



Operações para uploads de várias partes

StorageGRID

NetApp
March 10, 2025

Índice

Operações para uploads de várias partes	1
Listar carregamentos Multipart	2
Controle de versão	2
Inicie o carregamento de várias peças	2
Cabeçalhos de solicitação para criptografia do lado do servidor	5
Cabeçalhos de solicitação não suportados	5
Controle de versão	5
Carregar artigo	5
Cabeçalhos de solicitação suportados	5
Cabeçalhos de solicitação para criptografia do lado do servidor	6
Controle de versão	6
Carregar artigo - Copiar	6
Cabeçalhos de solicitação para criptografia do lado do servidor	6
Controle de versão	7
Concluir carregamento Multipart	7
Resolução de conflitos	7
Tamanho do objeto	7
Cabeçalhos de solicitação	7
Controle de versão	8
Falha na replicação, notificação ou notificação de metadados	8

Operações para uploads de várias partes

Esta seção descreve como o StorageGRID suporta operações para uploads de várias partes.

- ["Listar carregamentos de várias partes"](#)
- ["Inicie o carregamento de várias peças"](#)
- ["Carregar artigo"](#)
- ["Carregar artigo - Copiar"](#)
- ["Concluir carregamento Multipart"](#)

As seguintes condições e notas aplicam-se a todas as operações de carregamento em várias partes:

- Você não deve exceder 1.000 uploads simultâneos de várias partes para um único bucket, porque os resultados das consultas de uploads de várias partes para esse bucket podem retornar resultados incompletos.
- O StorageGRID impõe limites de tamanho da AWS para peças multipeças. S3 os clientes devem seguir estas diretrizes:
 - Cada parte em um upload de várias partes deve estar entre 5 MIB (5.242.880 bytes) e 5 GiB (5.368.709.120 bytes).
 - A última parte pode ser menor que 5 MIB (5.242.880 bytes).
 - Em geral, os tamanhos das peças devem ser tão grandes quanto possível. Por exemplo, use tamanhos de peças de 5 GiB para um objeto de 100 GiB. Como cada peça é considerada um objeto exclusivo, o uso de tamanhos de peças grandes reduz a sobrecarga de metadados do StorageGRID.
 - Para objetos menores que 5 GiB, considere usar upload não multipart.
- O ILM é avaliado para cada parte de um objeto multipart à medida que é ingerido e para o objeto como um todo quando o upload multipart é concluído, se a regra ILM usa o comportamento de ingestão rigoroso ou equilibrado. Você deve estar ciente de como isso afeta o posicionamento do objeto e da peça:
 - Se o ILM mudar enquanto um upload multipart S3 estiver em andamento, quando o upload multipart concluir algumas partes do objeto talvez não atendam aos requisitos atuais do ILM. Qualquer peça que não seja colocada corretamente está na fila para reavaliação ILM e é movida para o local correto mais tarde.
 - Ao avaliar o ILM para uma peça, o StorageGRID filtra o tamanho da peça, não o tamanho do objeto. Isso significa que partes de um objeto podem ser armazenadas em locais que não atendem aos requisitos de ILM para o objeto como um todo. Por exemplo, se uma regra específica que todos os objetos de 10 GB ou maior são armazenados em DC1 enquanto todos os objetos menores são armazenados em DC2, na ingestão cada parte de 1 GB de um upload multipart de 10 partes é armazenado em DC2. Quando ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.
- Todas as operações de upload em várias partes suportam controles de consistência do StorageGRID.
- Conforme necessário, você pode usar a criptografia do lado do servidor com uploads de várias partes. Para usar o SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID), você inclui o `x-amz-server-side-encryption` cabeçalho da solicitação somente na solicitação de upload de múltiplas partes. Para usar SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente), você especifica os mesmos três cabeçalhos de solicitação de chave de criptografia na solicitação de carregamento de múltiplas partes Iniciar e em cada solicitação de peça de carregamento subsequente.

Operação	Implementação
Listar carregamentos Multipart	Consulte " Listar carregamentos Multipart "
Inicie o carregamento de várias peças	Consulte " Inicie o carregamento de várias peças "
Carregar artigo	Consulte " Carregar artigo "
Carregar artigo - Copiar	Consulte " Carregar artigo - Copiar "
Concluir carregamento Multipart	Consulte " Concluir carregamento Multipart "
Abortar carregamento Multipart	Implementado com todo o comportamento da API REST do Amazon S3
Listar peças	Implementado com todo o comportamento da API REST do Amazon S3

Informações relacionadas

["Controles de consistência"](#)

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

Listar carregamentos Multipart

A operação List Multipart uploads lista uploads em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

- `encoding-type`
- `max-uploads`
- `key-marker`
- `prefix`
- `upload-id-marker`

O `delimiter` parâmetro Request não é suportado.

