



# **Operações em objetos**

## **StorageGRID**

NetApp

October 03, 2025

# Índice

|  |    |
|--|----|
| Operações em objetos   | 1  |
| Usando S3 Object Lock  | 6  |
| Ativar o bloqueio de objetos S3D para um balde   | 6  |
| Determinar se o bloqueio de objeto S3 está ativado para um bucket  | 6  |
| Criando um objeto com S3 configurações de bloqueio de objeto   | 6  |
| A atualizar as definições de bloqueio de objetos do S3   | 7  |
| Usando criptografia do lado do servidor  | 8  |
| Usando SSE   | 9  |
| Usando SSE-C   | 9  |
| Considerações sobre o uso de criptografia no lado do servidor com chaves fornecidas pelo cliente (SSE-C)                   | 9  |
| Objeto GET   | 10 |
| O parâmetro pedido de número de peça não é suportado   | 10 |
| Cabeçalhos de solicitação para criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C) | 11 |
| UTF-8 caracteres em metadados do usuário   | 11 |
| Cabeçalho de pedido não suportado  | 11 |
| Controle de versão   | 11 |
| Comportamento DO GET Object para objetos Pool de storage de nuvem  | 11 |
| Objetos segmentados ou multiparte em um pool de armazenamento em nuvem   | 12 |
| Objeto HEAD  | 12 |
| Cabeçalhos de solicitação para criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C) | 13 |
| UTF-8 caracteres em metadados do usuário   | 13 |
| Cabeçalho de pedido não suportado  | 13 |
| Cabeçalhos de resposta para objetos Pool de armazenamento em nuvem   | 13 |
| Objetos segmentados ou multiparte em um pool de armazenamento em nuvem   | 15 |
| Controle de versão   | 15 |
| Restauração PÓS-objeto   | 15 |
| Tipo de solicitação suportada  | 15 |
| Controle de versão   | 16 |
| Comportamento da restauração PÓS-objeto em objetos do Cloud Storage Pool   | 16 |
| Objeto PUT   | 17 |
| Resolução de conflitos   | 17 |
| Tamanho do objeto  | 17 |
| Tamanho dos metadados do usuário   | 17 |
| UTF-8 caracteres em metadados do usuário   | 17 |
| Limites da etiqueta do objeto  | 18 |
| Propriedade do objeto  | 18 |
| Cabeçalhos de solicitação suportados   | 18 |
| Cabeçalhos de solicitação não suportados   | 19 |
| Opções de classe de armazenamento  | 19 |
| Cabeçalhos de solicitação para criptografia do lado do servidor  | 20 |

|   |    |
|---|----|
| Controle de versão .....  | 21 |
| COLOCAR Objeto - Copiar .....   | 21 |
| Resolução de conflitos .....  | 21 |
| Tamanho do objeto .....   | 22 |
| UTF-8 caracteres em metadados do usuário .....                        | 22 |
| Cabeçalhos de solicitação suportados .....                            | 22 |
| Cabeçalhos de solicitação não suportados .....                        | 23 |
| Opções de classe de armazenamento .....                               | 23 |
| Usando x-amz-copy-source em PUT Object - Copy .....                   | 24 |
| Cabeçalhos de solicitação para criptografia do lado do servidor ..... | 24 |
| Controle de versão .....  | 25 |

# Operações em objetos

Esta seção descreve como o sistema StorageGRID implementa S3 operações de API REST para objetos.

- "Usando S3 Object Lock"
- "Usando criptografia do lado do servver"
- "Objeto GET"
- "Objeto HEAD"
- "Restauração PÓS-objeto"
- "Objeto PUT"
- "COLOCAR Objeto - Copiar"

As seguintes condições se aplicam a todas as operações de objetos:

- Os controles de consistência do StorageGRID são suportados por todas as operações em objetos, com exceção do seguinte:
  - OBTER ACL Objeto
  - OPTIONS /
  - COLOCAR guarda legal Objeto
  - COLOCAR retenção Objeto
- As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.
- Todos os objetos em um bucket do StorageGRID são de propriedade do proprietário do bucket, incluindo objetos criados por um usuário anônimo ou por outra conta.
- Os objetos de dados ingeridos para o sistema StorageGRID através do Swift não podem ser acedidos através do S3.

