Suporte para API REST do Amazon S3

StorageGRID software

NetApp
December 03, 2025

Índice

Suporte para API REST do Amazon S3

Detalhes da implementação da API REST S3

O sistema StorageGRID implementa a API do Simple Storage Service (versão da API 2006-03-01) com suporte para a maioria das operações e com algumas limitações. Você precisa entender os detalhes de implementação ao integrar aplicativos cliente da API REST do S3.

O sistema StorageGRID oferece suporte a solicitações no estilo de hospedagem virtual e solicitações no estilo de caminho.

Manuseio de data

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

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

Cabeçalhos de solicitação comuns

O sistema StorageGRID suporta os cabeçalhos de solicitação comuns definidos por "Referência da API do Amazon Simple Storage Service: Cabeçalhos de solicitação comuns" , com uma exceção.

Cabeçalho da solicitação	Implementação
Autorização	Suporte total para AWS Signature versão 2 Suporte para AWS Signature versão 4, com as seguintes exceções: • Quando você fornece o valor real da soma de verificação da carga útil em `x-amz-content-sha256` , o valor é aceito sem validação, como se o valor `UNSIGNED-PAYLOAD` tinha sido fornecido para o cabeçalho. Quando você fornece um `x-amz-content-sha256` valor do cabeçalho que implica `aws-chunked` streaming (por exemplo, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), as assinaturas dos blocos não são verificadas em relação aos dados dos blocos.
token de segurança x-amz	Não implementado. Devoluções `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 oferece suporte ao acesso autenticado e anônimo a objetos usando a API S3.

A API do S3 oferece suporte ao Signature versão 2 e ao Signature versão 4 para autenticação de solicitações da API do S3.

Solicitações autenticadas devem ser assinadas usando seu ID de chave de acesso e sua chave de acesso secreta.

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

Use o cabeçalho de autorização HTTP

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

Usar parâmetros de consulta

Você pode usar parâmetros de consulta para adicionar informações de autenticação a uma URL. Isso é conhecido como pré-assinatura de URL, que pode ser usado para conceder acesso temporário a recursos específicos. Usuários com a URL pré-assinada não precisam saber a chave de acesso secreta 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
ListBuckets (anteriormente chamado de Serviço GET)	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
Uso de armazenamento GET	O StorageGRID"Uso de armazenamento GET" A solicitação 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 armazenamento, sem fornecer credenciais de autenticação S3, para determinar se o nó de armazenamento está disponível. Você pode usar essa solicitação para monitoramento ou para permitir que balanceadores de carga externos identifiquem quando um nó de armazenamento está inativo.

Operações em baldes

O sistema StorageGRID suporta no máximo 5.000 buckets para cada conta de locatário do S3.

Cada grade pode ter no máximo 100.000 buckets.

Para dar suporte a 5.000 buckets, cada nó de armazenamento na grade deve ter no mínimo 64 GB de RAM.

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

Veja o seguinte para mais informações:

- "Guia do usuário do Amazon Simple Storage Service: cotas, restrições e limitações de bucket"
- "Configurar nomes de domínio de endpoint S3"

As operações ListObjects (GET Bucket) e ListObjectVersions (versões do objeto GET Bucket) oferecem suporte ao StorageGRID"valores de consistência" .

Você pode verificar se as atualizações do último horário de acesso estão habilitadas ou desabilitadas para buckets individuais. Ver "Último horário de acesso do Bucket GET" .

A tabela a seguir descreve como o StorageGRID implementa as operações de bucket da API REST do S3. Para executar qualquer uma dessas operações, é necessário fornecer as credenciais de acesso necessárias para a conta.

