



Operações em objetos

StorageGRID software

NetApp
July 23, 2026

Índice

Operações em objetos	1
Como o StorageGRID implementa operações da API REST do S3 para objetos	1
Operações Amazon S3 Select suportadas no StorageGRID	4
Cláusulas	5
Tipos de dados	5
Operadores	5
Funções agregadas	6
Funções condicionais	6
Funções de conversão	6
Funções de data	6
Funções de string	7
Como StorageGRID usa criptografia do lado do servidor	7
Use SSE	7
Use SSE-C	8
Considerações sobre o uso de criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)	8
Crie uma cópia de um objeto no StorageGRID com a solicitação S3 CopyObject	9
Resolver conflitos	9
Tamanho do objeto	9
Caracteres UTF-8 nos metadados do usuário	9
Cabeçalhos de solicitação suportados	10
Cabeçalhos de solicitação não suportados	11
Opções de classe de armazenamento	11
Usando x-amz-copy-source em CopyObject	12
Cabeçalhos de solicitação para criptografia do lado do servidor	12
Controle de versões	13
Recuperar um objeto de um bucket no StorageGRID com a solicitação GetObject	13
GetObject e objetos multipartes	13
Caracteres UTF-8 nos metadados do usuário	13
Cabeçalho de solicitação compatível	13
Cabeçalho de solicitação não suportado	14
Controle de versões	14
Cabeçalhos de solicitação para criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)	14
Comportamento de GetObject para objetos do Cloud Storage Pool	14
GetObject e replicação entre grades	15
Recuperar metadados de um objeto no StorageGRID com a solicitação S3 HeadObject	16
HeadObject e objetos multipartes	16
Caracteres UTF-8 nos metadados do usuário	16
Cabeçalho de solicitação compatível	16
Cabeçalho de solicitação não suportado	16
Controle de versões	16
Cabeçalhos de solicitação para criptografia do lado do servidor com chaves de criptografia fornecidas	

pelo cliente (SSE-C)	17
HeadObject respostas para objetos do Cloud Storage Pool	17
HeadObject e replicação entre grades	19
Adicionar um objeto a um bucket no StorageGRID com a solicitação S3 PutObject	19
Resolver conflitos	19
Tamanho do objeto	19
Tamanho dos metadados do usuário	19
Caracteres UTF-8 nos metadados do usuário	20
Limites de tags de objeto	20
Propriedade do objeto	20
Cabeçalhos de solicitação suportados	20
Cabeçalhos de solicitação não suportados	21
Opções de classe de armazenamento	22
Cabeçalhos de solicitação para criptografia do lado do servidor	23
Controle de versões	24
Cálculos de assinatura para o cabeçalho Authorization	24
Restaurar um objeto no StorageGRID com a solicitação S3 RestoreObject	24
Tipo de solicitação compatível	24
Controle de versões	24
Comportamento de RestoreObject em objetos do Cloud Storage Pool	24
Filtrar dados de objetos no StorageGRID com a solicitação S3 SelectObjectContent	25
Exemplo de sintaxe de solicitação CSV	26
Exemplo de sintaxe de solicitação Parquet	27
Exemplo de consulta SQL	28
Exemplo de uso do AWS-CLI (CSV)	29
Exemplo de uso da AWS-CLI (Parquet)	30

Operações em objetos

Como o StorageGRID implementa operações da API REST do S3 para objetos

Esta seção descreve como o sistema StorageGRID implementa as operações da API REST do S3 para objetos.

As seguintes condições aplicam-se a todas as operações de objeto:

- StorageGRID "[valores de consistência](#)" é compatível com todas as operações em objetos, com exceção das seguintes:
 - `GetObjectAcl`
 - `OPTIONS /`
 - `PutObjectLegalHold`
 - `PutObjectRetention`
 - `SelectObjectContent`
- Solicitações conflitantes de clientes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio "latest-wins". O momento da avaliação do "latest-wins" é determinado quando o sistema StorageGRID conclui uma determinada solicitação, e não quando os clientes S3 iniciam uma operação.
- Todos os objetos em um bucket do StorageGRID pertencem ao proprietário do bucket, incluindo objetos criados por um usuário anônimo ou por outra conta.

A tabela a seguir descreve como o StorageGRID implementa as operações de objetos da API REST do S3.

Operação	Implementação
DeleteObject	Ao processar uma solicitação DeleteObject, StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais de armazenamento. Se for bem-sucedido, StorageGRID retorna uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas em 30 segundos (por exemplo, porque um local está temporariamente indisponível), StorageGRID coloca as cópias em fila para remoção e então indica sucesso ao cliente. Restrições • A autenticação multifator (MFA) e o cabeçalho de resposta <code>x-amz-mfa</code> não são suportados. • Os <code>If-None</code> e <code>If-None-Match</code> cabeçalhos são aceitos, mas não funcionais. Controle de versões Para remover uma versão específica, o solicitante deve ser o proprietário do bucket e usar o <code>versionId</code> sub-recurso. Usar esse sub-recurso exclui permanentemente a versão. Se o <code>versionId</code> corresponder a um marcador de exclusão, o cabeçalho de resposta <code>x-amz-delete-marker</code> é retornado definido como <code>true</code>. • Se um objeto for excluído sem o <code>versionId</code> sub-recurso em um bucket com versionamento ativado, isso resulta na geração de um marcador de exclusão. O <code>versionId</code> marcador de exclusão é retornado usando o <code>x-amz-version-id</code> cabeçalho de resposta, e o <code>x-amz-delete-marker</code> cabeçalho de resposta é retornado definido como <code>true</code>. • Se um objeto for excluído sem o <code>versionId</code> sub-recurso em um bucket com versionamento suspenso, isso resulta na exclusão permanente de uma versão "null" já existente ou de um marcador de exclusão "null", e na geração de um novo marcador de exclusão "null". O cabeçalho de resposta <code>x-amz-delete-marker</code> é retornado definido como <code>true</code>. Nota: Em certos casos, vários marcadores de exclusão podem existir para um objeto. Veja "Use a API REST S3 para configurar o S3 Object Lock" para saber como excluir versões de objetos no modo GOVERNANÇA.
DeleteObjects (anteriormente chamado de DELETE Multiple Objects)	A autenticação multifator (MFA) e o cabeçalho de resposta <code>x-amz-mfa</code> não são suportados. Vários objetos podem ser excluídos na mesma mensagem de solicitação. Veja "Use a API REST S3 para configurar o S3 Object Lock" para saber como excluir versões de objetos no modo GOVERNANÇA.