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

| Operação               | Implementação  |
|------------------------|--|
| Objeto DELETE          | <p data-bbox="818 155 1479 226">Autenticação multifator (MFA) e o cabeçalho de resposta <code>x-amz-mfa</code> não são suportados.</p> <p data-bbox="818 260 1479 604">Ao processar uma solicitação DE EXCLUSÃO de objetos, o StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais armazenados. Se for bem-sucedido, o StorageGRID retornará uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas dentro de 30 segundos (por exemplo, porque um local está temporariamente indisponível), o StorageGRID coloca as cópias em fila para remoção e, em seguida, indica sucesso para o cliente.</p> <p data-bbox="818 638 1070 667"><b>Controle de versão</b></p> <p data-bbox="818 701 1479 945">Para remover uma versão específica, o solicitante deve ser o proprietário do bucket e usar o <code>versionId</code> subrecurso. O uso deste subrecurso 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> será retornado como <code>true</code>.</p> <ul data-bbox="844 978 1479 1528" style="list-style-type: none"> <li>• Se um objeto for excluído sem o <code>versionId</code> subrecurso em um bucket habilitado para versão, isso resultará na geração de um marcador de exclusão. O <code>versionId</code> para o 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 como <code>true</code>.</li> <li>• Se um objeto for excluído sem o <code>versionId</code> subrecurso em um bucket suspenso de versão, ele resultará em uma exclusão permanente de uma versão 'null' já existente ou um marcador 'null' delete, e a geração de um novo marcador 'null' delete. O <code>x-amz-delete-marker</code> cabeçalho de resposta é retornado definido como <code>true</code>.</li> </ul> <p data-bbox="818 1562 1479 1633"><b>Nota:</b> Em certos casos, vários marcadores de exclusão podem existir para um objeto.</p> |
| Excluir vários objetos | <p data-bbox="818 1682 1479 1753">Autenticação multifator (MFA) e o cabeçalho de resposta <code>x-amz-mfa</code> não são suportados.</p> <p data-bbox="818 1787 1479 1858">Vários objetos podem ser excluídos na mesma mensagem de solicitação.</p>  |

| Operação                    | Implementação   |
|-----------------------------|---|
| ELIMINAR marcação Objeto    | <p>Usa o <code>tagging</code> subrecurso para remover todas as tags de um objeto. Implementado com todo o comportamento da API REST do Amazon S3.</p> <p><b>Controle de versão</b></p> <p>Se o <code>versionId</code> parâmetro de consulta não for especificado na solicitação, a operação excluirá todas as tags da versão mais recente do objeto em um bucket com versão. Se a versão atual do objeto for um marcador de exclusão, um status <code>"MethodNotAllowed"</code> será retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.</p>    |
| Objeto GET                  | "Objeto GET"  |
| OBTER ACL Objeto            | Se as credenciais de acesso necessárias forem fornecidas para a conta, a operação retornará uma resposta positiva e a ID, DisplayName e permissão do proprietário do objeto, indicando que o proprietário tem acesso total ao objeto.   |
| OBTER retenção legal Objeto | "Usando S3 Object Lock"   |
| OBTER retenção de objetos   | "Usando S3 Object Lock"   |
| OBTER marcação de objetos   | <p>Usa o <code>tagging</code> subrecurso para retornar todas as tags para um objeto. Implementado com todo o comportamento da API REST do Amazon S3</p> <p><b>Controle de versão</b></p> <p>Se o <code>versionId</code> parâmetro de consulta não for especificado na solicitação, a operação retornará 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 <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.</p> |
| Objeto HEAD                 | "Objeto HEAD"   |
| Restauração PÓS-objeto      | "Restauração PÓS-objeto"  |
| Objeto PUT                  | "Objeto PUT"  |

| Operação                    | Implementação             |
|-----------------------------|---------------------------|
| COLOCAR Objeto - Copiar     | "COLOCAR Objeto - Copiar" |
| COLOCAR guarda legal Objeto | "Usando S3 Object Lock"   |
| COLOCAR retenção Objeto     | "Usando S3 Object Lock"   |