Operação	Implementação
CriarBucket	Cria um novo bucket. Ao criar o bucket, você se torna o proprietário do bucket. • Os nomes dos buckets devem obedecer às seguintes regras: ◦ Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário). ◦ Deve ser compatível com DNS. ◦ Deve conter no mínimo 3 e no máximo 63 caracteres. ◦ Pode ser uma série de um ou mais rótulos, com rótulos adjacentes separados por um ponto. Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hifens. ◦ Não deve parecer um endereço IP formatado em texto. ◦ Não deve usar pontos em solicitações de estilo de hospedagem virtual. Os períodos causarão problemas com a verificação do certificado curinga do servidor. • Por padrão, os buckets são criados no `us-east-1` região; no entanto, você pode usar o `LocationConstraint` elemento request 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 Grid Manager ou a Grid Management API. Entre em contato com o administrador do sistema se você não souber o nome da região que deve usar. **Observação**: Ocorrerá um erro se sua solicitação CreateBucket usar uma região que não foi definida em StorageGRID. • Você pode incluir o `x-amz-bucket-object-lock-enabled` cabeçalho de solicitação para criar um bucket com o S3 Object Lock habilitado. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3" . Você deve habilitar o S3 Object Lock ao criar o bucket. Não é possível adicionar ou desabilitar o S3 Object Lock após a criação de um bucket. O S3 Object Lock requer controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.
ExcluirBucket	Exclui o bucket.
ExcluirBucketCors	Exclui a configuração CORS do bucket.
DeleteBucketEncryption	Exclui a criptografia padrão do bucket. Os objetos criptografados existentes permanecem criptografados, mas quaisquer novos objetos adicionados ao bucket não são criptografados.
Ciclo de vida do DeleteBucket	Exclui a configuração do ciclo de vida do bucket. Ver "Criar configuração do ciclo de vida do S3" .

Operação	Implementação
Política de exclusão de balde	Exclui a política anexada ao bucket.
DeleteBucketReplication	Exclui a configuração de replicação anexada ao bucket.
ExcluirBucketTagging	Usa o `tagging` sub-recurso para remover todas as tags de um bucket. **Cuidado**: Se uma tag de política ILM não padrão for definida para este bucket, haverá um `NTAP-SG-ILM-BUCKET-TAG` tag de bucket com um valor atribuído a ela. Não emita uma solicitação DeleteBucketTagging se houver um `NTAP-SG-ILM-BUCKET-TAG` etiqueta de balde. Em vez disso, emita uma solicitação PutBucketTagging apenas com o `NTAP-SG-ILM-BUCKET-TAG` tag e seu valor atribuído para remover todas as outras tags do bucket. Não modifique ou remova o `NTAP-SG-ILM-BUCKET-TAG` etiqueta de balde.
ObterBucketAcl	Retorna uma resposta positiva e o ID, DisplayName e Permissão do proprietário do bucket, indicando que o proprietário tem acesso total ao bucket.
ObterBucketCors	Retorna o `cors` configuração para o bucket.
Obter criptografia do Bucket	Retorna a configuração de criptografia padrão para o bucket.
Obter configuração do ciclo de vida do Bucket (anteriormente chamado de ciclo de vida do GET Bucket)	Retorna a configuração do ciclo de vida do bucket. Ver "Criar configuração do ciclo de vida do S3" .
ObterBucketLocation	Retorna a região que foi definida usando o `LocationConstraint` elemento na solicitação CreateBucket. Se a região do balde for `us-east-1` , uma string vazia é retornada para a região.
Obter configuração de notificação de bucket (anteriormente chamado de notificação GET Bucket)	Retorna a configuração de notificação anexada ao bucket.
ObterBucketPolicy	Retorna a política anexada ao bucket.
Obter replicação do Bucket	Retorna a configuração de replicação anexada ao bucket.

