S3 operações e limitações suportadas pela API REST

StorageGRID

NetApp
March 12, 2025

Índice

S3 operações e limitações suportadas pela API REST

O sistema StorageGRID implementa a API de serviço de armazenamento simples (API versão 2006-03-01) com suporte para a maioria das operações e com algumas limitações. Você precisa entender os detalhes da implementação quando você está integrando aplicativos clientes REST API do S3.

O sistema StorageGRID oferece suporte a solicitações virtuais de estilo hospedado e a solicitações de estilo de caminho.

Tratamento da data

A implementação do StorageGRID da API REST S3 suporta apenas formatos de data HTTP válidos.

O sistema StorageGRID suporta apenas formatos de data HTTP válidos para qualquer cabeçalho que aceite valores de data. A parte da hora da data pode ser especificada no formato Greenwich Mean Time (GMT) ou no formato Universal Coordinated Time (UTC) sem deslocamento de fuso horário (o 0000 deve ser especificado). Se você incluir o `x-amz-date` cabeçalho em sua solicitação, ele substituirá qualquer valor especificado no cabeçalho da solicitação de data. Ao usar o AWS Signature versão 4, o `x-amz-date` cabeçalho deve estar presente na solicitação assinada porque o cabeçalho de data não é suportado.

Cabeçalhos de solicitação comuns

O sistema StorageGRID suporta cabeçalhos de solicitação comuns definidos pelo "Documentação do Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service", com uma exceção.

Cabeçalho da solicitação	Implementação
Autorização	Suporte completo para AWS Signature versão 2 Suporte para AWS Signature versão 4, com as seguintes exceções: • O valor SHA256 não é calculado para o corpo da solicitação. O valor enviado pelo usuário é aceito sem validação, como se o valor `UNSIGNED-PAYLOAD` tivesse sido fornecido para o `x-amz-content-sha256` cabeçalho.
x-amz-security-token	Não implementado. Retorna `XNotImplemented`.

Cabeçalhos de resposta comuns

O sistema StorageGRID suporta todos os cabeçalhos de resposta comuns definidos pela *Simple Storage Service API Reference*, com uma exceção.

Cabeçalho de resposta	Implementação
x-amz-id-2	Não utilizado

Autenticar solicitações

O sistema StorageGRID suporta acesso autenticado e anônimo a objetos usando a API S3.

A API S3 suporta a assinatura versão 2 e a assinatura versão 4 para autenticar solicitações de API S3.

As solicitações autenticadas devem ser assinadas usando seu ID de chave de acesso e chave de acesso secreta.

O sistema StorageGRID suporta dois métodos de autenticação: O cabeçalho HTTP `Authorization` e o uso de parâmetros de consulta.

Use o cabeçalho de autorização HTTP

O cabeçalho HTTP `Authorization` é usado por todas as operações da API S3, exceto solicitações anônimas, onde permitido pela política de bucket. O `Authorization` cabeçalho contém todas as informações de assinatura necessárias para autenticar uma solicitação.

Use parâmetros de consulta

Você pode usar parâmetros de consulta para adicionar informações de autenticação a um URL. Isso é conhecido como pré-assinar o URL, que pode ser usado para conceder acesso temporário a recursos específicos. Os usuários com o URL pré-assinado não precisam saber a chave de acesso secreto para acessar o recurso, o que permite que você forneça acesso restrito de terceiros a um recurso.

Operações no serviço

O sistema StorageGRID suporta as seguintes operações no serviço.

Operação	Implementação
Serviço GET	Implementado com todo o comportamento da API REST do Amazon S3.
OBTER uso de armazenamento	A solicitação OBTER uso do armazenamento informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta. Esta é uma operação no serviço com um caminho de / e um parâmetro de consulta personalizado (`?x-ntap-sg-usage`) adicionado.

Operação	Implementação
OPÇÕES /	Os aplicativos clientes podem emitir `OPTIONS /` solicitações para a porta S3 em um nó de storage, sem fornecer credenciais de autenticação S3.1X, para determinar se o nó de storage está disponível. Você pode usar essa solicitação para monitoramento ou permitir que balanceadores de carga externos identifiquem quando um nó de storage está inativo.

Informações relacionadas

OBTER solicitação de uso de armazenamento

Operações em baldes

O sistema StorageGRID dá suporte a um máximo de 1.000 buckets para cada conta de locatário de S3 TB.

As restrições de nome de bucket seguem as restrições de região padrão dos EUA da AWS, mas você deve restringi-las ainda mais a convenções de nomenclatura de DNS para oferecer suporte a solicitações de estilo hospedado virtual do S3.

"Documentação do Amazon Web Services (AWS): Restrições e limitações do bucket"

Configure os nomes de domínio de endpoint da API S3

As operações GET Bucket (List Objects) e GET Bucket Versions suportam controles de consistência do StorageGRID.

Você pode verificar se as atualizações para a última hora de acesso estão ativadas ou desativadas para buckets individuais.

A tabela a seguir descreve como o StorageGRID implementa as operações de bucket da API REST do S3. Para realizar qualquer uma dessas operações, as credenciais de acesso necessárias devem ser fornecidas para a conta.