| Operação                  | Implementação  |
|---------------------------|--|
| COLOQUE a marcação Objeto | <p data-bbox="815 157 1484 294">Usa o <code>tagging</code> subrecurso para adicionar um conjunto de tags a um objeto existente. Implementado com todo o comportamento da API REST do Amazon S3</p> <p data-bbox="815 325 1484 394"><b>Atualizações de tags e comportamento de ingestão</b></p> <p data-bbox="815 426 1484 735">Quando você usa a marcação "COLOCAR objeto" para atualizar as tags de um objeto, o StorageGRID não reingere o objeto. Isso significa que a opção de comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento de objetos que são acionadas pela atualização são feitas quando o ILM é reavaliado por processos normais de ILM em segundo plano.</p> <p data-bbox="815 766 1484 1039">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-exigido não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível.</p> <p data-bbox="815 1071 1484 1102"><b>Resolução de conflitos</b></p> <p data-bbox="815 1134 1484 1375">As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.</p> <p data-bbox="815 1407 1484 1438"><b>Controle de versão</b></p> <p data-bbox="815 1470 1484 1753">Se o <code>versionId</code> parâmetro de consulta não for especificado na solicitação, a operação adicionará tags à versão mais recente do objeto em um bucket com versão. Se a versão atual do objeto for um marcador de exclusão, um status <code>"MethodNotAllowed"</code> será retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.</p> |

## Informações relacionadas

["Controles de consistência"](#)



## Usando S3 Object Lock

Se a configuração global de bloqueio de objetos S3 estiver ativada para o seu sistema StorageGRID, você poderá criar buckets com o bloqueio de objetos S3 ativado e, em seguida, especificar as configurações de retenção legal e de retenção para cada versão de objeto adicionada a esse bucket.

O bloqueio de objetos S3 permite especificar configurações no nível do objeto para impedir que objetos sejam excluídos ou substituídos por um período fixo de tempo ou indefinidamente.

O recurso bloqueio de objetos do StorageGRID S3 fornece um modo de retenção único equivalente ao modo de conformidade do Amazon S3. Por padrão, uma versão de objeto protegido não pode ser substituída ou excluída por nenhum usuário. O recurso bloqueio de objetos do StorageGRID S3 não suporta um modo de governança e não permite que usuários com permissões especiais ignorem as configurações de retenção ou excluam objetos protegidos.

### Ativar o bloqueio de objetos S3D para um balde

Se a configuração global de bloqueio de objetos S3 estiver ativada para o seu sistema StorageGRID, você poderá ativar opcionalmente o bloqueio de objetos S3 quando criar cada bucket. Você pode usar qualquer um destes métodos:

- Crie o bucket usando o Gerenciador do locatário.

"Use uma conta de locatário"

- Crie o bucket usando uma solicitação DE COLOCAR balde com o `x-amz-bucket-object-lock_enabled` cabeçalho de solicitação.

"Operações em baldes"

Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação do bucket. O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.

Um bucket com S3 Object Lock ativado pode conter uma combinação de objetos com e sem configurações de bloqueio de objeto S3. O StorageGRID não suporta retenção padrão para os objetos nos buckets do bloqueio de objetos do S3, portanto, a operação do bucket Configuração do bloqueio de objetos do PUT não é suportada.

### Determinar se o bloqueio de objeto S3 está ativado para um bucket

Para determinar se o bloqueio de objeto S3 está ativado, use a solicitação DE configuração OBTER bloqueio de objeto.

"Operações em baldes"

### Criando um objeto com S3 configurações de bloqueio de objeto

Para especificar as configurações de bloqueio de objeto S3 ao adicionar uma versão de objeto a um intervalo que tenha o bloqueio de objeto S3 ativado, emita um Objeto PUT, COLOCAR Objeto - Copiar ou inicie uma

solicitação de upload de várias partes. Use os cabeçalhos de solicitação a seguir.



Você deve habilitar o bloqueio de objeto S3 quando criar um bucket. Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação de um intervalo.

- `x-amz-object-lock-mode`, Que deve ser CONFORMIDADE (sensível a maiúsculas e minúsculas).



Se você especificar `x-amz-object-lock-mode`, você também deve especificar `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - O valor `reter-até-data` deve estar no formato `2020-08-10T21:46:00Z`. Segundos fracionários são permitidos, mas apenas 3 dígitos decimais são preservados (precisão de milissegundos). Outros formatos ISO 8601 não são permitidos.
  - A data de retenção deve ser no futuro.
- `x-amz-object-lock-legal-hold`

Se a retenção legal estiver ATIVADA (sensível a maiúsculas e minúsculas), o objeto é colocado sob uma retenção legal. Se a retenção legal estiver DESLIGADA, nenhuma retenção legal será colocada. Qualquer outro valor resulta em um erro de 400 Bad Request (InvalidArgument).