Operação	Implementação
Obter marcação de balde	Usa o `tagging` sub-recurso para retornar todas as tags de um bucket. **Cuidado**: Se uma tag de política ILM não padrão for definida para este bucket, haverá um `NTAP-SG-ILM-BUCKET-TAG` tag de bucket com um valor atribuído a ela. Não modifique ou remova esta tag.
ObterVersionamento doBucket	Esta implementação utiliza o `versioning` sub-recurso para retornar o estado de controle de versão de um bucket. • *blank*: O controle de versão nunca foi habilitado (o bucket é "Sem versão") • Habilitado: o controle de versão está habilitado • Suspenso: o controle de versão foi habilitado anteriormente e está suspenso
ObterConfiguraçãoObject Lock	Retorna o modo de retenção padrão do bucket e o período de retenção padrão, se configurado. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3" .
Balde de cabeça	Determina se um bucket existe e se 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.
ListObjects e ListObjectsV2 (anteriormente chamado de GET Bucket)	Retorna alguns ou todos (até 1.000) objetos em um bucket. A classe de armazenamento para objetos pode ter um dos dois valores, mesmo que o objeto tenha sido ingerido com o `REDUCED_REDUNDANCY` opção de classe de armazenamento: • `STANDARD`, que indica que o objeto está armazenado em um pool de armazenamento composto por nós de armazenamento. • `GLACIER`, que indica que o objeto foi movido para o bucket externo especificado pelo Cloud Storage Pool. Se o bucket contiver um grande número de chaves excluídas com o mesmo prefixo, a resposta poderá incluir algumas `CommonPrefixes` que não contêm chaves.
Versões do objeto de lista (anteriormente chamadas de versões do objeto GET Bucket)	Com acesso READ em um bucket, usando esta operação com o `versions` subresource lista metadados de todas as versões de objetos no bucket.

Operação	Implementação
ColoqueBucketCors	Define a configuração CORS para um bucket para que o bucket possa atender a solicitações de origem cruzada. O compartilhamento de recursos entre origens (CORS) é um mecanismo de segurança que permite que aplicativos web clientes 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` bucket, você pode permitir que as imagens nesse bucket sejam exibidas no site `http://www.example.com` .
PutBucketEncryption	Define o estado de criptografia padrão de um bucket existente. Quando a criptografia em nível de bucket está habilitada, todos os novos objetos adicionados ao bucket são criptografados. O StorageGRID oferece suporte à criptografia do lado do servidor com chaves gerenciadas StorageGRID. Ao especificar a regra de configuração de criptografia do lado do servidor, defina o `SSEAlgorithm` parâmetro para `AES256` , e não use o `KMSMasterKeyID` parâmetro. A configuração de criptografia padrão do bucket será ignorada se a solicitação de upload do objeto já especificar a criptografia (ou seja, se a solicitação incluir o `x-amz-server-side-encryption-*` cabeçalho da solicitação).
Configuração do ciclo de vida do PutBucket (anteriormente chamado de ciclo de vida do PUT Bucket)	Cria uma nova configuração de ciclo de vida para o bucket ou substitui uma configuração de ciclo de vida existente. O StorageGRID suporta até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML: • Expiração (Dias, Data, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtro (Prefixo, Tag) • Status • EU IA O StorageGRID não oferece suporte a estas ações: • AbortarIncompletoMultipartUpload • Transição Ver "Criar configuração do ciclo de vida do S3" . Para entender como a ação Expiração em um ciclo de vida de bucket interage com as instruções de posicionamento do ILM, consulte"Como o ILM opera ao longo da vida de um objeto" . **Observação**: a configuração do ciclo de vida do bucket pode ser usada com buckets que tenham o S3 Object Lock habilitado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis legados.

Operação	Implementação

Configuração de notificação PutBucket
 	
(anteriormente chamado de notificação PUT Bucket)
	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 ao Amazon Simple Notification Service (Amazon SNS) ou a tópicos do Kafka como destinos. Os endpoints do Simple Queue Service (SQS) ou do Amazon Lambda não são suportados.
	• O destino das notificações deve ser especificado como o URN de um ponto de extremidade do StorageGRID . Os endpoints podem ser criados usando o Tenant Manager ou a Tenant Management API.
	
	O ponto de extremidade deve existir para que a configuração da notificação seja bem-sucedida. Se o ponto final 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 **não** são 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, conforme mostrado na lista a seguir:
	◦ **fonte do evento**
	
	`sgws:s3`
	
	◦ **Região aws**
	
	não incluído
	
	◦ **x-amz-id-2**
	
	não incluído
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	Define a política anexada ao bucket. Ver "Use políticas de acesso a buckets e grupos" .