Operação	Implementação
ELIMINAR balde	Implementado com todo o comportamento da API REST do Amazon S3.
ELIMINAR Cors balde	Esta operação exclui a configuração CORS para o bucket.
ELIMINAR encriptação Bucket	Esta operação exclui a criptografia padrão do intervalo. Os objetos criptografados existentes permanecem criptografados, mas todos os novos objetos adicionados ao bucket não são criptografados.
ELIMINAR ciclo de vida do balde	Esta operação exclui a configuração do ciclo de vida do bucket.

Operação	Implementação
ELIMINAR política de balde	Esta operação exclui a política anexada ao bucket.
ELIMINAR replicação de balde	Esta operação exclui a configuração de replicação anexada ao bucket.
ELIMINAR marcação de intervalo	Esta operação usa o `tagging` subrecurso para remover todas as tags de um bucket.
GET Bucket (List Objects), versão 1 e versão 2	Esta operação retorna alguns ou todos (até 1.000) dos objetos em um balde. A Classe de armazenamento para objetos pode ter um de dois valores, mesmo que o objeto tenha sido ingerido com a `REDUCED_REDUNDANCY` opção de classe de armazenamento: • `STANDARD`, Que indica que o objeto está armazenado em um pool de storage que consiste em nós de storage. • `GLACIER`, Que indica que o objeto foi movido para o bucket externo especificado pelo pool de armazenamento em nuvem. Se o intervalo contiver um grande número de chaves excluídas que tenham o mesmo prefixo, a resposta pode incluir algumas `CommonPrefixes` que não contêm chaves.
OBTER acl balde	Esta operação retorna uma resposta positiva e a ID, DisplayName e permissão do proprietário do bucket, indicando que o proprietário tem acesso total ao bucket.
OBTER Bucket Cors	Esta operação retorna a `cors` configuração do balde.
OBTER criptografia Bucket	Esta operação retorna a configuração de criptografia padrão para o bucket.
OBTENHA o ciclo de vida do Bucket	Esta operação retorna a configuração do ciclo de vida do bucket.
OBTER localização do balde	Esta operação retorna a região que foi definida usando o `LocationConstraint` elemento na solicitação PUT Bucket. Se a região do bucket for `us-east-1`, uma string vazia será retornada para a região.
OBTER notificação Bucket	Esta operação retorna a configuração de notificação anexada ao bucket.
OBTER versões Objeto balde	Com ACESSO DE LEITURA em um bucket, essa operação com o `versions` subrecurso lista metadados de todas as versões de objetos no bucket.
OBTER política Bucket	Esta operação retorna a política anexada ao bucket.

Operação	Implementação
OBTER replicação do bucket	Esta operação retorna a configuração de replicação anexada ao bucket.
OBTER marcação Bucket	Esta operação usa o `tagging` subrecurso para retornar todas as tags para um bucket.
OBTENHA o controle de versão do Bucket	Essa implementação usa `versioning` o subrecurso para retornar o estado de controle de versão de um bucket. • *Blank*: O controle de versão nunca foi habilitado (o bucket é "não versionado") • Habilitado: O controle de versão está habilitado • Suspenso: O controle de versão foi ativado anteriormente e está suspenso
OBTER Configuração bloqueio Objeto	Esta operação retorna o modo de retenção padrão do bucket e o período de retenção padrão, se configurado. OBTER Configuração bloqueio ObjetoConsulte para obter informações detalhadas.
Balde DA cabeça	Esta operação determina se existe um intervalo e você tem permissão para acessá-lo. Esta operação retorna: • `x-ntap-sg-bucket-id`: O UUID do bucket no formato UUID. • `x-ntap-sg-trace-id`: O ID de rastreamento exclusivo da solicitação associada.

Operação	Implementação
COLOQUE o balde	Esta operação cria um novo balde. Ao criar o balde, você se torna o proprietário do balde. • Os nomes dos buckets devem estar em conformidade com as seguintes regras: ◦ Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário). ◦ Deve ser compatível com DNS. ◦ Deve conter pelo menos 3 e não mais de 63 carateres. ◦ Pode ser uma série de uma ou mais etiquetas, com etiquetas adjacentes separadas por um período. Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens. ◦ Não deve se parecer com um endereço IP formatado em texto. ◦ Não deve usar períodos em solicitações de estilo hospedadas virtuais. Os períodos causarão problemas com a verificação do certificado curinga do servidor. • Por padrão, os intervalos são criados na `us-east-1` região; no entanto, você pode usar o `LocationConstraint` elemento de solicitação no corpo da solicitação para especificar uma região diferente. Ao usar o `LocationConstraint` elemento, você deve especificar o nome exato de uma região que foi definida usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Contacte o administrador do sistema se não souber o nome da região que deve utilizar. **Nota**: Ocorrerá um erro se a solicitação PUT Bucket usar uma região que não foi definida no StorageGRID. • Você pode incluir o `x-amz-bucket-object-lock-enabled` cabeçalho de solicitação para criar um bucket com o bloqueio de objeto S3 ativado. Use o bloqueio de objetos S3D.Consulte . Você deve ativar o bloqueio de objeto S3 quando você criar o bucket. Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação de um intervalo. O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.
COLOQUE cors de balde	Esta operação define a configuração do CORS para um bucket de modo que o bucket possa atender às solicitações de origem cruzada. O compartilhamento de recursos de origem cruzada (CORS) é um mecanismo de segurança que permite que aplicativos da Web do cliente em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket S3 chamado `images` para armazenar gráficos. Ao definir a configuração CORS para o `images` intervalo, pode permitir que as imagens nesse intervalo sejam apresentadas no website `http://www.example.com`.