Se você usar qualquer um desses cabeçalhos de solicitação, esteja ciente dessas restrições:

- O `Content-MD5` cabeçalho de solicitação é necessário se qualquer `x-amz-object-lock-*` cabeçalho de solicitação estiver presente na solicitação DE Objeto PUT. `Content-MD5` Não é necessário para COLOCAR Objeto - Copiar ou iniciar carregamento Multipart.
- Se o bucket não tiver o bloqueio de objeto S3 ativado e um `x-amz-object-lock-*` cabeçalho de solicitação estiver presente, um erro de solicitação incorreta 400 (InvalidRequest) será retornado.
- A solicitação put Object suporta o uso do `x-amz-storage-class: REDUCED_REDUNDANCY` para corresponder ao comportamento da AWS. No entanto, quando um objeto é ingerido em um bucket com o bloqueio de objeto S3 ativado, o StorageGRID sempre realizará uma ingestão de confirmação dupla.
- Uma resposta DE versão DE GET ou HEAD Object posterior incluirá os cabeçalhos `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e `x-amz-object-lock-legal-hold`, se configurado e se o remetente da solicitação tiver as permissões corretas `s3:Get*`.
- Uma solicitação DE versão DE EXCLUSÃO de objeto subsequente ou versões de EXCLUSÃO de objetos falhará se for antes da data de retenção ou se uma retenção legal estiver ativada.

## A atualizar as definições de bloqueio de objetos do S3

Se você precisar atualizar as configurações de retenção legal ou retenção para uma versão de objeto existente, poderá executar as seguintes operações de subrecursos de objeto:

- `PUT Object legal-hold`

Se o novo valor de retenção legal estiver ATIVADO, o objeto será colocado sob uma retenção legal. Se o valor de retenção legal estiver DESLIGADO, a retenção legal é levantada.

- `PUT Object retention`

- O valor do modo deve ser CONFORMIDADE (sensível a maiúsculas e minúsculas).
- O valor reter-até-data deve estar no formato 2020-08-10T21:46:00Z. Segundos fracionários são permitidos, mas apenas 3 dígitos decimais são preservados (precisão de milissegundos). Outros formatos ISO 8601 não são permitidos.
- Se uma versão de objeto tiver uma data retida-até-data existente, você só poderá aumentá-la. O novo valor deve estar no futuro.

#### Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Use uma conta de locatário"](#)

["Objeto PUT"](#)

["COLOCAR Objeto - Copiar"](#)

["Inicie o carregamento de várias peças"](#)

["Controle de versão de objetos"](#)

["Guia do usuário do Amazon Simple Storage Service: Usando o bloqueio de objeto S3"](#)

## Usando criptografia do lado do servidor

A criptografia do lado do servidor permite proteger os dados do objeto em repouso. O StorageGRID criptografa os dados enquanto grava o objeto e descriptografa os dados quando você acessa o objeto.

Se você quiser usar a criptografia do lado do servidor, você 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 emite uma solicitação S3 para armazenar um objeto, o StorageGRID criptografa o objeto com uma chave exclusiva. Quando você emite uma solicitação S3 para recuperar o objeto, o StorageGRID usa a chave armazenada para descriptografar o objeto.
- **SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente):** Quando você emite uma solicitação S3 para armazenar um objeto, você fornece sua própria chave de criptografia. Quando você recupera um objeto, você fornece a mesma chave de criptografia como parte de sua solicitação. Se as duas chaves de criptografia corresponderem, o objeto será descriptografado e seus dados de objeto serão retornados.

Enquanto o StorageGRID gerencia todas as operações de criptografia e descriptografia de objetos, você deve gerenciar as chaves de criptografia fornecidas.



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 no nível de bucket ou no nível de grade serão ignoradas.

## Usando SSE

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

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

O cabeçalho de solicitação SSE é suportado pelas seguintes operações de objeto:

- Objeto PUT
- COLOCAR Objeto - Copiar
- Inicie o carregamento de várias peças

## Usando SSE-C

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

| Cabeçalho da solicitação                        | Descrição  |
|---|--|
| x-amz-server-side-encryption-customer-algorithm | Especifique o algoritmo de criptografia. O valor da plataforma 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 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 usada para garantir que a chave de criptografia foi transmitida sem erros. O valor para o resumo MD5 deve ser base64-codificado 128-bit. |

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

- Objeto GET
- Objeto HEAD
- Objeto PUT
- COLOCAR Objeto - Copiar
- Inicie o carregamento de várias peças
- Carregar artigo
- Carregar artigo - Copiar

## Considerações sobre o uso de criptografia no lado do servidor com chaves fornecidas pelo cliente (SSE-C)

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

- Você deve usar https.