Operação	Implementação
PutBucketReplicação	Configura"Replicação do StorageGRID CloudMirror" para o bucket usando o XML de configuração de replicação fornecido no corpo da solicitação. Para replicação do CloudMirror, você deve estar ciente dos seguintes detalhes de implementação: • O StorageGRID suporta apenas a V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue as convenções V1 para exclusão de versões de objetos. Para mais detalhes, veja "Guia do usuário do Amazon Simple Storage Service: configuração de replicação" . • A replicação de buckets pode ser configurada em buckets versionados ou não versionados. • Você pode especificar um bucket 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 o URN dos endpoints do StorageGRID , conforme especificado no Tenant Manager ou na Tenant Management API. Ver "Configurar a replicação do CloudMirror" . O ponto de extremidade deve existir para que a configuração da replicação seja bem-sucedida. Se o ponto final não existir, a solicitação falhará como um `400 Bad Request` . A mensagem de erro diz: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Você não precisa 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 o `STANDARD` classe de armazenamento por padrão. • Se você excluir um objeto do bucket de origem ou excluir o próprio bucket de origem, o comportamento de replicação entre regiões será o seguinte: ◦ Se você excluir o objeto ou bucket antes que ele seja replicado, o objeto/bucket não será replicado e você não será notificado. ◦ Se você excluir o objeto ou bucket após ele ter sido replicado, o StorageGRID seguirá o comportamento de exclusão padrão do Amazon S3 para a V1 da replicação entre regiões.

Operação	Implementação
Colocar marcação de balde	Usa o `tagging` sub-recurso para adicionar ou atualizar um conjunto de tags para um bucket. Ao adicionar tags de bucket, esteja ciente das seguintes limitações: • Tanto o StorageGRID quanto 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 caracteres Unicode de comprimento. • Os valores das tags podem ter até 256 caracteres Unicode. • Chaves e valores diferenciam maiúsculas de minúsculas. **Cuidado**: Se uma tag de política ILM não padrão for definida para este bucket, haverá um `NTAP-SG-ILM-BUCKET-TAG` tag de bucket com um valor atribuído a ela. Certifique-se de que o `NTAP-SG-ILM-BUCKET-TAG` A tag bucket é incluída com o valor atribuído em todas as solicitações PutBucketTagging. Não modifique ou remova esta tag. **Observação**: esta operação substituirá quaisquer tags atuais que o bucket já tenha. Se alguma tag existente for omitida do conjunto, essas tags serão removidas do bucket.
Versão PutBucket	Usa o `versioning` sub-recurso 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: habilita o controle de versão para os objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo. • Suspenso: desabilita o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão `null` .
PutObjectLockConfiguration	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 das versões de objetos existentes permanecerá a mesma e não será recalculada usando o novo período de retenção padrão. Ver"Use a API REST do S3 para configurar o bloqueio de objeto do S3" para informações detalhadas.

Operações em objetos

Operações em objetos

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

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

- StorageGRID"valores de consistência" são suportados por todas as operações em objetos, com exceção das seguintes:
  - ObterAclObjeto
  - `OPTIONS /`
  - ColocarObjetoLegalHold
  - ColocarRetençãoDeObjeto
  - SelecionarObjetoConteúdo
- Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.
- Todos os objetos em um bucket StorageGRID são de propriedade do proprietário do bucket, incluindo objetos criados por um usuário anônimo ou por outra conta.
- Objetos de dados ingeridos no sistema StorageGRID por meio do Swift não podem ser acessados pelo S3.

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

Operação	Implementação
ExcluirObjeto	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. Ao processar uma solicitação DeleteObject, o StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais armazenados. Se bem-sucedido, o StorageGRID retornará uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas em 30 segundos (por exemplo, porque um local está temporariamente indisponível), o StorageGRID enfileira as cópias para remoção e então indica o sucesso ao cliente. **Controle de versão** Para remover uma versão específica, o solicitante deve ser o proprietário do bucket e usar o `versionId` sub-recurso. Usar este sub-recurso exclui permanentemente a versão. Se o `versionId` corresponde a um marcador de exclusão, o cabeçalho de resposta `x-amz-delete-marker` é retornado definido para `true` . • Se um objeto for excluído sem o `versionId` sub-recurso em um bucket com controle de versão habilitado, isso resulta 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` o cabeçalho de resposta é retornado definido como `true` . • Se um objeto for excluído sem o `versionId` sub-recurso em um bucket com controle de versão suspenso, isso resulta em uma exclusão permanente de uma versão 'nula' já existente ou de um marcador de exclusão 'nulo' e na geração de um novo marcador de exclusão 'nulo'. O `x-amz-delete-marker` o cabeçalho de resposta é retornado definido como `true` . **Observação**: Em certos casos, podem existir vários marcadores de exclusão para um objeto. Ver"Use a API REST do S3 para configurar o bloqueio de objeto do S3" para aprender como excluir versões de objetos no modo GOVERNANCE.
ExcluirObjetos (anteriormente chamado de DELETE Multiple Objects)	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. Vários objetos podem ser excluídos na mesma mensagem de solicitação. Ver"Use a API REST do S3 para configurar o bloqueio de objeto do S3" para aprender como excluir versões de objetos no modo GOVERNANCE.