Operação	Implementação
COLOQUE a criptografia Bucket	Esta operação define o estado de criptografia padrão de um bucket existente. Quando a criptografia no nível do bucket está ativada, todos os novos objetos adicionados ao bucket são criptografados. O StorageGRID suporta criptografia no lado do servidor com chaves gerenciadas pelo StorageGRID. Ao especificar a regra de configuração de criptografia do lado do servidor, defina o `SSEAlgorithm` parâmetro como `AES256`, e não use o `KMSMasterKeyID` parâmetro. A configuração de criptografia padrão do bucket é ignorada se a solicitação de upload de objeto já especificar criptografia (ou seja, se a solicitação incluir o `x-amz-server-side-encryption-*` cabeçalho da solicitação).
COLOQUE o ciclo de vida do balde	Essa operação cria uma nova configuração de ciclo de vida para o bucket ou substitui uma configuração de ciclo de vida existente. O StorageGRID dá suporte a até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML: • Validade (dias, Data) • Não-currentVersionExpiration (não-currentDays) • Filtro (prefixo, Tag) • Estado • ID O StorageGRID não oferece suporte a essas ações: • AbortIncompleteMultipartUpload • ExpiredObjectDeleteMarker • Transição Para entender como a ação Expiration em um ciclo de vida de um bucket interage com as instruções de colocação do ILM, consulte "como o ILM opera ao longo da vida de um objeto" nas instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações. **Nota**: A configuração do ciclo de vida do bucket pode ser usada com buckets que têm o S3 Object Lock ativado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis com o legado.

Operação	Implementação

COLOCAR notificação de balde	Esta operação configura notificações para o bucket usando o XML de configuração de notificação incluído no corpo da solicitação. Você deve estar ciente dos seguintes detalhes de implementação:
	
	• O StorageGRID oferece suporte a tópicos do Serviço de notificação simples (SNS) como destinos. Os endpoints do Simple Queue Service (SQS) ou do Amazon Lambda não são suportados.
	• O destino das notificações deve ser especificado como a URNA de um endpoint do StorageGRID. Os endpoints podem ser criados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário.
	
	O endpoint deve existir para que a configuração de notificação seja bem-sucedida. Se o endpoint não existir, um `400 Bad Request` erro é retornado com o código `InvalidArgument`.
	
	• Não é possível configurar uma notificação para os seguintes tipos de eventos. Esses tipos de eventos são **não** suportados.
	
	◦ `s3:ReducedRedundancyLostObject`
	
	◦ `s3:ObjectRestore:Completed`
	
	• As notificações de eventos enviadas do StorageGRID usam o formato JSON padrão, exceto que elas não incluem algumas chaves e usam valores específicos para outras, como mostrado na seguinte listagem:
	• **EventSource**
	
	`sgws:s3`
	
	• **AwsRegion**
	
	não incluído
	
	• **x-amz-id-2**
	
	não incluído
	
	• **arn**
	
	`urn:sgws:s3:::bucket_name`

Política COLOCAR balde	Esta operação define a política anexada ao balde.

Operação	Implementação
COLOQUE a replicação do balde	Esta operação configura a replicação do StorageGRID CloudMirror para o bucket usando o XML de configuração de replicação fornecido no corpo da solicitação. Para a replicação do CloudMirror, você deve estar ciente dos seguintes detalhes de implementação: • O StorageGRID suporta apenas V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue convenções V1 para exclusão de versões de objetos. Para obter detalhes, consulte "Documentação do Amazon S3 sobre configuração de replicação" . • A replicação do bucket pode ser configurada em buckets versionados ou não versionados. • Você pode especificar um intervalo de destino diferente em cada regra do XML de configuração de replicação. Um bucket de origem pode ser replicado para mais de um bucket de destino. • Os buckets de destino devem ser especificados como a URN dos endpoints do StorageGRID, conforme especificado no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. O endpoint deve existir para que a configuração de replicação seja bem-sucedida. Se o endpoint não existir, a solicitação falhará como um `400 Bad Request`. a mensagem de erro indica: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Não é necessário especificar um `Role` no XML de configuração. Este valor não é usado pelo StorageGRID e será ignorado se enviado. • Se você omitir a classe de armazenamento do XML de configuração, o StorageGRID usará a `STANDARD` classe de armazenamento por padrão. • Se você excluir um objeto do bucket de origem ou excluir o bucket de origem, o comportamento de replicação entre regiões é o seguinte: ◦ Se você excluir o objeto ou o bucket antes que ele tenha sido replicado, o objeto/bucket não será replicado e você não será notificado. ◦ Se você excluir o objeto ou o bucket depois que ele foi replicado, o StorageGRID segue o comportamento padrão de exclusão do Amazon S3 para V1 TB de replicação entre regiões.
COLOQUE a marcação de balde	Esta operação usa o `tagging` subrecurso para adicionar ou atualizar um conjunto de tags para um bucket. Ao adicionar etiquetas de bucket, esteja ciente das seguintes limitações: • O StorageGRID e o Amazon S3 suportam até 50 tags para cada bucket. • As tags associadas a um bucket devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 carateres Unicode de comprimento. • Os valores de tag podem ter até 256 carateres Unicode de comprimento. • Chave e valores são sensíveis a maiúsculas e minúsculas.