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Quando a operação completa de Upload Multipart é executada, esse é o ponto em que os objetos são criados (e versionados, se aplicável).

Inicie o carregamento de várias peças

A operação Iniciar carregamento Multipart inicia um upload multipart para um objeto e

retorna um ID de upload.

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.

Os seguintes cabeçalhos de solicitação são suportados:

- Content-Type
- 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.



A adição `creation-time` de metadados definidos pelo usuário não é permitida se você estiver adicionando um objeto a um bucket que tenha a conformidade legada habilitada. Um erro será retornado.

- 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"



Para obter informações sobre como o StorageGRID lida com caracteres UTF-8, consulte a documentação do PUT Object.

Cabeçalhos de solicitação para criptografia do lado do servidor

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

- **SSE:** Use o seguinte cabeçalho na solicitação de carregamento de múltiplas partes se você quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações de Upload Part.
 - `x-amz-server-side-encryption`
- **SSE-C:** Use todos esses três cabeçalhos na solicitação de Upload Multipart iniciada (e em cada solicitação de Upload Part subsequente) 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.

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".

Cabeçalhos de solicitação não suportados

O cabeçalho de solicitação a seguir não é suportado e retorna `XNotImplemented`

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

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação completa de Upload Multipart é executada.

Informações relacionadas

["Gerenciar objetos com ILM"](#)

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

["Objeto PUT"](#)

Carregar artigo

A operação Upload Part carrega uma peça em um upload multipart para um objeto.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Length`

- Content-MD5

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação de carregamento de múltiplas peças iniciada, você também deve incluir os seguintes cabeçalhos de solicitação em cada solicitação de Upload de peça:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256.
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia fornecida na solicitação Iniciar carregamento Multipart.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação de Envio de Multipart Iniciar.



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".

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação completa de Upload Multipart é executada.

Informações relacionadas

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

Carregar artigo - Copiar

A operação Upload Part - Copy carrega uma parte de um objeto copiando dados de um objeto existente como fonte de dados.

A operação Upload Part - Copy é implementada com todo o comportamento da API REST do Amazon S3.

Essa solicitação lê e grava os dados de objeto especificados no `x-amz-copy-source-range` sistema StorageGRID.

Os seguintes cabeçalhos de solicitação são suportados:

- `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`

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação de carregamento de múltiplas partes, você também deve incluir os seguintes cabeçalhos de solicitação em cada peça de carregamento - solicitação de cópia:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256.
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia fornecida na solicitação Iniciar carregamento Multipart.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação de Envio de Multipart Iniciar.

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 de Upload Part - Copy, para que o objeto possa ser descriptografado e copiado:

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



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".

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação completa de Upload Multipart é executada.

Concluir carregamento Multipart

A operação completa de Upload Multipart completa um upload multipart de um objeto, montando as peças carregadas anteriormente.

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.

Cabeçalhos de solicitação

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.



Se um upload multipart não for concluído dentro de 15 dias, a operação será marcada como inativa e todos os dados associados serão excluídos do sistema.



O ETag valor retornado não é uma soma MD5 dos dados, mas segue a implementação da API do Amazon S3 do ETag valor para objetos multipart.

Controle de versão

Esta operação completa um upload de várias partes. Se o controle de versão estiver habilitado para um bucket, a versão do objeto será criada após a conclusão do upload de várias partes.

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.



Quando o controle de versão está habilitado para um bucket, concluir um upload multipart sempre cria uma nova versão, mesmo que haja carregamentos simultâneos de várias partes concluídos na mesma chave de objeto. Quando o controle de versão não está habilitado para um bucket, é possível iniciar um upload multipart e, em seguida, ter outro upload multipart iniciado e concluído primeiro na mesma chave de objeto. Em buckets não versionados, o upload multipart que completa o último tem precedência.

Falha na replicação, notificação ou notificação de metadados

Se o intervalo onde ocorre o upload de várias partes estiver configurado para um serviço de plataforma, o upload de várias partes será bem-sucedido mesmo se a ação de replicação ou notificação associada falhar.

Se isso ocorrer, um alarme é gerado no Gerenciador de Grade em Eventos totais (SMTT). A mensagem último evento exibe "'Falha ao publicar notificações para chave de bucket-naameobject'" para o último objeto cuja notificação falhou. (Para ver esta mensagem, selecione **nós Storage Node Eventos**. Veja o último evento no topo da tabela.) As mensagens de evento também são listadas em `/var/local/log/bycast-err.log`.

Um locatário pode acionar a replicação ou notificação com falha atualizando os metadados ou as tags do objeto. Um locatário pode reenviar os valores existentes para evitar fazer alterações indesejadas.

Informações relacionadas

["Gerenciar objetos com ILM"](#)

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.