Operação	Implementação
ExcluirMarcaçãoDeObjeto	Usa o `tagging` sub-recurso para remover todas as tags de um objeto. **Controle de versão** Se o `versionId` se o parâmetro de consulta não for especificado na solicitação, a operação excluirá 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` .
ObterObjeto	"ObterObjeto"
ObterAclObjeto	Se as credenciais de acesso necessárias forem fornecidas para a conta, a operação retornará uma resposta positiva e o ID, o DisplayName e a Permissão do proprietário do objeto, indicando que o proprietário tem acesso total ao objeto.
ObterObjetoLegalHold	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"
ObterRetençãoDeObjeto	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"
Obter marcação de objeto	Usa o `tagging` sub-recurso para retornar todas as tags de um objeto. **Controle de versão** Se o `versionId` se o 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` .
CabeçaObjeto	"CabeçaObjeto"
RestaurarObjeto	"RestaurarObjeto"
ColocarObjeto	"ColocarObjeto"
CopiarObjeto (anteriormente chamado de Objeto PUT - Copiar)	"CopiarObjeto"
ColocarObjetoLegalHold	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"
ColocarRetençãoDeObjeto	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"

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

Use o S3 Select

O StorageGRID oferece suporte às seguintes cláusulas, tipos de dados e operadores do

Amazon S3 Select para o"Comando SelectObjectContent" .

Itens não listados não são suportados.

Para sintaxe, veja"SelecionarObjetoConteúdo" . Para obter mais informações sobre o S3 Select, consulte o "Documentação da AWS para S3 Select" .

Somente contas de locatários que tenham o S3 Select habilitado podem emitir consultas SelectObjectContent. Veja o"considerações e requisitos para usar o S3 Select" .

Cláusulas

- Lista SELECIONAR
- cláusula FROM
- Cláusula WHERE
- Cláusula LIMIT

Tipos de dados

- bool
- inteiro
- corda
- flutuador
- decimal, numérico
- carimbo de data/hora

Operadores

Operadores lógicos

- E
- NÃO
- OU

Operadores de comparação

- <
- >
- ⇐
- >=
- =
- =
- <>
- !=
- ENTRE

- EM

Operadores de correspondência de padrões

- COMO
- _
- %

Operadores unitários

- É NULO
- NÃO É NULO

Operadores matemáticos

- +
- -
- *
- /
- %

O StorageGRID segue a precedência do operador Amazon S3 Select.

Funções agregadas

- MÉDIA()
- CONTAR(*)
- MÁXIMO()
- MÍNIMO()
- SOMA()

Funções condicionais

- CASO
- COALESCE
- NULLIF

Funções de conversão

- CAST (para tipo de dados suportado)

Funções de data

- DATA_ADICIONADA
- DATA_DIFF
- EXTRAIR
- PARA_STRING

- PARA_CARIMBO_DE_HORA
- UTCNOW

Funções de string

- COMPRIMENTO_CARACTERE, COMPRIMENTO_CARACTERE
- MAIS BAIXO
- SUBSTRING
- APARAR
- SUPERIOR

Use criptografia do lado do servidor

A criptografia do lado do servidor permite que você proteja os dados do seu 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, poderá 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 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. Ao recuperar 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 os dados do objeto serão retornados.