Operação	Implementação
DeleteObjectTagging	Utiliza o tagging subrecurso para remover todas as tags de um objeto. Controle de versões Se o <code>versionId</code> parâmetro de consulta não for especificado na solicitação, a operação exclui todas as tags da versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status " <code>MethodNotAllowed</code> " será retornado com o cabeçalho de resposta <code>x-amz-delete-marker</code> definido como <code>true</code>.
GetObject	"GetObject"
GetObjectAcl	Se as credenciais de acesso necessárias forem fornecidas para a conta, a operação retorna uma resposta positiva e o ID, DisplayName e a Permissão do proprietário do objeto, indicando que o proprietário tem acesso total ao objeto.
GetObjectLegalHold	"Use a API REST S3 para configurar o S3 Object Lock"
GetObjectRetention	"Use a API REST S3 para configurar o S3 Object Lock"
GetObjectTagging	Utiliza o tagging subrecurso para retornar todas as tags de um objeto. Controle de versões Se o <code>versionId</code> parâmetro de consulta não for especificado na solicitação, a operação retorna todas as tags da versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status " <code>MethodNotAllowed</code> " será retornado com o cabeçalho de resposta <code>x-amz-delete-marker</code> definido como <code>true</code>.
HeadObject	"HeadObject"
RestoreObject	"RestoreObject"
PutObject	"PutObject"
CopyObject (anteriormente denominado PUT Object - Copy)	"CopyObject"
PutObjectLegalHold	"Use a API REST S3 para configurar o S3 Object Lock"
PutObjectRetention	"Use a API REST S3 para configurar o S3 Object Lock"

Operação	Implementação
PutObjectTagging	Utiliza o <code>tagging</code> subrecurso para adicionar um conjunto de tags a um objeto existente. Limites de tags de objeto Você pode adicionar tags a novos objetos ao carregá-los ou pode adicioná-las a objetos existentes. Tanto StorageGRID quanto Amazon S3 suportam até 10 tags por objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode e os valores de tag podem ter até 256 caracteres Unicode. Chaves e valores diferenciam maiúsculas de minúsculas. Atualizações de tags e comportamento de ingestão Quando você usa PutObjectTagging para atualizar as tags de um objeto, o StorageGRID não o ingere novamente. Isso significa que a opção de Comportamento de Ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento do objeto acionadas pela atualização são feitas quando o ILM é reavaliado pelos processos normais de ILM em segundo plano. Isso significa que, se a regra ILM usar a opção "Estrita" para o comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objeto necessários não puderem ser feitos (por exemplo, porque um local recém-necessário não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível. Resolução de conflitos Solicitações conflitantes de clientes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio "latest-wins". O momento da avaliação do "latest-wins" é determinado quando o sistema StorageGRID conclui uma determinada solicitação, e não quando os clientes S3 iniciam uma operação. Controle de versões Se o <code>versionId</code> parâmetro de consulta não for especificado na solicitação, a operação adiciona tags à versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status <code>""MethodNotAllowed""</code> é retornado com o cabeçalho de resposta <code>`x-amz-delete-marker`</code> definido como <code>`true`</code>.
SelectObjectContent	"SelectObjectContent"

Operações Amazon S3 Select suportadas no StorageGRID

StorageGRID oferece suporte às seguintes cláusulas SELECT do Amazon S3, tipos de

dados e operadores para o ["Comando SelectObjectContent"](#).



Quaisquer itens não listados não são suportados.

Para sintaxe, consulte ["SelectObjectContent"](#). Para mais informações sobre S3 Select, consulte o ["Documentação da AWS para S3 Select"](#).

Somente contas de locatário com o S3 Select ativado podem emitir consultas SelectObjectContent. Consulte o ["Considerações e requisitos para usar o S3 Select"](#).

Cláusulas

- Lista de seleção
- Cláusula FROM
- Cláusula WHERE
- Cláusula LIMIT

Tipos de dados

- bool
- inteiro
- string
- float
- decimal, numérico
- carimbo de data/hora

Operadores

Operadores lógicos

- E
- NÃO
- OU

Operadores de comparação

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

- ENTRE
- EM

Operadores de correspondência de padrões

- CURTIR
- _
- %

Operadores unitários

- É NULO
- NÃO É NULO

Operadores matemáticos

- +
- -
- *
- /
- %

StorageGRID segue a precedência do operador Amazon S3 Select.

Funções agregadas

- AVG()
- COUNT(*)
- MAX()
- MIN()
- SOMA()

Funções condicionais

- CASO
- COALESCE
- NULLIF

Funções de conversão

- CAST (para tipo de dados suportado)

Funções de data

- DATE_ADD
- DATE_DIFF

- EXTRAIR
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

Funções de string

- CHAR_LENGTH, CHARACTER_LENGTH
- MAIS BAIXO
- SUBSTRING
- TRIM
- SUPERIOR

Como StorageGRID usa criptografia do lado do servidor

A criptografia do lado do servidor permite que você proteja seus dados de objeto em repouso. StorageGRID criptografa os dados ao gravar o objeto e os descriptografa quando você acessa o objeto.