O StorageGRID rejeita quaisquer solicitações feitas por http ao usar SSE-C. para considerações de segurança, você deve considerar qualquer chave que você enviar acidentalmente usando http para ser comprometida. Elimine a chave e rode-a conforme adequado.

- O ETag na resposta não é o MD5 dos dados do objeto.
- É necessário gerenciar o mapeamento de chaves de criptografia para objetos. O StorageGRID não armazena chaves de criptografia. Você é responsável por rastrear a chave de criptografia fornecida para cada objeto.
- Se seu bucket estiver habilitado para versionamento, cada versão do objeto deve ter sua própria chave de criptografia. Você é responsável por rastrear a chave de criptografia usada para cada versão do objeto.
- Como você gerencia chaves de criptografia no lado do cliente, você também deve gerenciar quaisquer proteções adicionais, como 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 do CloudMirror estiver configurada para o bucket, você não poderá ingerir objetos SSE-C. A operação de ingestão falhará.

#### Informações relacionadas

["Objeto GET"](#)

["Objeto HEAD"](#)

["Objeto PUT"](#)

["COLOCAR Objeto - Copiar"](#)

["Inicie o carregamento de várias peças"](#)

["Carregar artigo"](#)

["Carregar artigo - Copiar"](#)

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

## Objeto GET

Você pode usar a solicitação S3 GET Object para recuperar um objeto de um bucket do S3.

### O parâmetro pedido de número de peça não é suportado

O `partNumber` parâmetro Request não é suportado para OBTER solicitações Objeto. Não é possível executar uma SOLICITAÇÃO GET para recuperar uma parte específica de um objeto multipart. Um erro 501 não implementado é retornado com a seguinte mensagem:

GET Object by partNumber is not implemented

## Cabeçalhos de solicitação para criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use todos os três cabeçalhos se o objeto for 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 os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

## UTF-8 caracteres em metadados do usuário

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

## Cabeçalho de pedido não suportado

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

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

## Controle de versão

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

## Comportamento DO GET Object para objetos Pool de storage de nuvem

Se um objeto tiver sido armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), o comportamento de uma SOLICITAÇÃO GET Object depende do estado do objeto. Consulte "Objeto PRINCIPAL" para obter mais detalhes.



Se um objeto for armazenado em um pool de armazenamento em nuvem e uma ou mais cópias do objeto também existirem na grade, as SOLICITAÇÕES DE OBTENÇÃO de objetos tentarão recuperar dados da grade, antes de recuperá-los do pool de armazenamento em nuvem.

| Estado do objeto  | Comportamento de GET Object  |
|---|--|
| Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento | 200 OK<br><br>Uma cópia do objeto é recuperada.  |
| Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável  | 200 OK<br><br>Uma cópia do objeto é recuperada.  |
| Objeto transicionado para um estado não recuperável   | 403 Forbidden, InvalidObjectState<br><br>Use uma solicitação de restauração PÓS-objeto para restaurar o objeto para um estado recuperável. |
| Objeto em processo de restauração a partir de um estado não recuperável   | 403 Forbidden, InvalidObjectState<br><br>Aguarde até que a solicitação de restauração PÓS-objeto seja concluída.                           |
| Objeto totalmente restaurado para o Cloud Storage Pool  | 200 OK<br><br>Uma cópia do objeto é recuperada.  |

## Objetos segmentados ou multiparte em um pool de armazenamento em nuvem

Se você carregou um objeto multipart ou se o StorageGRID dividir um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no pool de armazenamento em nuvem amostrando um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação GET Object pode retornar incorretamente 200 OK quando algumas partes do objeto já tiverem sido transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não tiverem sido restauradas.

Nestes casos:

- A solicitação GET Object pode retornar alguns dados, mas parar no meio da transferência.
- Uma solicitação OBTER Objeto subsequente pode retornar 403 Forbidden.

### Informações relacionadas

["Usando criptografia do lado do servidor"](#)

["Gerenciar objetos com ILM"](#)

["Restauração PÓS-objeto"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

## Objeto HEAD

Você pode usar a solicitação de Objeto S3 HEAD para recuperar metadados de um

objeto sem retornar o próprio objeto. Se o objeto for armazenado em um pool de armazenamento em nuvem, você poderá usar Objeto HEAD para determinar o estado de transição do objeto.

## Cabeçalhos de solicitação para criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use os três cabeçalhos se o objeto for 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 os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

## UTF-8 caracteres em metadados do usuário

O StorageGRID não analisa nem interpreta caracteres UTF-8 escapados em metadados definidos pelo usuário. As SOLICITAÇÕES 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 ou valor da chave incluir caracteres não imprimíveis.

