado del objeto	Comportamiento de <code>GetObject</code>
Objeto ingerido en <code>StorageGRID</code> pero aún no evaluado por ILM, u objeto almacenado en un grupo de almacenamiento tradicional o que utiliza codificación de borrado	200 OK Se recupera una copia del objeto.
Objeto en el grupo de almacenamiento en la nube pero que aún no ha pasado a un estado no recuperable	200 OK Se recupera una copia del objeto.

Estado del objeto	Comportamiento de GetObject
Objeto en transición a un estado no recuperable	403 Forbidden , InvalidObjectState Utilice un "Restaurar objeto" solicitud para restaurar el objeto a un estado recuperable.
Objeto en proceso de restauración desde un estado no recuperable	403 Forbidden , InvalidObjectState Espere a que se complete la solicitud RestoreObject.
Objeto completamente restaurado al grupo de almacenamiento en la nube	200 OK Se recupera una copia del objeto.

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

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

En estos casos:

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

GetObject y replicación entre cuadrículas

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

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



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

Objeto principal

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

Objetos HeadObject y multipart

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

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

Caracteres UTF-8 en metadatos de usuario

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

Encabezado de solicitud compatible

Se admite el siguiente encabezado de solicitud:

- `x-amz-checksum-mode`

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

Encabezado de solicitud no compatible

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

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

Control de versiones

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

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

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

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



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

Respuestas de HeadObject para objetos de Cloud Storage Pool

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

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

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

Estado del objeto	Respuesta a HeadObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un grupo de almacenamiento tradicional o que utiliza codificación de borrado	200 OK(No se devuelve ningún encabezado de respuesta especial).
Objeto en el grupo de almacenamiento en la nube pero que aún no ha pasado a un estado no recuperable	<p>200 OK</p> <p><code>x-amz-storage-class</code>: GLACIER</p> <p><code>x-amz-restore</code>: <code>ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code></p> <p>Hasta que el objeto pase a un estado no recuperable, el valor de <code>expiry-date</code> Está ambientado en un momento distante en el futuro. El tiempo exacto de transición no está controlado por el sistema StorageGRID .</p>

Estado del objeto	Respuesta a HeadObject
El objeto ha pasado al estado no recuperable, pero también existe al menos una copia en la cuadrícula	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>El valor de expiry-date Está ambientado en un momento distante en el futuro.</p> <p>Nota: Si la copia en la red no está disponible (por ejemplo, un nodo de almacenamiento está inactivo), debe emitir un "Restaurar objeto" solicitud para restaurar la copia del grupo de almacenamiento en la nube antes de poder recuperar el objeto con éxito.</p>
El objeto pasó a un estado no recuperable y no existe ninguna copia en la cuadrícula	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
Objeto en proceso de restauración desde un estado no recuperable	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>
Objeto completamente restaurado al grupo de almacenamiento en la nube	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"</p> <p>El expiry-date Indica cuándo el objeto en el grupo de almacenamiento en la nube volverá a un estado no recuperable.</p>

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

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

Replicación de HeadObject y entre cuadrículas

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

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



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

PonerObjeto

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

Resolver conflictos

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

Tamaño del objeto

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

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



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

Tamaño de los metadatos del usuario

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

Caracteres UTF-8 en metadatos de usuario

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

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

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

Límites de etiquetas de objetos

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

Propiedad de los objetos

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

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

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

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

Se admite la codificación de transferencia fragmentada si `aws-chunked`. También se utiliza la firma de

carga útil.

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

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

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

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

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

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



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

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

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

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

Ver [Encabezados de solicitud para el cifrado del lado del servidor](#)

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

- `x-amz-acl`

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

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

Opciones de clase de almacenamiento

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

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

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

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

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

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

Usando el **REDUCED_REDUNDANCY** Esta opción no se recomienda en otras circunstancias.

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



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

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



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

Encabezados de solicitud para el cifrado del lado del servidor

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

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

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

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

- **SSE-C:** utilice estos tres encabezados si desea cifrar el objeto con una clave única que usted proporcione y administre.

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

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

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



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



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

Control de versiones

Si el control de versiones está habilitado para un bucket, se creará un único `versionId` Se genera automáticamente para la versión del objeto que se está almacenando. Este `versionId` También se devuelve

en la respuesta utilizando el `x-amz-version-id` encabezado de respuesta.

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

Cálculos de firma para el encabezado de autorización

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

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



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

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

Información relacionada

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

Restaurar objeto

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

Tipo de solicitud admitido

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

Control de versiones

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

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

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



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

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

Seleccionar contenido del objeto

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

Para más información véase ["Referencia de la API de Amazon Simple Storage Service: SelectObjectContent"](#)

Antes de empezar

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

Ejemplo de sintaxis de solicitud CSV

```

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

```

Ejemplo de sintaxis de solicitud de Parquet

```

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

```

Ejemplo de consulta SQL

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

```

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

```

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

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

Ejemplo de uso de AWS-CLI (CSV)

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

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

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


Ejemplo de uso de AWS-CLI (Parquet)

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

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

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

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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