Se você deseja usar criptografia do lado do servidor, pode escolher uma das duas opções mutuamente exclusivas, com base em como as chaves de criptografia são gerenciadas:

- **SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID):** Quando você envia uma solicitação S3 para armazenar um objeto, o StorageGRID criptografa o objeto com uma chave exclusiva. Quando você envia uma solicitação S3 para recuperar o objeto, o StorageGRID usa a chave armazenada para descriptografar o objeto.
- **SSE-C (server-side encryption with customer-provided keys):** Ao enviar uma solicitação ao S3 para armazenar um objeto, você fornece sua própria chave de criptografia. Ao recuperar um objeto, você fornece a mesma chave de criptografia como parte da sua solicitação. Se as duas chaves de criptografia coincidirem, o objeto é descriptografado e seus dados do objeto são retornados.

Embora o StorageGRID gerencie todas as operações de criptografia e descriptografia de objetos, você deve gerenciar as chaves de criptografia que fornecer.



As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente.



Se um objeto for criptografado com SSE ou SSE-C, quaisquer configurações de criptografia em nível de bucket ou de grid serão ignoradas.

Use SSE

Para criptografar um objeto com uma chave exclusiva gerenciada pelo StorageGRID, você usa o seguinte cabeçalho de solicitação:

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

O cabeçalho de solicitação SSE é compatível com as seguintes operações de objeto:

- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"

Use SSE-C

Para criptografar um objeto com uma chave exclusiva que você gerencia, você usa três cabeçalhos de solicitação:

Cabeçalho da solicitação	Descrição
x-amz-server-side-encryption-customer-algorithm	Especifique o algoritmo de criptografia. O valor do cabeçalho deve ser AES256.
x-amz-server-side-encryption-customer-key	Especifique a chave de criptografia que será usada para criptografar ou descriptografar o objeto. O valor da chave deve ser de 256 bits, codificado em base64.
x-amz-server-side-encryption-customer-key-MD5	Especifique o resumo MD5 da chave de criptografia de acordo com a RFC 1321, que é usado para garantir que a chave de criptografia foi transmitida sem erro. O valor do resumo MD5 deve ser codificado em base64 com 128 bits.

Os cabeçalhos de solicitação SSE-C são suportados pelas seguintes operações de objeto:

- "GetObject"
- "HeadObject"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Considerações sobre o uso de criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Antes de usar o SSE-C, esteja ciente das seguintes considerações:

- Você deve usar https.



StorageGRID rejeita quaisquer solicitações feitas via http ao usar SSE-C. Por questões de segurança, você deve considerar qualquer chave enviada acidentalmente via http como comprometida. Descarte a chave e faça a rotação conforme apropriado.

- O ETag na resposta não é o MD5 dos dados do objeto.

- Você deve gerenciar o mapeamento das chaves de criptografia para os objetos. StorageGRID não armazena chaves de criptografia. Você é responsável por controlar a chave de criptografia que fornecer para cada objeto.
- Se o seu bucket tiver o versionamento ativado, cada versão do objeto deverá ter sua própria chave de criptografia. Você é responsável por controlar a chave de criptografia usada para cada versão do objeto.
- Como você gerencia as chaves de criptografia no lado do cliente, também deve gerenciar quaisquer medidas de segurança adicionais, como a rotação de chaves, no lado do cliente.



As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente.

- Se a replicação entre grades ou a replicação CloudMirror estiver configurada para o bucket, você não poderá ingerir objetos SSE-C. A operação de ingestão falhará.

Informações relacionadas

["Guia do usuário do Amazon S3: usando criptografia do lado do servidor com chaves fornecidas pelo cliente \(SSE-C\)"](#)

Crie uma cópia de um objeto no StorageGRID com a solicitação S3 CopyObject

Você pode usar a solicitação S3 CopyObject para criar uma cópia de um objeto que já está armazenado no S3. Uma operação CopyObject é a mesma que executar GetObject seguido de PutObject.

Resolver conflitos

Solicitações conflitantes de clientes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio "latest-wins". O momento da avaliação do "latest-wins" é determinado quando o sistema StorageGRID conclui uma determinada solicitação, e não quando os clientes S3 iniciam uma operação.

Tamanho do objeto

O tamanho máximo *recomendado* para uma única operação PutObject é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use ["upload multipart"](#) em vez disso.

O tamanho máximo *suportado* para uma única operação PutObject é de 5 TiB (5.497.558.138.880 bytes).



Se você atualizou do StorageGRID 11.6 ou anterior, o alerta "Tamanho do objeto S3 PUT muito grande" será acionado se você tentar fazer o upload de um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11.7 ou 11.8, o alerta não será acionado nesse caso. No entanto, para alinhar com o padrão AWS S3, as versões futuras do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

Caracteres UTF-8 nos metadados do usuário

Se uma solicitação incluir valores UTF-8 (sem escape) no nome da chave ou no valor dos metadados definidos pelo usuário, o comportamento do StorageGRID será indefinido.

StorageGRID não analisa nem interpreta caracteres UTF-8 escapados incluídos no nome da chave ou no

valor dos metadados definidos pelo usuário. Caracteres UTF-8 escapados são tratados como caracteres ASCII:

- As solicitações são bem-sucedidas se os metadados definidos pelo usuário incluírem caracteres UTF-8 escapados.
- StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome ou valor da chave incluir caracteres não imprimíveis.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `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 por um par nome-valor contendo metadados definidos pelo usuário
- `x-amz-metadata-directive`: O valor padrão é `COPY`, o que permite que você copie o objeto e os metadados associados.

Você pode especificar `REPLACE` para sobrescrever os metadados existentes ao copiar o objeto ou para atualizar os metadados do objeto.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: O valor padrão é `COPY`, que permite copiar o objeto e todas as tags.

Você pode especificar `REPLACE` para sobrescrever as tags existentes ao copiar o objeto ou para atualizar as tags.