## Cabeçalho de pedido não suportado

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

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

## Cabeçalhos de resposta para objetos Pool de armazenamento em nuvem

Se o objeto for armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), 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 armazenamento em nuvem, opcionalmente transferido para um estado não recuperável e restaurado.



| Estado do objeto  | Resposta ao objeto PRINCIPAL  |
|---|---|
| Objeto ingerido 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 Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável  | <p>200 OK</p> <p><code>x-amz-storage-class: GLACIER</code></p> <p><code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code></p> <p>Até que o objeto seja transferido para um estado não recuperável, o valor para <code>expiry-date</code> é definido para algum tempo distante no futuro. A hora exata da transição não é controlada pelo sistema StorageGRID.</p>  |
| O objeto fez a transição para o estado não recuperável, mas pelo menos uma cópia também existe na grade   | <p>200 OK</p> <p><code>x-amz-storage-class: GLACIER</code></p> <p><code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code></p> <p>O valor para <code>expiry-date</code> é definido para algum tempo distante no futuro.</p> <p><b>Nota:</b> Se a cópia na grade não estiver disponível (por exemplo, um nó de armazenamento está inativo), você deve emitir uma solicitação de restauração PÓS-Objeto para restaurar a cópia do pool de armazenamento em nuvem antes de recuperar o objeto com êxito.</p> |
| Objeto transicionado para um estado não recuperável e nenhuma cópia existe na grade   | <p>200 OK</p> <p><code>x-amz-storage-class: GLACIER</code></p>  |
| Objeto em processo de restauração a partir de um estado não recuperável   | <p>200 OK</p> <p><code>x-amz-storage-class: GLACIER</code></p> <p><code>x-amz-restore: ongoing-request="true"</code></p>  |

| Estado do objeto                                       | Resposta ao objeto PRINCIPAL  |
|--|---|
| Objeto totalmente restaurado para o Cloud Storage Pool | <p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 2018 00:00:00 GMT"</p> <p>O expiry-date indica quando o objeto no pool de armazenamento em nuvem será retornado a um estado não recuperável.</p> |

## Objetos segmentados ou multiparte em um pool de armazenamento em nuvem

Se você carregou um objeto multipart ou se o StorageGRID dividir um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no pool de armazenamento em nuvem amostrando um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação de objeto PRINCIPAL pode retornar incorretamente `x-amz-restore: ongoing-request="false"` quando algumas partes do objeto já tiverem sido transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não tiverem sido restauradas.

## Controle de versão

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

### Informações relacionadas

["Usando criptografia do lado do servidor"](#)

["Gerenciar objetos com ILM"](#)

["Restauração PÓS-objeto"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

## Restauração PÓS-objeto

Você pode usar a solicitação de restauração PÓS-objeto S3 para restaurar um objeto armazenado em um pool de storage de nuvem.

### Tipo de solicitação suportada

O StorageGRID suporta apenas solicitações de restauração PÓS-objeto para restaurar um objeto. Não suporta o `SELECT` tipo de restauração. Selecione `Requests Return` (retornar solicitações `XNotImplemented`).

## Controle de versão

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

## Comportamento da restauração PÓS-objeto em objetos do Cloud Storage Pool

Se um objeto tiver sido armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), uma solicitação de restauração PÓS-objeto terá o seguinte comportamento, com base no estado do objeto. Consulte "Objeto PRINCIPAL" para obter mais detalhes.



Se um objeto for armazenado em um pool de armazenamento em nuvem e uma ou mais cópias do objeto também existirem na grade, não será necessário restaurar o objeto emitindo uma solicitação de restauração PÓS-objeto. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma SOLICITAÇÃO GET Object.

| Estado do objeto   | Comportamento da restauração PÓS-objeto   |
|--|---|
| Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto não está em um pool de storage de nuvem | 403 Forbidden, InvalidObjectState   |
| Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável                           | 200 OK Nenhuma alteração é feita.<br><br><b>Nota:</b> Antes de um objeto ser transferido para um estado não recuperável, não é possível alterar o seu <code>expiry-date</code> .  |
| Objeto transicionado para um estado não recuperável  | 202 Accepted Restaura uma cópia recuperável do objeto para o pool de armazenamento em nuvem pelo número de dias especificado no corpo da solicitação. No final desse período, o objeto é retornado a um estado não recuperável.<br><br>Opcionalmente, use o <code>Tier</code> elemento de solicitação para determinar quanto tempo o trabalho de restauração levará para concluir ( <code>Expedited</code> , <code>Standard</code> ou <code>Bulk</code> ). Se você não especificar <code>Tier</code> , o <code>Standard</code> nível será usado.<br><br><b>Atenção:</b> Se um objeto tiver sido transferido para o S3 Glacier Deep Archive ou se o Cloud Storage Pool usar o armazenamento Blob do Azure, não será possível restaurá-lo usando o <code>Expedited</code> nível. O seguinte erro é retornado 403 Forbidden, <code>InvalidTier: Retrieval option is not supported by this storage class</code> . |
| Objeto em processo de restauração a partir de um estado não recuperável  | 409 Conflict, RestoreAlreadyInProgress  |