Operação	Implementação
COLOQUE o controle de versão do Bucket	Essa implementação usa `versioning` o subrecurso para definir o estado de controle de versão de um bucket existente. Você pode definir o estado de controle de versão com um dos seguintes valores: • Habilitado: Permite o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo. • Suspenso: Desativa o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão `null` .
COLOCAR Configuração bloqueio Objeto	Esta operação configura ou remove o modo de retenção padrão do bucket e o período de retenção padrão. Se o período de retenção padrão for modificado, a data de retenção até as versões de objetos existentes permanecerá a mesma e não será recalculada usando o novo período de retenção padrão. COLOCAR Configuração bloqueio ObjetoConsulte para obter informações detalhadas.

Informações relacionadas

Controles de consistência

OBTER último pedido de tempo de acesso do Bucket

Políticas de acesso ao bucket e ao grupo

S3 operações rastreadas em logs de auditoria

Gerenciar objetos com ILM

Use a conta de locatário

Crie a configuração do ciclo de vida do S3

Você pode criar uma configuração de ciclo de vida do S3 para controlar quando objetos específicos são excluídos do sistema StorageGRID.

O exemplo simples nesta seção ilustra como uma configuração do ciclo de vida do S3 pode controlar quando certos objetos são excluídos (expirados) de buckets específicos do S3. O exemplo nesta seção é apenas para fins ilustrativos. Para obter detalhes completos sobre como criar configurações de ciclo de vida do S3, "Amazon Simple Storage Service Developer Guide: Gerenciamento do ciclo de vida do objeto" consulte . Observe que o StorageGRID suporta apenas ações de expiração; ele não oferece suporte a ações de transição.

Qual é a configuração do ciclo de vida

Uma configuração de ciclo de vida é um conjunto de regras que são aplicadas aos objetos em buckets específicos do S3. Cada regra especifica quais objetos são afetados e quando esses objetos expirarão (em uma data específica ou após algum número de dias).

O StorageGRID dá suporte a até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML:

- Expiração: Exclua um objeto quando uma data especificada é atingida ou quando um número especificado de dias é atingido, a partir de quando o objeto foi ingerido.
- NoncurrentVersionExpiration: Exclua um objeto quando um número especificado de dias é atingido, a partir de quando o objeto se tornou inatual.
- Filtro (prefixo, Tag)
- Estado
- ID

Se você aplicar uma configuração de ciclo de vida a um bucket, as configurações de ciclo de vida do bucket sempre substituem as configurações de ILM do StorageGRID. O StorageGRID usa as configurações de expiração para o bucket, não o ILM, para determinar se deseja excluir ou reter objetos específicos.

Como resultado, um objeto pode ser removido da grade, mesmo que as instruções de colocação em uma regra ILM ainda se apliquem ao objeto. Ou, um objeto pode ser retido na grade mesmo depois que quaisquer instruções de colocação de ILM para o objeto tiverem expirado. Para obter detalhes, Como o ILM opera ao longo da vida de um objetoconsulte .

> A configuração do ciclo de vida do bucket pode ser usada com buckets que têm o S3 Object Lock ativado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis com legado.

O StorageGRID dá suporte ao uso das seguintes operações de bucket para gerenciar configurações do ciclo de vida:

- ELIMINAR ciclo de vida do balde
- OBTENHA o ciclo de vida do Bucket
- COLOQUE o ciclo de vida do balde

Criar configuração do ciclo de vida

Como primeira etapa na criação de uma configuração de ciclo de vida, você cria um arquivo JSON que inclui uma ou mais regras. Por exemplo, este arquivo JSON inclui três regras, como segue:

1. A regra 1 aplica-se apenas a objetos que correspondam ao prefixo `category1/` e que tenham um `key2` valor `tag2` de . O `Expiration` parâmetro especifica que os objetos correspondentes ao filtro expirarão à meia-noite de 22 de agosto de 2020.
2. A regra 2 aplica-se apenas a objetos que correspondam ao prefixo `category2/`. O `Expiration` parâmetro especifica que os objetos correspondentes ao filtro expirarão 100 dias após serem ingeridos.

   > As regras que especificam um número de dias são relativas a quando o objeto foi ingerido. Se a data atual exceder a data de ingestão mais o número de dias, alguns objetos podem ser removidos do intervalo assim que a configuração do ciclo de vida for aplicada.

3. A regra 3 aplica-se apenas a objetos que correspondam ao prefixo `category3/`. O `Expiration` parâmetro especifica que quaisquer versões não atuais de objetos correspondentes expirarão 50 dias após se tornarem não atuais.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Aplique a configuração do ciclo de vida ao bucket

Depois de criar o arquivo de configuração do ciclo de vida, aplique-o a um bucket emitindo uma solicitação DE ciclo de vida do PUT Bucket.

Essa solicitação aplica a configuração do ciclo de vida no arquivo de exemplo a objetos em um bucket `testbucket` chamado .

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que uma configuração de ciclo de vida foi aplicada com sucesso ao bucket, emita uma solicitação DE ciclo de vida do GET Bucket. Por exemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Uma resposta bem-sucedida lista a configuração do ciclo de vida que você acabou de aplicar.