- Cabeçalhos da solicitação S3 Object Lock:

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

Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular o modo de versão do objeto e a data de retenção. Consulte ["Use a API REST S3 para configurar o S3 Object Lock"](#).

- Cabeçalhos de solicitação 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 [Cabeçalhos de solicitação para criptografia do lado do servidor](#)

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- If-Match

O If-Match header é aceito, mas não funcional.

- If-None-Match

O If-None-Match header é aceito, mas não funcional.

- x-amz-checksum-algorithm

Ao copiar um objeto, se o objeto de origem tiver um checksum, StorageGRID não copia esse valor de checksum para o novo objeto. Esse comportamento se aplica independentemente de você tentar usar x-amz-checksum-algorithm na solicitação do objeto.

- x-amz-website-redirect-location

Opções de classe de armazenamento

O `x-amz-storage-class` cabeçalho da solicitação é compatível e afeta quantas cópias de objetos o StorageGRID cria se a regra ILM correspondente usar o Dual commit ou Balanced "[opção de ingestão](#)".

- STANDARD

(Padrão) Especifica uma operação de ingestão de confirmação dupla quando a regra ILM usa a opção Dual commit ou quando a opção Balanced recorre à criação de cópias intermediárias.

- REDUCED_REDUNDANCY

Especifica uma operação de ingestão de confirmação única quando a regra ILM usa a opção de confirmação dupla ou quando a opção balanceada recorre à criação de cópias intermediárias.



Se você estiver ingerindo um objeto em um bucket com S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket legado Compliant, a `REDUCED_REDUNDANCY` opção retornará um erro. StorageGRID sempre realizará uma ingestão com confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Usando x-amz-copy-source em CopyObject

Se o bucket e a chave de origem, especificados no `x-amz-copy-source` cabeçalho, forem diferentes do bucket de destino e da chave de destino, uma cópia dos dados do objeto de origem é gravada no destino.

Se a origem e o destino coincidirem e o `x-amz-metadata-directive` cabeçalho for especificado como `REPLACE`, os metadados do objeto serão atualizados com os valores de metadados fornecidos na solicitação. Nesse caso, StorageGRID não reingere o objeto. Isso tem duas consequências importantes:

- Não é possível usar CopyObject para criptografar um objeto existente no local ou para alterar a criptografia de um objeto existente no local. Se você fornecer o `x-amz-server-side-encryption` cabeçalho ou o `x-amz-server-side-encryption-customer-algorithm` cabeçalho, StorageGRID rejeita a solicitação e retorna `XNotImplemented`.
- A opção de Comportamento de Ingestão especificada na regra ILM correspondente não é utilizada. Quaisquer alterações no posicionamento do objeto que sejam acionadas pela atualização são feitas quando o ILM é reavaliado pelos processos ILM normais em segundo plano.

Isso significa que, se a regra ILM usar a opção "Estrita" para o comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objeto necessários não puderem ser feitos (por exemplo, porque um local recém-necessário não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível.

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você "[usar criptografia do lado do servidor](#)" fizer isso, os cabeçalhos da solicitação que você fornecer dependerão de o objeto de origem estar criptografado e de você planejar criptografar o objeto de destino.

- Se o objeto de origem estiver criptografado usando uma chave fornecida pelo cliente (SSE-C), você deverá incluir os três cabeçalhos a seguir na solicitação CopyObject, para que o objeto possa ser descriptografado e copiado:
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: especifique AES256.
 - `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia que você forneceu ao criar o objeto de origem.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu ao criar o objeto de origem.
- Se você deseja criptografar o objeto de destino (a cópia) com uma chave exclusiva que você fornece e gerencia, inclua os três cabeçalhos a seguir:
 - `x-amz-server-side-encryption-customer-algorithm`: Especifique AES256.
 - `x-amz-server-side-encryption-customer-key`: Especifique uma nova chave de criptografia para o objeto de destino.
 - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o hash MD5 da nova chave

de criptografia.



As chaves de criptografia fornecidas por você nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para ["usando criptografia do lado do servidor"](#).

- Se você deseja criptografar o objeto de destino (a cópia) com uma chave exclusiva gerenciada pelo StorageGRID (SSE), inclua este cabeçalho na solicitação CopyObject:

◦ `x-amz-server-side-encryption`



O `server-side-encryption` valor do objeto não pode ser atualizado. Em vez disso, faça uma cópia com um novo `server-side-encryption` valor usando `x-amz-metadata-directive: REPLACE`.

Controle de versões

Se o bucket de origem for versionado, você pode usar o `x-amz-copy-source` cabeçalho para copiar a versão mais recente de um objeto. Para copiar uma versão específica de um objeto, você deve especificar explicitamente a versão a ser copiada usando o `versionId` sub-recurso. Se o bucket de destino for versionado, a versão gerada será retornada no `x-amz-version-id` cabeçalho da resposta. Se o versionamento estiver suspenso para o bucket de destino, então `x-amz-version-id` retorna o valor "null".

Recuperar um objeto de um bucket no StorageGRID com a solicitação GetObject

Você pode usar a solicitação S3 GetObject para recuperar um objeto de um bucket S3.

GetObject e objetos multipartes

Você pode usar o `partNumber` parâmetro de solicitação para recuperar uma parte específica de um objeto multipart ou segmentado. O `x-amz-mp-parts-count` elemento de resposta indica quantas partes o objeto possui.

Você pode definir `partNumber` como 1 tanto para objetos segmentados/multipartes quanto para objetos não segmentados/não multipartes; no entanto, o elemento de resposta `x-amz-mp-parts-count` só é retornado para objetos segmentados ou multipartes.

Caracteres UTF-8 nos metadados do usuário

StorageGRID não analisa nem interpreta caracteres UTF-8 escapados em metadados definidos pelo usuário. Solicitações GET para um objeto com caracteres UTF-8 escapados em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome da chave ou o valor incluir caracteres não imprimíveis.