| Estado do objeto                                       | Comportamento da restauração PÓS-objeto  |
|--|--|
| Objeto totalmente restaurado para o Cloud Storage Pool | 200 OK<br><br><b>Observação:</b> se um objeto foi restaurado para um estado recuperável, você pode alterar o mesmo <code>expiry-date</code> reemitindo a solicitação de restauração PÓS-objeto com um novo valor para <code>Days</code> . A data de restauração é atualizada em relação à hora da solicitação. |

#### Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Objeto HEAD"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

## Objeto PUT

Você pode usar a solicitação de objetos S3D PUT para adicionar um objeto a um bucket.

### Resolução de conflitos

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

### Tamanho do objeto

O StorageGRID suporta objetos de até 5 TB de tamanho.

### Tamanho dos metadados do usuário

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

### UTF-8 caracteres em metadados do usuário

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

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

- As solicitações PUT, PUT Object-Copy, GET e HEAD são bem-sucedidas se os metadados definidos pelo usuário incluírem caracteres UTF-8 escapados.

- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome ou valor da chave incluir caracteres não imprimíveis.

## Limites da etiqueta do objeto

Você pode adicionar tags a novos objetos ao enviá-los ou adicioná-los a objetos existentes. O StorageGRID e o Amazon S3 suportam até 10 tags para cada objeto. Tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento e os valores de tag podem ter até 256 caracteres Unicode de comprimento. Chave e valores são sensíveis a maiúsculas e minúsculas.

## Propriedade do objeto

No StorageGRID, todos os objetos são de propriedade da conta de proprietário do bucket, incluindo objetos criados por uma conta não proprietária ou um usuário anônimo.

## Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

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

Quando você especifica `aws-chunked` para `Content-Encoding` StorageGRID não verifica os seguintes itens:

- O StorageGRID não verifica o `chunk-signature` contra os dados de bloco.
- O StorageGRID não verifica o valor que você fornece `x-amz-decoded-content-length` em relação ao objeto.

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

A codificação de transferência Chunked é suportada se `aws-chunked` a assinatura de payload também for usada.

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

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

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

Se você quiser usar a opção **tempo de criação definido pelo usuário** como tempo de referência para

uma regra ILM, você deve usar `creation-time` como o nome dos metadados que Registram quando o objeto foi criado. Por exemplo:

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

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



Uma regra ILM não pode usar um **tempo de criação definido pelo usuário** para o tempo de referência e as opções balanceadas ou rigorosas para o comportamento de ingestão. Um erro é retornado quando a regra ILM é criada.

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

### "Usando S3 Object Lock"

- Cabeçalhos de pedido 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`

### "S3 operações e limitações suportadas pela API REST"

## Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- O `x-amz-acl` cabeçalho da solicitação não é suportado.
- O `x-amz-website-redirect-location` cabeçalho da solicitação não é suportado e retorna `XNotImplemented`.

## Opções de classe de armazenamento

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

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

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

- **STANDARD (Predefinição)**

- **\* Commit duplo\***: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, assim que um objeto é ingerido, uma segunda cópia desse objeto é criada e distribuída para um nó de armazenamento diferente (commit duplo). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais satisfazem as instruções de colocação na regra. Caso contrário, novas cópias de objetos podem precisar ser feitas em locais diferentes e as cópias provisórias iniciais podem precisar ser excluídas.
- **Balanced**: Se a regra ILM especificar a opção Balanced e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em nós de storage diferentes.

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

- **REDUCED\_REDUNDANCY**

- **Commit duplo**: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, o StorageGRID cria uma única cópia provisória à medida que o objeto é ingerido (commit único).
- **Balanced**: Se a regra ILM especificar a opção Balanced, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito. A `REDUCED_REDUNDANCY` opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso, o uso `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia de objeto extra para cada operação de ingestão.