Valide que a expiração do ciclo de vida do bucket se aplica ao objeto

É possível determinar se uma regra de expiração na configuração do ciclo de vida se aplica a um objeto específico ao emitir uma SOLICITAÇÃO PUT Object, HEAD Object ou GET Object. Se uma regra se aplicar, a resposta inclui um `Expiration` parâmetro que indica quando o objeto expira e qual regra de expiração foi correspondida.

> Como o ciclo de vida do bucket substitui o ILM, a `expiry-date` mostrada é a data real em que o objeto será excluído. Para obter detalhes, Como a retenção de objetos é determinadaconsulte .

Por exemplo, essa SOLICITAÇÃO PUT Object foi emitida em 22 de junho de 2020 e coloca um objeto no `testbucket` intervalo.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

A resposta de sucesso indica que o objeto expirará em 100 dias (01 de outubro de 2020) e que correspondia à regra 2 da configuração do ciclo de vida.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Por exemplo, essa solicitação de objeto PRINCIPAL foi usada para obter metadados para o mesmo objeto no bucket do testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

A resposta de sucesso inclui os metadados do objeto e indica que o objeto expirará em 100 dias e que correspondia à regra 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Use retenção padrão do bucket do bloqueio de objetos S3

Se um bucket tiver o bloqueio de objetos S3 ativado, você poderá especificar um modo de retenção padrão e um período de retenção padrão que é aplicado a cada objeto adicionado ao bucket.

- S3 o bloqueio de objetos pode ser ativado ou desativado para um balde durante a criação do balde.
- Se o bloqueio de objetos S3 estiver ativado para um bucket, você poderá configurar a retenção padrão para o bucket.
- A configuração de retenção padrão especifica:
  - Modo de retenção padrão: O StorageGRID suporta apenas o modo de "CONFORMIDADE".
  - Período de retenção padrão em dias ou anos.

OBTER Configuração bloqueio Objeto

A solicitação DE configuração GET Object Lock permite determinar se o Object Lock está habilitado para um bucket e, se ele está ativado, ver se há um modo de retenção padrão e período de retenção configurados para o bucket.

Quando novas versões de objetos são ingeridas para o bucket, o modo de retenção padrão é aplicado se `x-amz-object-lock-mode` não for especificado. O período de retenção padrão é usado para calcular a data de retenção até se `x-amz-object-lock-retain-until-date` não for especificado.