Cabeçalho de solicitação compatível

O seguinte cabeçalho de solicitação é compatível:

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

O Range`cabeçalho não é compatível com `x-amz-checksum-mode para GetObject. Quando você inclui Range na solicitação com x-amz-checksum-mode ativado, StorageGRID não retorna um valor de checksum na resposta.

Cabeçalho de solicitação não suportado

O seguinte cabeçalho de solicitação não é compatível e retorna XNotImplemented:

- x-amz-website-redirect-location

Controle de versões

Se um versionId subrecurso não for especificado, a operação busca a versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, o status "Não encontrado" é retornado com o x-amz-delete-marker cabeçalho de resposta definido como true.

Cabeçalhos de solicitação para criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Utilize os três cabeçalhos se o objeto estiver criptografado com uma chave exclusiva que você forneceu.

- x-amz-server-side-encryption-customer-algorithm: Especifique AES256.
- x-amz-server-side-encryption-customer-key: Especifique sua chave de criptografia para o objeto.
- x-amz-server-side-encryption-customer-key-MD5: Especifique o resumo MD5 da chave de criptografia do objeto.



As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em ["Use criptografia do lado do servidor"](#).

Comportamento de GetObject para objetos do Cloud Storage Pool

Se um objeto foi armazenado em um ["Pool de storage em nuvem"](#), o comportamento de uma solicitação GetObject depende do estado do objeto. Veja ["HeadObject"](#) para mais detalhes.



Se um objeto estiver armazenado em um Cloud Storage Pool e uma ou mais cópias do objeto também existirem na grid, as solicitações GetObject tentarão recuperar os dados da grid antes de recuperá-los do Cloud Storage Pool.

Estado do objeto	Comportamento de GetObject
Objeto inserido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento	200 OK Uma cópia do objeto é recuperada.

Estado do objeto	Comportamento de GetObject
Objeto no pool de Cloud Storage, mas ainda não foi transferido para um estado não recuperável	200 OK Uma cópia do objeto é recuperada.
Objeto passou para um estado não recuperável	403 Forbidden, InvalidObjectState Utilize uma solicitação "RestoreObject" para restaurar o objeto a um estado recuperável.
Objeto em processo de restauração a partir de um estado irrecuperável	403 Forbidden, InvalidObjectState Aguarde a conclusão da solicitação RestoreObject.
Objeto totalmente restaurado ao pool de storage em nuvem	200 OK Uma cópia do objeto é recuperada.

Objetos multipartes ou segmentados em um pool de storage em nuvem

Se você carregou um objeto multipart ou se StorageGRID dividiu um objeto grande em segmentos, StorageGRID determina se o objeto está disponível no Cloud Storage Pool ao amostrar um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação GetObject pode retornar incorretamente 200 OK quando algumas partes do objeto já foram transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não foram restauradas.

Nesses casos:

- A solicitação GetObject pode retornar alguns dados, mas ser interrompida no meio da transferência.
- Uma solicitação GetObject subsequente pode retornar 403 Forbidden.

GetObject e replicação entre grades

Se você estiver usando **"federação de grid"** e **"replicação entre grids"** estiver habilitado para um bucket, o cliente pode verificar o status de replicação de um objeto emitindo uma solicitação GetObject. A resposta inclui o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

Grid	Status de replicação
Fonte	• CONCLUÍDO: A replicação foi bem-sucedida. • PENDENTE: O objeto ainda não foi replicado. • FALHA: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	RÉPLICA: O objeto foi replicado da grid de origem.



StorageGRID não suporta o `x-amz-replication-status` header.

Recuperar metadados de um objeto no StorageGRID com a solicitação S3 HeadObject

Você pode usar a solicitação S3 HeadObject para recuperar metadados de um objeto sem retornar o próprio objeto. Se o objeto estiver armazenado em um pool de storage em nuvem, você pode usar HeadObject para determinar o estado de transição do objeto.

HeadObject e objetos multipartes

Você pode usar o `partNumber` parâmetro de solicitação para recuperar metadados de uma parte específica de um objeto multipart ou segmentado. O `x-amz-mp-parts-count` elemento de resposta indica quantas partes o objeto possui.

Você pode definir `partNumber` como 1 tanto para objetos segmentados/multipartes quanto para objetos não segmentados/não multipartes; no entanto, o elemento de resposta `x-amz-mp-parts-count` só é retornado para objetos segmentados ou multipartes.

Caracteres UTF-8 nos metadados do usuário

StorageGRID não analisa nem interpreta caracteres UTF-8 escapados em metadados definidos pelo usuário. Requisições HEAD para um objeto com caracteres UTF-8 escapados em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome da chave ou o valor incluir caracteres não imprimíveis.

Cabeçalho de solicitação compatível

O seguinte cabeçalho de solicitação é compatível:

- `x-amz-checksum-mode`

O `partNumber` parâmetro e o `Range` cabeçalho não são suportados com `x-amz-checksum-mode` para HeadObject. Quando você os inclui na solicitação com `x-amz-checksum-mode` ativado, StorageGRID não retorna um valor de checksum na resposta.

Cabeçalho de solicitação não suportado

O seguinte cabeçalho de solicitação não é compatível e retorna `XNotImplemented`:

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

Controle de versões

Se um `versionId` subrecurso não for especificado, a operação busca a versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, o status "Não encontrado" é retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Cabeçalhos de solicitação para criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Utilize todos os três cabeçalhos se o objeto estiver criptografado com uma chave exclusiva que você forneceu.

- `x-amz-server-side-encryption-customer-algorithm`: Especifique AES256.
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do objeto.



As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em ["Use criptografia do lado do servidor"](#).

