Operações para uploads de várias partes

StorageGRID

NetApp
March 12, 2025

Índice

Operações para uploads de várias partes

Operações para uploads de várias partes: Visão geral

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

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

- Você não deve exceder 1.000 carregamentos simultâneos de várias partes para um único bucket, porque os resultados das consultas ListMultipartUploads 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 grandes de peças 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 balanced ou strict ."opção de ingestão" 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, algumas partes do objeto podem não atender aos requisitos atuais do ILM quando o upload multipart for concluído. Qualquer peça que não seja colocada corretamente está na fila para reavaliação ILM e 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 especifica que todos os objetos de 10 GB ou maior são armazenados em DC1 enquanto todos os objetos menores são armazenados em DC2, cada parte de 1 GB de um upload multipart de 10 partes é armazenada em DC2 na ingestão. No entanto, quando ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.
- Todas as operações de upload multipart suportam StorageGRID "valores de consistência".
- Quando um objeto é ingerido utilizando o carregamento em várias partes, o "Limite de segmentação de objetos (1 GiB)"não é aplicado.
- Conforme necessário, você pode usar "criptografia do lado do servidor" com uploads de várias partes. Para usar 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 CreateMultipartUpload. 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 CreateMultipartUpload e em cada solicitação de UploadPart subsequente.

Operação	Implementação
AbortMultipartUpload	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio.
CompleteMultipartUpload	Consulte "CompleteMultipartUpload"
CreateMultipartUpload (Anteriormente nomeado iniciar carregamento de várias partes)	Consulte "CreateMultipartUpload"
ListMultipartUploads	Consulte "ListMultipartUploads"
ListParts	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio.
UploadPart	Consulte "UploadPart"
UploadPartCopy	Consulte "UploadPartCopy"

CompleteMultipartUpload

A operação CompleteMultipartUpload completa um upload em várias partes de um objeto montando as peças carregadas anteriormente.

Resolver conflitos

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo 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.

Cabeçalhos de solicitação

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

- `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 a 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.

CreateMultipartUpload

A operação CreateMultipartUpload (anteriormente chamada 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 o strict "opção 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 ingestão de commit duplo, 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 diferentes nós de storage.

    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 Commit duplo, 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.

> 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 pelas políticas ativas de ILM e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

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`

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do intervalo serão usadas para calcular a versão do objeto retida até a data.

  "Use a API REST do S3 para configurar o bloqueio de objetos do S3"

- 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`

    Cabeçalhos de solicitação para criptografia do lado do servidor

Para obter informações sobre como o StorageGRID lida com carateres UTF-8, "PutObject"consulte .

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 CreateMultipartUpload se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações UploadPart.
  - `x-amz-server-side-encryption`
- **SSE-C**: Use todos esses três cabeçalhos na solicitação CreateMultipartUpload (e em cada solicitação UploadPart subsequente) 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.

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 para "usando 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 CompleteMultipartUpload é executada.

ListMultipartUploads

A operação ListMultipartUploads lista os carregamentos de várias partes em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

- `encoding-type`
- `key-marker`

- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

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 CompleteMultipartUpload é executada.

UploadPart

A operação UploadPart carrega uma parte 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 criptografia SSE-C para a solicitação CreateMultipartUpload, você também deve incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPart:

- `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 CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação CreateMultipartUpload.

> 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 no "Use a 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 CompleteMultipartUpload é executada.

UploadPartCopy

A operação UploadPartCopy carrega uma parte de um objeto copiando dados de um objeto existente como fonte de dados.

A operação UploadPartCopy é implementada com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio.

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 criptografia SSE-C para a solicitação CreateMultipartUpload, você também deve incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPartCopy:

- `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 CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação CreateMultipartUpload.

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 UploadPartCopy, 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 no "Use a 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 CompleteMultipartUpload é executada.

Informações sobre direitos autorais

Informações sobre marcas comerciais