Você deve ter a permissão S3:GetBucketObjectLockConfiguration, ou ser raiz da conta, para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization string
Authorization: authorization string
```

Exemplo de resposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

COLOCAR Configuração bloqueio Objeto

A solicitação de configuração de bloqueio de objeto PUT permite modificar o modo de retenção padrão e o período de retenção padrão para um bucket que tem bloqueio de objeto ativado. Você também pode remover as configurações de retenção padrão configuradas anteriormente.

Quando novas versões de objetos são ingeridas para o bucket, o modo de retenção padrão é aplicado se `x-amz-object-lock-mode` não for especificado. O período de retenção padrão é usado para calcular a data de retenção até se `x-amz-object-lock-retain-until-date` não for especificado.

Se o período de retenção padrão for modificado após a ingestão de uma versão de objeto, a data de retenção até a versão do objeto permanecerá a mesma e não será recalculada usando o novo período de retenção padrão.

Você deve ter a permissão S3:PutBucketObjectLockConfiguration, ou ser raiz da conta, para concluir esta operação.

O `Content-MD5` cabeçalho da solicitação deve ser especificado na solicitação DE COLOCAÇÃO.

Exemplo de solicitação

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization string
Authorization: authorization string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Operações personalizadas em buckets

O sistema StorageGRID dá suporte a operações de bucket personalizadas que são adicionadas à API REST do S3 e são específicas do sistema.

A tabela a seguir lista as operações de bucket personalizadas suportadas pelo StorageGRID.

Operação	Descrição	Para mais informações
OBTER consistência de balde	Retorna o nível de consistência que está sendo aplicado a um balde específico.	OBTER pedido de consistência de balde

Operação	Descrição	Para mais informações
COLOQUE a consistência do balde	Define o nível de consistência aplicado a um balde específico.	COLOCAR pedido consistência balde
OBTER último tempo de acesso do Bucket	Retorna se as atualizações da última hora de acesso estão ativadas ou desativadas para um intervalo específico.	OBTER último pedido de tempo de acesso do Bucket
COLOQUE o último tempo de acesso do balde	Permite-lhe ativar ou desativar as atualizações da última hora de acesso para um intervalo específico.	COLOCAR o último pedido de tempo de acesso do balde
ELIMINAR configuração de notificação de metadados do bucket	Exclui o XML de configuração de notificação de metadados associado a um bucket específico.	EXCLUIR solicitação de configuração de notificação de metadados do bucket
OBTER configuração de notificação de metadados do bucket	Retorna o XML de configuração de notificação de metadados associado a um intervalo específico.	OBTER solicitação de configuração de notificação de metadados do bucket
COLOQUE a configuração de notificação de metadados do bucket	Configura o serviço de notificação de metadados para um bucket.	COLOCAR solicitação de configuração de notificação de metadados do bucket
COLOQUE o balde com as definições de conformidade	Obsoleto e não suportado: Você não pode mais criar novos buckets com a conformidade ativada.	Obsoleto: COLOQUE o Bucket com as configurações de conformidade
OBTENHA conformidade com o balde	Obsoleto, mas suportado: Retorna as configurações de conformidade atualmente em vigor para um bucket compatível com legado existente.	Obsoleto: OBTER solicitação de conformidade do bucket
COLOQUE a conformidade do balde	Obsoleto, mas suportado: Permite modificar as configurações de conformidade para um bucket compatível com legado existente.	Obsoleto: COLOQUE a solicitação de conformidade do bucket

Informações relacionadas

S3 operações rastreadas nos logs de auditoria

Operações em objetos

Esta seção descreve como o sistema StorageGRID implementa S3 operações de API

REST para objetos.

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

- Os StorageGRID controles de consistênciasão suportados por todas as operações em objetos, com exceção dos seguintes:
  - OBTER ACL Objeto
  - `OPTIONS /`
  - COLOCAR guarda legal Objeto
  - COLOCAR retenção Objeto
  - SELECIONE conteúdo do objeto
- 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.
- 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	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. 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. **Controle de versão** Para remover uma versão específica, o solicitante deve ser o proprietário do bucket e usar o `versionId` subrecurso. O uso deste subrecurso exclui permanentemente a versão. Se o `versionId` corresponder a um marcador de exclusão, o cabeçalho de resposta `x-amz-delete-marker` será retornado como `true`. • Se um objeto for excluído sem o `versionId` subrecurso em um bucket habilitado para versão, isso resultará na geração de um marcador de exclusão. O `versionId` para o marcador de exclusão é retornado usando o `x-amz-version-id` cabeçalho de resposta e o `x-amz-delete-marker` cabeçalho de resposta é retornado como `true`. • Se um objeto for excluído sem o `versionId` sub-recurso 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 `x-amz-delete-marker` cabeçalho de resposta é retornado definido como `true`. **Nota**: Em certos casos, vários marcadores de exclusão podem existir para um objeto.
Excluir vários objetos	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. Vários objetos podem ser excluídos na mesma mensagem de solicitação.

Operação	Implementação
ELIMINAR marcação Objeto	Usa o `tagging` subrecurso para remover todas as tags de um objeto. Implementado com todo o comportamento da API REST do Amazon S3. **Controle de versão** Se o `versionId` 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 "'MethodNotAllowed'" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.
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	Use o bloqueio de objetos S3D.
OBTER retenção de objetos	Use o bloqueio de objetos S3D.
OBTER marcação de objetos	Usa o `tagging` subrecurso para retornar todas as tags para um objeto. Implementado com todo o comportamento da API REST do Amazon S3 **Controle de versão** Se o `versionId` 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 "'MethodNotAllowed'" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.
Objeto HEAD	Objeto HEAD
Restauração PÓS-objeto	Restauração PÓS-objeto
Objeto PUT	Objeto PUT
COLOCAR Objeto - Copiar	COLOCAR Objeto - Copiar
COLOCAR guarda legal Objeto	Use o bloqueio de objetos S3D.
COLOCAR retenção Objeto	Use o bloqueio de objetos S3D.

Operação	Implementação
COLOQUE a marcação Objeto	Usa o `tagging` subrecurso para adicionar um conjunto de tags a um objeto existente. Implementado com todo o comportamento da API REST do Amazon S3 • Limites de tag de 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 carateres Unicode de comprimento e os valores de tag podem ter até 256 carateres Unicode de comprimento. Chave e valores são sensíveis a maiúsculas e minúsculas. **Atualizações de tags e comportamento de ingestão** 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. 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. **Resolução de 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. **Controle de versão** Se o `versionId` 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 "'MethodNotAllowed'" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Informações relacionadas

S3 operações rastreadas em logs de auditoria

Use o bloqueio de objetos S3D.