HeadObject respostas para objetos do Cloud Storage Pool

Se o objeto estiver armazenado em um ["Pool de storage em nuvem"](#), os seguintes cabeçalhos de resposta serão retornados:

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

Os cabeçalhos de resposta fornecem informações sobre o estado de um objeto à medida que ele é movido para um pool de storage em nuvem, opcionalmente transitado para um estado não recuperável e restaurado.

Estado do objeto	Resposta a HeadObject
Objeto inserido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento	200 OK (Nenhum cabeçalho de resposta especial é retornado.)
Objeto no pool de Cloud Storage, mas ainda não foi transferido para um estado não recuperável	200 OK <code>x-amz-storage-class</code>: GLACIER <code>x-amz-restore</code>: <code>ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Até que o objeto seja levado a um estado irrecuperável, o valor para <code>expiry-date</code> é definido para um momento distante no futuro. O momento exato da transição não é controlado pelo sistema StorageGRID.

Estado do objeto	Resposta a HeadObject
O objeto passou para um estado não recuperável, mas pelo menos uma cópia também existe na grid	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" O valor para expiry-date é definido para um momento distante no futuro. Nota: Se a cópia na grade não estiver disponível (por exemplo, se um Storage Node estiver inativo), você deve emitir uma "RestoreObject" solicitação para restaurar a cópia do Cloud Storage Pool antes de conseguir recuperar o objeto.
O objeto passou para um estado não recuperável e não existe nenhuma cópia no grid	200 OK x-amz-storage-class: GLACIER
Objeto em processo de restauração a partir de um estado irrecuperável	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"
Objeto totalmente restaurado ao pool de storage em nuvem	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" O expiry-date indica quando o objeto no pool de storage em nuvem será retornado a um estado não recuperável.

Objetos multipartes ou segmentados no Cloud Storage Pool

Se você carregou um objeto multipart ou se StorageGRID dividiu um objeto grande em segmentos, StorageGRID determina se o objeto está disponível no Cloud Storage Pool ao amostrar um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação HeadObject pode retornar incorretamente x-amz-restore: ongoing-request="false" quando algumas partes do objeto já foram transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não foram restauradas.

HeadObject e replicação entre grades

Se você estiver usando ["federação de grid"](#) e ["replicação entre grids"](#) estiver habilitado para um bucket, o cliente S3 pode verificar o status de replicação de um objeto emitindo uma solicitação HeadObject. A resposta inclui o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

Grid	Status de replicação
Fonte	• CONCLUÍDO: A replicação foi bem-sucedida. • PENDENTE: O objeto ainda não foi replicado. • FALHA: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	RÉPLICA : O objeto foi replicado da grid de origem.



StorageGRID não suporta o `x-amz-replication-status` header.

Adicionar um objeto a um bucket no StorageGRID com a solicitação S3 PutObject

Você pode usar a solicitação S3 PutObject para adicionar um objeto a um bucket.

Resolver conflitos

Solicitações conflitantes de clientes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio "latest-wins". O momento da avaliação do "latest-wins" é determinado quando o sistema StorageGRID conclui uma determinada solicitação, e não quando os clientes S3 iniciam uma operação.

Tamanho do objeto

O tamanho máximo *recomendado* para uma única operação PutObject é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use ["upload multipart"](#) em vez disso.

O tamanho máximo *suportado* para uma única operação PutObject é de 5 TiB (5.497.558.138.880 bytes).



Se você atualizou do StorageGRID 11.6 ou anterior, o alerta "Tamanho do objeto S3 PUT muito grande" será acionado se você tentar fazer o upload de um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11.7 ou 11.8, o alerta não será acionado nesse caso. No entanto, para alinhar com o padrão AWS S3, as versões futuras do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

Tamanho dos metadados do usuário

Amazon S3 limita o tamanho dos metadados definidos pelo usuário em cada cabeçalho de solicitação PUT a 2 KB. StorageGRID limita os metadados do usuário a 24 KiB. O tamanho dos metadados definidos pelo usuário é medido pela soma do número de bytes na codificação UTF-8 de cada chave e valor.

Caracteres UTF-8 nos metadados do usuário

Se uma solicitação incluir valores UTF-8 (sem escape) no nome da chave ou no valor dos metadados definidos pelo usuário, o comportamento do StorageGRID será indefinido.

StorageGRID não analisa nem interpreta caracteres UTF-8 escapados incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Caracteres UTF-8 escapados são tratados como caracteres ASCII:

- PutObject, CopyObject, GetObject, e HeadObject as solicitações são bem-sucedidas se os metadados definidos pelo usuário incluírem caracteres UTF-8 escapados.
- StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome ou valor da chave incluir caracteres não imprimíveis.

Limites de tags de objeto

Você pode adicionar tags a novos objetos ao carregá-los ou pode adicioná-las a objetos existentes. Tanto StorageGRID quanto Amazon S3 suportam até 10 tags por objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode e os valores de tag podem ter até 256 caracteres Unicode. Chaves e valores diferenciam maiúsculas de minúsculas.

Propriedade do objeto

No StorageGRID, todos os objetos pertencem à conta proprietária do bucket, incluindo objetos criados por uma conta que não seja proprietária ou por um usuário anônimo.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

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

Ao especificar ``aws-chunked`` para `Content-Encoding` StorageGRID, o StorageGRID não verifica os seguintes itens:

- StorageGRID não verifica o `chunk-signature` em relação aos dados em blocos.
- StorageGRID não verifica o valor que você fornece para `x-amz-decoded-content-length` em relação ao objeto.
- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

A codificação de transferência em partes é suportada se `aws-chunked` a assinatura da carga também for

usada.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguido por um par nome-valor contendo metadados definidos pelo usuário.

Ao especificar o par nome-valor para metadados definidos pelo usuário, utilize este formato geral:

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

Se você deseja usar a opção **Hora de criação definida pelo usuário** como a hora de referência para uma regra ILM, você deve usar `creation-time` como o nome do metadado que registra quando o objeto foi criado. Por exemplo:

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

O valor de `creation-time` é avaliado em segundos desde 1º de janeiro de 1970.