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

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

> Se um objeto for criptografado com SSE ou SSE-C, todas as configurações de criptografia em nível de bucket ou de grade serão ignoradas.

Usar 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:

- "ColocarObjeto"

- "CopiarObjeto"
- "CriarMultipartUpload"

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

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

- "ObterObjeto"
- "CabeçaObjeto"
- "ColocarObjeto"
- "CopiarObjeto"
- "CriarMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

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

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

- Você deve usar https.

> O StorageGRID rejeita quaisquer solicitações feitas via http ao usar SSE-C. Por questões de segurança, considere que qualquer chave enviada acidentalmente via http estará comprometida. Descarte a chave e gire conforme apropriado.

- O ETag na resposta não é o MD5 dos dados do objeto.
- Você deve 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 o seu bucket tiver controle de versão habilitado, cada versão do objeto deverá 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, também deve gerenciar quaisquer proteções adicionais, como rotação de chaves, no lado do cliente.

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

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

Informações relacionadas

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

CopiarObjeto

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

Resolver conflitos

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

Tamanho do objeto

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

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

> Se você atualizou do StorageGRID 11.6 ou anterior, o alerta de tamanho de objeto S3 PUT muito grande será acionado se você tentar carregar um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11.7 ou 11.8, o alerta não será acionado neste caso. No entanto, para se alinhar ao padrão AWS S3, versões futuras do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

Caracteres UTF-8 em metadados do usuário

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

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

- As solicitações serão bem-sucedidas se os metadados definidos pelo usuário incluírem caracteres UTF-8 de escape.

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

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, seguido por um par nome-valor contendo metadados definidos pelo usuário
- `x-amz-metadata-directive`: O valor padrão é `COPY` , 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.

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

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular o modo de versão do objeto e reter até a data. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3" .

- Cabeçalhos de solicitação SSE:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

VerCabeçalhos 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-checksum-algorithm`

  Quando você copia um objeto, se o objeto de origem tiver uma soma de verificação, o StorageGRID não copia esse valor de soma de verificação para o novo objeto. Este comportamento se aplica independentemente de você tentar usar ou não `x-amz-checksum-algorithm` na solicitação do objeto.

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

Opções de classe de armazenamento

O `x-amz-storage-class` O cabeçalho de solicitação é suportado e afeta quantas cópias de objeto o StorageGRID cria se a regra ILM correspondente usa o Dual commit ou Balanced"opção de ingestão" .

- `STANDARD`

  (Padrão) Especifica uma operação de ingestão de confirmação dupla quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

- `REDUCED_REDUNDANCY`

  Especifica uma operação de ingestão de confirmação única quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

> ⓘ Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Usando x-amz-copy-source em CopyObject

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

Se a origem e o destino corresponderem, e o `x-amz-metadata-directive` cabeçalho é especificado como `REPLACE` , os metadados do objeto são atualizados com os valores de metadados fornecidos na solicitação. Nesse caso, o StorageGRID não ingere novamente o objeto. Isto tem duas consequências importantes:

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

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

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você"usar criptografia do lado do servidor" , os cabeçalhos de solicitação que você fornece 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 deverá incluir os três cabeçalhos a seguir na solicitação CopyObject para que o objeto possa ser descriptografado e copiado:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especifique `AES256` .
  - `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia que você forneceu quando 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`: Especifique `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Especifique uma nova chave de criptografia para o objeto de destino.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da nova chave de criptografia.

  > As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para"usando criptografia do lado do servidor" .
- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva gerenciada pelo StorageGRID (SSE), inclua este cabeçalho na solicitação CopyObject:
  - `x-amz-server-side-encryption`

  > O `server-side-encryption` o 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` sub-recurso. Se o bucket de destino for versionado, a versão gerada será retornada no `x-amz-version-id` cabeçalho de resposta. Se o controle de versão for suspenso para o bucket de destino, então `x-amz-version-id` retorna um valor "nulo".

ObterObjeto

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

GetObject e objetos multipartes

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

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

Caracteres UTF-8 em metadados do usuário

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

Cabeçalho de solicitação suportado

O seguinte cabeçalho de solicitação é suportado:

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

  O `Range` cabeçalho não é suportado com `x-amz-checksum-mode` para GetObject. Quando você inclui `Range` no pedido com `x-amz-checksum-mode` habilitado, o StorageGRID não retorna um valor de soma de verificação na resposta.