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 especificar períodos de retenção padrão para cada bucket ou configurações específicas de retenção até a data e retenção legal 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.

Ative o bloqueio de objetos S3D para o 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 a 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 oferece suporte a períodos de retenção padrão para os objetos nos buckets do bloqueio de objetos do S3 e suporta a operação do bucket Configuração do bloqueio de objetos do PUT. A `s3:object-lock-remaining-retention-days` chave de condição de política define os períodos de retenção mínimo e máximo permitidos para seus objetos.

Determinar se o bloqueio de objetos S3 está ativado para o balde

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

Crie objeto com as configurações de bloqueio de objeto S3

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.

Atualizar as definições do 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 a 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"

Utilize S3 Select (Selecionar)

O StorageGRID oferece suporte às seguintes cláusulas, tipos de dados e operadores do AWS S3 Select para o SelectObjectContent - comando.

Os itens não listados não são suportados.

Para obter a sintaxe, Selecione ObjectContentconsulte . Para obter mais informações sobre S3 Select, consulte "Documentação da AWS para o S3 Select".

Apenas as contas de inquilino que tenham S3 Select ativado podem emitir consultas SelectObjectContent. Consulte Considerações e requisitos para usar o S3 Select.

Cláusulas

- Selecione a lista
- Da cláusula
- Cláusula where
- CLÁUSULA LIMIT (LIMITE)

Tipos de dados

- bool
- número inteiro
- cadeia de carateres
- flutuação
- decimal, numérico
- timestamp

Operadores

Operadores lógicos

- E
- NÃO
- OU

Operadores de comparação

* * * lt * gt * . * . * * ! * ENTRE * EM

Operadores de correspondência de padrões

- GOSTO
- _
- %

Operadores unitários

- É NULO
- NÃO É NULL

Operadores de matemática

- E
- -
- *
- /
- %

O StorageGRID segue a precedência do operador AWS S3 Select.

Agregar funções

- MÉDIA ()
- CONTAGEM (*)
- MÁX. ()
- MIN. ()
- SOMA()

Funções condicionais

- CASO
- COALESCE
- NULLIF

Funções de conversão

- CAST (para tipos de dados suportados)

Funções de data

- DATE_ADD
- DATE_DIFF
- EXTRAIR
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

Funções de cadeia de carateres

- CHAR_LENGTH, CHARACTER_LENGTH
- BAIXAR
- SUBSTRING
- APARAR
- SUPERIOR

Use a 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.

Use 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

Use 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.

OBTER objetos e multipartes

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

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

apenas para objetos segmentados ou multipartes.

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`: Especificar `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 carateres em metadados do usuário

O StorageGRID não analisa nem interpreta carateres UTF-8 escapados em metadados definidos pelo usuário. Obter solicitações para um objeto com carateres UTF-8 escapados em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome ou valor da chave incluir carateres 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` Uma cópia do objeto é recuperada.
Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável	`200 OK` Uma cópia do objeto é recuperada.
Objeto transicionado para um estado não recuperável	`403 Forbidden, InvalidObjectState` 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` Aguarde até que a solicitação de restauração PÓS-objeto seja concluída.
Objeto totalmente restaurado para o Cloud Storage Pool	`200 OK` 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

Use a criptografia do lado do servidor

Gerenciar objetos com ILM

Restauração PÓS-objeto

S3 operações rastreadas em 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.

Objeto PRINCIPAL e objetos multipart

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

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

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`: Especificar `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 carateres em metadados do usuário

O StorageGRID não analisa nem interpreta carateres UTF-8 escapados em metadados definidos pelo usuário. As SOLICITAÇÕES HEAD para um objeto com carateres UTF-8 escapados em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome ou valor da chave incluir carateres 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	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Até que o objeto seja transferido para um estado não recuperável, o valor para `expiry-date` é definido para algum tempo distante no futuro. A hora exata da transição não é controlada pelo sistema StorageGRID.

O objeto fez a transição para o estado não recuperável, mas pelo menos uma cópia também existe na grade	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	O valor para `expiry-date` é definido para algum tempo distante no futuro.
	
	Nota: 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.

Objeto transicionado para um estado não recuperável e nenhuma cópia existe na grade	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Estado do objeto	Resposta ao objeto PRINCIPAL

Objeto em processo de restauração a partir de um estado não recuperável	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Objeto totalmente restaurado para o Cloud Storage Pool	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	O `expiry-date` indica quando o objeto no pool de armazenamento em nuvem será retornado a um estado não recuperável.

Objetos segmentados ou multiparte no Cloud Storage Pool

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

Use a criptografia do lado do servidor

Gerenciar objetos com ILM

Restauração PÓS-objeto

S3 operações rastreadas em 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. **Nota**: Antes de um objeto ser transferido para um estado não recuperável, não é possível alterar o seu `expiry-date`.

Estado do objeto	Comportamento da restauração PÓS-objeto
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. Opcionalmente, use o `Tier` elemento de solicitação para determinar quanto tempo o trabalho de restauração levará para concluir (`Expedited`, `Standard` ou `Bulk`). Se você não especificar `Tier`, o `Standard` nível será usado. **Atenção**: 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 `Expedited` nível. O seguinte erro é retornado `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class.`
Objeto em processo de restauração a partir de um estado não recuperável	`409 Conflict`, `RestoreAlreadyInProgress`
Objeto totalmente restaurado para o Cloud Storage Pool	`200 OK` **Observação:** se um objeto foi restaurado para um estado recuperável, você pode alterar o mesmo `expiry-date` reemitindo a solicitação de restauração PÓS-objeto com um novo valor para `Days`. A data de restauração é atualizada em relação à hora da solicitação.

Informações relacionadas

Gerenciar objetos com ILM

Objeto HEAD

S3 operações rastreadas em logs de auditoria

Objeto PUT

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

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.

Tamanho do objeto

O tamanho máximo *recommended* para uma única operação PUT Object é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multipart.

> No StorageGRID 11,6, o tamanho máximo *suportado* para uma operação de objeto PUT único é de 5 TIB (5.497.558.138.880 bytes). No entanto, o alerta **S3 PUT Object Size too large** será acionado se você tentar fazer o upload de um objeto que exceda 5 GiB.