Uma regra ILM não pode usar simultaneamente um **horário de criação definido pelo usuário** para o horário de referência e a opção de ingestão balanceada ou estrita. Um erro é retornado quando a regra ILM é criada.

- `x-amz-tagging`
- Cabeçalhos de solicitação de bloqueio de objeto S3
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular o modo de versão do objeto e a data de retenção. Consulte ["Use a API REST S3 para configurar o S3 Object Lock"](#).

- Cabeçalhos de solicitação 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 [Cabeçalhos de solicitação para criptografia do lado do servidor](#)

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `If-Match`

O `If-Match` header é aceito, mas não funcional.

- `If-None-Match`

O `If-None-Match` header é aceito, mas não funcional.

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

O `x-amz-website-redirect-location` cabeçalho retorna ``XNotImplemented`.

Opções de classe de armazenamento

O ``x-amz-storage-class`` cabeçalho da solicitação é compatível. O valor enviado para ``x-amz-storage-class`` afeta como o StorageGRID protege os dados do objeto durante a ingestão e não quantas cópias persistentes do objeto são armazenadas no sistema StorageGRID (o que é determinado pelo ILM).

Se a regra ILM correspondente a um objeto ingerido usar a opção de ingestão estrita, o `x-amz-storage-class` cabeçalho não terá efeito.

Os seguintes valores podem ser usados para `x-amz-storage-class`:

- **STANDARD (Padrão)**
 - **Confirmação dupla:** Se a regra ILM especificar a opção de confirmação dupla para o comportamento de ingestão, assim que um objeto for ingerido, uma segunda cópia desse objeto será criada e distribuída para um nó de armazenamento diferente (confirmação dupla). Quando a ILM é avaliada, o StorageGRID determina se essas cópias intermediárias iniciais atendem às instruções de posicionamento na regra. Se não atenderem, novas cópias do objeto podem precisar ser criadas em locais diferentes e as cópias intermediárias iniciais podem precisar ser excluídas.
 - **Balanceado:** Se a regra ILM especificar a opção Balanceado e StorageGRID não puder criar imediatamente todas as cópias especificadas na regra, StorageGRID faz duas cópias intermediárias em diferentes nós de armazenamento.

Se StorageGRID puder criar imediatamente todas as cópias de objetos especificadas na regra ILM (posicionamento síncrono), o `x-amz-storage-class` cabeçalho não terá efeito.

- **REDUCED_REDUNDANCY**
 - **Confirmação dupla:** Se a regra ILM especificar a opção de confirmação dupla para o comportamento de ingestão, StorageGRID cria uma única cópia intermediária à medida que o objeto é ingerido (confirmação única).
 - **Balanceado:** Se a regra ILM especificar a opção Balanceado, StorageGRID cria uma única cópia intermediária somente se o sistema não puder criar imediatamente todas as cópias especificadas na regra. Se StorageGRID puder realizar o posicionamento síncrono, este cabeçalho não terá efeito. A `REDUCED_REDUNDANCY` opção é mais adequada quando a regra ILM correspondente ao objeto cria uma única cópia replicada. Nesse caso, usar `REDUCED_REDUNDANCY` essa opção elimina a criação e exclusão desnecessárias de uma cópia extra do objeto para cada operação de ingestão.

O uso da `REDUCED_REDUNDANCY` opção não é recomendado em outras circunstâncias. `REDUCED_REDUNDANCY` Isso aumenta o risco de perda de dados de objeto durante a ingestão. Por exemplo, você pode perder dados se a cópia única for armazenada inicialmente em um Storage Node que falhe antes que a avaliação do ILM possa ocorrer.



Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se existir apenas uma cópia replicada de um objeto, esse objeto é perdido se um Storage Node falhar ou apresentar um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como upgrades.

A especificação `REDUCED_REDUNDANCY` afeta apenas quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas ILM ativas e não resulta no armazenamento de dados em níveis mais baixos de redundância no sistema StorageGRID.



Se você estiver ingerindo um objeto em um bucket com S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket legado Compliant, a `REDUCED_REDUNDANCY` opção retornará um erro. StorageGRID sempre realizará uma ingestão com confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Cabeçalhos de solicitação para criptografia do lado do servidor

Você pode usar os seguintes cabeçalhos de solicitação para criptografar um objeto com criptografia do lado do servidor. As opções SSE e SSE-C são mutuamente exclusivas.

- **SSE:** Use o seguinte cabeçalho se você quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID.

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

Quando o `x-amz-server-side-encryption` cabeçalho não está incluído na solicitação PutObject, o ["configuração de criptografia de objeto armazenado"](#) é omitido da resposta PutObject.

- **SSE-C:** Utilize todos os três cabeçalhos se você quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.

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

- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.

- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.



As chaves de criptografia fornecidas por você nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para ["usando criptografia do lado do servidor"](#).



Se um objeto for criptografado com SSE ou SSE-C, quaisquer configurações de criptografia em nível de bucket ou de grid serão ignoradas.

Controle de versões

Se o versionamento estiver habilitado para um bucket, um identificador único `versionId` é gerado automaticamente para a versão do objeto armazenado. Esse `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho da resposta.

Se o versionamento estiver suspenso, a versão do objeto será armazenada com um valor nulo `versionId` e, se já existir uma versão nula, ela será sobrescrita.

Cálculos de assinatura para o cabeçalho Authorization

Ao usar o `Authorization` cabeçalho para autenticar solicitações, StorageGRID difere da AWS das seguintes maneiras:

- StorageGRID não exige que os `host` cabeçalhos sejam incluídos em `CanonicalHeaders`.
- StorageGRID não precisa `Content-Type` ser incluído em `CanonicalHeaders`.
- StorageGRID não exige que os cabeçalhos `x-amz-*` sejam incluídos em `CanonicalHeaders`.