Cabeçalho de solicitação 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 buscará a versão mais recente do objeto em um bucket versionado. 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` .

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

Use todos os três cabeçalhos se o objeto estiver criptografado com uma chave exclusiva fornecida por você.

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

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

Comportamento de GetObject para objetos do Cloud Storage Pool

Se um objeto foi armazenado em um"Pool de armazenamento em nuvem" , o comportamento de uma solicitação GetObject depende do estado do objeto. Ver"CabeçaObjeto" para mais detalhes.

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

Estado do objeto	Comportamento de GetObject
Objeto ingerido no StorageGRID , mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de armazenamento tradicional ou usando codificação de eliminação	`200 OK` Uma cópia do objeto é recuperada.
Objeto no Cloud Storage Pool, mas ainda não transitado para um estado não recuperável	`200 OK` Uma cópia do objeto é recuperada.
Objeto transitado para um estado não recuperável	`403 Forbidden` , `InvalidObjectState` Use um"RestaurarObjeto" solicitação para restaurar o objeto a um estado recuperável.
Objeto em processo de restauração de um estado não recuperável	`403 Forbidden` , `InvalidObjectState` Aguarde a conclusão da solicitação RestoreObject.
Objeto totalmente restaurado no Cloud Storage Pool	`200 OK` Uma cópia do objeto é recuperada.

Objetos multipartes ou segmentados em um pool de armazenamento em nuvem

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

Nestes casos:

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

GetObject e replicação entre grades

Se você estiver usando"federação de grade" e"replicação entre grades" estiver habilitado para um bucket, o cliente S3 poderá verificar o status de replicação de um objeto emitindo uma solicitação GetObject. A resposta inclui o StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta, que terá um dos seguintes valores:

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

> ⓘ O StorageGRID não oferece suporte a `x-amz-replication-status` cabeçalho.

CabeçaObjeto

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

HeadObject e objetos multipartes

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

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

Caracteres UTF-8 em metadados do usuário

O StorageGRID não analisa nem interpreta caracteres UTF-8 de escape em metadados definidos pelo

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

Cabeçalho de solicitação suportado

O seguinte cabeçalho de solicitação é suportado:

- `x-amz-checksum-mode`

  O `partNumber` parâmetro e `Range` cabeçalho não é suportado com `x-amz-checksum-mode` para HeadObject. Quando você os inclui na solicitação com `x-amz-checksum-mode` habilitado, o StorageGRID não retorna um valor de soma de verificação na resposta.

Cabeçalho de solicitação 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 buscará a versão mais recente do objeto em um bucket versionado. 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` .

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

Use todos esses três cabeçalhos se o objeto estiver criptografado com uma chave exclusiva fornecida por você.

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

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

Respostas do HeadObject para objetos do Cloud Storage Pool

Se o objeto for armazenado em um"Pool de armazenamento em nuvem" , os seguintes cabeçalhos de resposta são 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 HeadObject
Objeto ingerido no StorageGRID , mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de armazenamento tradicional ou usando codificação de eliminação	`200 OK`(Nenhum cabeçalho de resposta especial é retornado.)

Objeto no Cloud Storage Pool, mas ainda não transitado 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` está definido para um tempo distante no futuro. O tempo exato da transição não é controlado pelo sistema StorageGRID .

O objeto passou para um 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` está definido para um tempo distante no futuro.
	
	Observação: Se a cópia na grade não estiver disponível (por exemplo, um nó de armazenamento estiver inativo), você deverá emitir uma"RestaurarObjeto" solicite a restauração da cópia do Cloud Storage Pool antes de poder recuperar o objeto com sucesso.

O objeto passou para um estado não recuperável e não há nenhuma cópia na grade	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Estado do objeto	Resposta ao HeadObject

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

Objeto totalmente restaurado no 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 Cloud Storage Pool será retornado a um estado não recuperável.