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 carateres 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 carateres UTF-8 escapados incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Os carateres UTF-8 escapados são tratados como carateres ASCII:

- As solicitações PUT, PUT Object-Copy, GET e HEAD são bem-sucedidas se os metadados definidos pelo usuário incluírem carateres UTF-8 escapados.
- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome ou valor da chave incluir carateres 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 carateres Unicode de comprimento e os valores de tag podem ter até 256 carateres 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`o 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`

    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 o bloqueio de objetos S3D.

- 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`

  Consulte Cabeçalhos de solicitação para criptografia do lado do servidor

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".

Observação: se um objeto for criptografado com SSE ou SSE-C, qualquer configuração de criptografia no nível de bucket ou no 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 em logs de auditoria

Use a 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.

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.

Tamanho do objeto

O tamanho máximo *recommended* para uma única operação PUT Object é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multipart.

> No StorageGRID 11,6, o tamanho máximo *suportado* para uma operação de objeto PUT único é de 5 TIB (5.497.558.138.880 bytes). No entanto, o alerta **S3 PUT Object Size too large** será acionado se você tentar fazer o upload de um objeto que exceda 5 GiB.

UTF-8 carateres 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 carateres UTF-8 escapados incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Os carateres UTF-8 escapados são tratados como carateres ASCII:

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

    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 o bloqueio de objetos S3D.

- 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`

    Consulte Cabeçalhos de solicitação para criptografia do lado do servidor

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `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

Use a criptografia do lado do servidor

S3 operações rastreadas em logs de auditoria

Objeto PUT

Selecione ObjectContent

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

Para obter mais informações, consulte "Documentação da AWS para SelectObjectContent" .

O que você vai precisar

- A conta de locatário tem a permissão S3 Select (Selecionar).
- Você tem `s3:GetObject` permissão para o objeto que deseja consultar.
- O objeto que você deseja consultar está em formato CSV ou é um arquivo compactado GZIP ou bzip2 contendo um arquivo formatado CSV.
- Sua expressão SQL tem um comprimento máximo de 256 KB.
- Qualquer Registro na entrada ou resultados tem um comprimento máximo de 1 MIB.

Exemplo de sintaxe de solicitação

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

Exemplo de consulta SQL

Esta consulta obtém o nome do estado, 2010 populações, 2015 populações estimadas e a porcentagem de mudança dos dados do censo americano. Os Registros no arquivo que não são estados são ignorados.

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

As primeiras linhas do arquivo a serem consultadas, `SUB-EST2020_ALL.csv`, são assim:

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

Exemplo de uso da AWS-CLI

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

As primeiras linhas do arquivo de saída, `changes.csv`, são assim:

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

Operações para uploads de várias partes

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 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 especifica 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
- Use a 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`

    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.

  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`

    Cabeçalhos de solicitação para criptografia do lado do servidor

Para obter informações sobre como o StorageGRID lida com carateres 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`: 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".

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

Use a 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

Use a 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.

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 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

Respostas de erro

O sistema StorageGRID suporta todas as respostas de erro padrão da API REST S3 que se aplicam. Além disso, a implementação do StorageGRID adiciona várias respostas personalizadas.

Códigos de erro S3 API suportados

Nome	Status HTTP
AccessDenied	403 proibido
BadDigest	400 pedido incorreto
BucketAlreadyExists	409 conflito
BucketNotEmpty	409 conflito
IncompleteBody	400 pedido incorreto
InternalError (erro internacional)	500 erro interno do servidor
InvalidAccessKeyId	403 proibido
InvalidArgument	400 pedido incorreto
InvalidBucketName	400 pedido incorreto
InvalidBucketState	409 conflito
InvalidDigest	400 pedido incorreto
InvalidEncryptionAlgorithmError	400 pedido incorreto
InvalidPart	400 pedido incorreto
InvalidPartOrder	400 pedido incorreto
Intervalo Invalidável	416 intervalo solicitado não satisfatório

Nome	Status HTTP
InvalidRequest	400 pedido incorreto
InvalidStorageClass	400 pedido incorreto
InvalidTag	400 pedido incorreto
InvalidURI	400 pedido incorreto
KeyTooLong	400 pedido incorreto
MalformedXML	400 pedido incorreto
MetadataTooLarge	400 pedido incorreto
MetodNotAlloved	Método 405 não permitido
MissingContentLength	411 comprimento necessário
MissingRequestBodyError	400 pedido incorreto
MissingSecurityHeader	400 pedido incorreto
NoSuchBucket	404 não encontrado
NoSuchKey	404 não encontrado
NoSuchUpload	404 não encontrado
Sem Implementado	501 não implementado
NoSuchBucketPolicy	404 não encontrado
ObjectLockConfigurationNotFounError	404 não encontrado
Pré-condiçãoFailed	412 Pré-condição falhou
RequestTimeTooSwed	403 proibido
Serviço indisponível	503 Serviço indisponível
SignatureDoesNotMatch	403 proibido
TooManyBuckets	400 pedido incorreto

Nome	Status HTTP
UserKeyMustBeSpecified	400 pedido incorreto

Códigos de erro personalizados do StorageGRID

Nome	Descrição	Status HTTP
XBucketLifecycleNotAllowed	A configuração do ciclo de vida do bucket não é permitida em um bucket compatível com legado	400 pedido incorreto
XBucketPolicyParseException	Falha ao analisar JSON da política de bucket recebida.	400 pedido incorreto
XComplianceConflict	Operação negada devido às configurações de conformidade legadas.	403 proibido
XComplianceReducedRedundancyForbidden	Redundância reduzida não é permitida no bucket em conformidade com o legado	400 pedido incorreto
XMaxBucketPolicyLengthExceeded	Sua política excede o comprimento máximo permitido da política de intervalo.	400 pedido incorreto
XMissingInternalRequestHeader	Falta um cabeçalho de uma solicitação interna.	400 pedido incorreto
XNoSuchBucketCompliance	O bucket especificado não tem conformidade legada habilitada.	404 não encontrado
XNotAcceptable	A solicitação contém um ou mais cabeçalhos de aceitação que não puderam ser satisfeitos.	406 não aceitável
XNotImplementado	A solicitação que você forneceu implica funcionalidade que não é implementada.	501 não implementado

Informações sobre direitos autorais

Informações sobre marcas comerciais