A utilização da `REDUCED_REDUNDANCY` opção não é recomendada noutras circunstâncias.

`REDUCED_REDUNDANCY` aumenta o risco de perda de dados do objeto durante a ingestão. Por exemplo, você pode perder dados se a única cópia for inicialmente armazenada em um nó de armazenamento que falha antes que a avaliação ILM possa ocorrer.

**Atenção:** Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Especificar `REDUCED_REDUNDANCY` apenas afeta quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Ele não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pela política ILM ativa e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

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

## Cabeçalhos de solicitação para criptografia do lado do servidor

Você pode usar os cabeçalhos de solicitação a seguir 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 quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID.

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

- **SSE-C:** Use 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`: Especificar 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.

**Atenção:** 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 os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

**Nota:** Se um objeto for criptografado com SSE ou SSE-C, qualquer configuração de criptografia em nível de bucket ou em nível de grade será ignorada.

## Controle de versão

Se o controle de versão estiver habilitado para um bucket, um exclusivo `versionId` será gerado automaticamente para a versão do objeto que está sendo armazenado. Isso `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho de resposta.

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

### Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Operações em baldes"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

["Usando criptografia do lado do servidor"](#)

["Como as conexões do cliente podem ser configuradas"](#)

## COLOCAR Objeto - Copiar

Você pode usar a solicitação S3 PUT Object - Copy para criar uma cópia de um objeto que já está armazenado no S3. Uma operação PUT Object - Copy é a mesma que executar um GET e depois um PUT.

## Resolução de conflitos

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.



## Tamanho do objeto

O StorageGRID suporta objetos de até 5 TB de tamanho.

## UTF-8 caracteres em metadados do usuário

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

O StorageGRID não analisa nem interpreta caracteres UTF-8 escapados incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Os 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.
- O 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 de nome-valor contendo metadados definidos pelo usuário
- `x-amz-metadata-directive`: O valor padrão é `COPY`, que permite copiar o objeto e os metadados associados.

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

- S3 cabeçalhos de solicitação de bloqueio de objetos:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

## "Usando S3 Object Lock"

- Cabeçalhos de pedido 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

"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
- x-amz-website-redirect-location

## Opções de classe de armazenamento

O `x-amz-storage-class` cabeçalho de solicitação é suportado e afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM correspondente especificar um comportamento de ingestão de confirmação dupla ou equilibrada.

- STANDARD

(Padrão) especifica uma operação de ingestão de commit duplo quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

- REDUCED\_REDUNDANCY

Especifica uma operação de ingestão de commit único quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.



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

## Usando x-amz-copy-source em PUT Object - Copy

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

Se a origem e o destino corresponderem 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, o StorageGRID não reingere o objeto. Isto tem duas consequências importantes:

- Não é possível usar COLOCAR Objeto - Copiar para criptografar um objeto existente no lugar ou para alterar a criptografia de um objeto existente no lugar. Se você fornecer o `x-amz-server-side-encryption` cabeçalho ou o `x-amz-server-side-encryption-customer-algorithm` cabeçalho, o StorageGRID rejeita a solicitação e retorna `XNotImplemented`.
- A opção de comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento de objetos que são acionadas pela atualização são feitas quando o ILM é reavaliado por 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-exigido 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 no lado do servidor, os cabeçalhos de solicitação fornecidos dependem se o objeto de origem está criptografado e se você planeja criptografar o objeto de destino.

- Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deve incluir os três cabeçalhos a seguir na solicitação PUT Object - Copy, para que o objeto possa ser descriptografado e copiado:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` AES256 Especifique .
  - `x-amz-copy-source-server-side-encryption-customer-key` Especifique a chave de criptografia fornecida quando você criou o objeto de origem.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu quando criou o objeto de origem.
- Se você quiser 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`: Especificar 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 resumo MD5 da nova chave de criptografia.

**Atenção:** 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 os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva gerenciada pelo StorageGRID (SSE), inclua esse cabeçalho no pedido COLOCAR Objeto - Copiar:

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

**Nota:** 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 versão

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` subrecurso. Se o intervalo de destino for versionado, a versão gerada será retornada `x-amz-version-id` no cabeçalho de resposta. Se o controle de versão estiver suspenso para o bucket de destino, `x-amz-version-id` então retornará um valor `"null"`.

### Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Usando criptografia do lado do servidor"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

["Objeto PUT"](#)

## **Informações sobre direitos autorais**

Copyright © 2025 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 SOBRESSALIENTES; 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.