Como prática recomendada geral, sempre inclua esses cabeçalhos dentro de `CanonicalHeaders` para garantir que sejam verificados; no entanto, se você excluir esses cabeçalhos, StorageGRID não retorna um erro.

Para obter detalhes, consulte ["Cálculos de assinatura para o cabeçalho de autorização: transferência de carga em um único bloco \(AWS Signature Version 4\)"](#).

Informações relacionadas

- ["Gerencie objetos com ILM"](#)
- ["Referência da API do Amazon Simple Storage Service: PutObject"](#)

Restaurar um objeto no StorageGRID com a solicitação S3 RestoreObject

Você pode usar a solicitação S3 `RestoreObject` para restaurar um objeto armazenado em um Cloud Storage Pool.

Tipo de solicitação compatível

StorageGRID suporta apenas solicitações `RestoreObject` para restaurar um objeto. Ele não suporta o tipo de restauração `SELECT`. As solicitações `Select` retornam `XNotImplemented`.

Controle de versões

Opcionalmente, especifique `versionId` para restaurar uma versão específica de um objeto em um bucket versionado. Se você não especificar `versionId`, a versão mais recente do objeto é restaurada.

Comportamento de RestoreObject em objetos do Cloud Storage Pool

Se um objeto foi armazenado em um ["Pool de storage em nuvem"](#), uma solicitação `RestoreObject` terá o seguinte comportamento, com base no estado do objeto. Veja ["HeadObject"](#) para mais detalhes.



Se um objeto estiver armazenado em um Cloud Storage Pool e uma ou mais cópias desse objeto também existirem na grid, não é necessário restaurar o objeto emitindo uma solicitação `RestoreObject`. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação `GetObject`.

Estado do objeto	Comportamento de <code>RestoreObject</code>
Objeto ingerido no <code>StorageGRID</code> , mas ainda não avaliado pelo ILM, ou objeto não está em um Cloud Storage Pool	403 Forbidden, InvalidObjectState
Objeto no pool de Cloud Storage, mas ainda não foi transferido para um estado não recuperável	<code>200 OK</code> Nenhuma alteração foi feita. Nota: Antes que um objeto tenha sido transferido para um estado não recuperável, você não pode alterar seu <code>expiry-date</code> .
Objeto passou para um estado não recuperável	<code>202 Accepted</code> Restaura uma cópia recuperável do objeto no Cloud Storage Pool pelo número de dias especificado no corpo da solicitação. Ao final desse período, o objeto retorna a um estado não recuperável. Opcionalmente, use o <code>Tier</code> elemento de solicitação para determinar quanto tempo a tarefa de restauração levará para ser concluída (<code>Expedited</code> , <code>Standard</code> , ou <code>Bulk</code>). Se você não especificar <code>Tier</code> , o <code>Standard</code> nível será usado. Importante: Se um objeto tiver sido migrado para o S3 Glacier Deep Archive ou se o Cloud Storage Pool usar Azure Blob storage, você não poderá restaurá-lo usando a <code>Expedited</code> camada. O seguinte erro é retornado 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.
Objeto em processo de restauração a partir de um estado irrecuperável	409 Conflict, RestoreAlreadyInProgress
Objeto totalmente restaurado ao pool de storage em nuvem	200 OK Nota: Se um objeto foi restaurado a um estado recuperável, você pode alterar seu <code>expiry-date</code> reenviando a solicitação <code>RestoreObject</code> com um novo valor para <code>Days</code> . A data de restauração é atualizada em relação ao momento da solicitação.

Filtrar dados de objetos no `StorageGRID` com a solicitação `S3 SelectObjectContent`

Você pode usar a solicitação `S3 SelectObjectContent` para filtrar o conteúdo de um objeto S3 com base em uma instrução SQL simples.

Para obter mais informações, consulte ["Referência da API do Amazon Simple Storage Service: SelectObjectContent"](#).

Antes de começar

- A conta do locatário possui a permissão S3 Select.
- Você tem `s3:GetObject` permissão para o objeto que você deseja consultar.
- O objeto que você deseja consultar deve estar em um dos seguintes formatos:
 - **CSV**. Pode ser usado como está ou compactado em arquivos GZIP ou BZIP2.
 - **Parquet**. Requisitos adicionais para objetos Parquet:
 - O S3 Select suporta apenas compressão colunar usando GZIP ou Snappy. O S3 Select não suporta compressão de objeto inteiro para objetos Parquet.
 - O S3 Select não suporta saída em Parquet. Você deve especificar o formato de saída como CSV ou JSON.
 - O tamanho máximo de um grupo de linhas não compactadas é de 512 MB.
 - Você deve usar os tipos de dados especificados no esquema do objeto.
 - Não é possível usar os tipos lógicos INTERVAL, JSON, LIST, TIME ou UUID.
- Sua expressão SQL tem um comprimento máximo de 256 KB.
- Qualquer registro na entrada ou nos resultados tem um comprimento máximo de 1 MiB.

Exemplo de sintaxe de solicitação 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>

```

Exemplo de sintaxe de solicitação 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>

```

Exemplo de consulta SQL

Esta consulta obtém o nome do estado, a população em 2010, a população estimada para 2015 e a porcentagem de variação a partir de dados do censo dos EUA. Registros no arquivo que não são estados são ignorados.

```

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

```

As primeiras linhas do arquivo a ser consultado, SUB-EST2020_ALL.csv são semelhantes a estas:

```
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
```

Exemplo de uso do 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
```

As primeiras linhas do arquivo de saída, `changes.csv`, têm a seguinte aparência:

```
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
```

Exemplo de uso da 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
```

As primeiras linhas do arquivo de saída, changes.csv, têm a seguinte aparência:

```
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
```

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.