Objetos multipartes ou segmentados no Cloud Storage Pool

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

HeadObject e replicação entre grades

Se você estiver usando"federação de grade" e"replicação entre grades" estiver habilitado para um bucket, o cliente S3 poderá verificar o status de replicação de um objeto emitindo uma solicitação HeadObject. A resposta inclui o StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta, que terá um dos seguintes valores:

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

> ⓘ O StorageGRID não oferece suporte a `x-amz-replication-status` cabeçalho.

ColocarObjeto

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

Resolver conflitos

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

Tamanho do objeto

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

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

> Se você atualizou do StorageGRID 11.6 ou anterior, o alerta de tamanho de objeto S3 PUT muito grande será acionado se você tentar carregar um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11.7 ou 11.8, o alerta não será acionado neste caso. No entanto, para se alinhar ao padrão AWS S3, versões futuras do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

Tamanho dos metadados do usuário

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

Caracteres UTF-8 em metadados do usuário

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

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

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

Limites de tags de objeto

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

Propriedade do objeto

No StorageGRID, todos os objetos são de propriedade da conta do 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 do bloco.
  - O StorageGRID não verifica o valor que você fornece para `x-amz-decoded-content-length` contra o objeto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  A codificação de transferência em blocos é suportada se `aws-chunked` a assinatura de carga útil também é usada.

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

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

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

  Se você quiser usar a opção **Tempo de criação definido pelo usuário** como o 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 como segundos desde 1º de janeiro de 1970.

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

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

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular o modo de versão do objeto e reter até a data. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3" .
- Cabeçalhos de solicitação SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    VerCabeçalhos de solicitação para criptografia do lado do servidor

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

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

  O `x-amz-website-redirect-location` retornos de cabeçalho `XNotImplemented` .

Opções de classe de armazenamento

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

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

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

- `STANDARD`(Padrão)

- **Confirmação dupla**: se a regra do ILM especificar a opção Confirmação dupla para o comportamento de ingestão, assim que um objeto for ingerido, uma segunda cópia desse objeto será criada e distribuída para um nó de armazenamento diferente (confirmação dupla). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais atendem às instruções de posicionamento na regra. Caso contrário, talvez seja necessário fazer novas cópias de objetos em locais diferentes e as cópias provisórias iniciais talvez precisem ser excluídas.
- **Balanceado**: Se a regra do ILM especificar a opção Balanceado e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes Nós de Armazenamento.

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

- `REDUCED_REDUNDANCY`
  - **Confirmação dupla**: se a regra do ILM especificar a opção Confirmação dupla para o comportamento de ingestão, o StorageGRID criará uma única cópia provisória à medida que o objeto for ingerido (confirmação única).
  - **Balanceado**: Se a regra ILM especificar a opção Balanceado, 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. O `REDUCED_REDUNDANCY` A opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso usando `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia extra do objeto para cada operação de ingestão.

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

> Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se existir apenas uma cópia replicada de um objeto, esse objeto 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.

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

> Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará 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 seguintes cabeçalhos de solicitação para criptografar um objeto com criptografia do lado do servidor. As opções SSE e SSE-C são mutuamente exclusivas.

- **SSE**: Use o cabeçalho a seguir se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID.
  - `x-amz-server-side-encryption`

    Quando o `x-amz-server-side-encryption` o cabeçalho não está incluído na solicitação PutObject, a grade inteira"configuração de criptografia de objeto armazenado" é omitido da resposta PutObject.
- **SSE-C**: Use todos esses três cabeçalhos se quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
  - `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.

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

> Se um objeto for criptografado com SSE ou SSE-C, todas as configurações de criptografia em nível de bucket ou de grade serão ignoradas.

Controle de versão

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

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

Cálculos de assinatura para o cabeçalho de autorização

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

- StorageGRID não requer `host` cabeçalhos a serem incluídos dentro `CanonicalHeaders` .
- StorageGRID não requer `Content-Type` para ser incluído dentro `CanonicalHeaders` .
- StorageGRID não requer `x-amz-*` cabeçalhos a serem incluídos dentro `CanonicalHeaders` .

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

Para mais detalhes, consulte "Cálculos de assinatura para o cabeçalho de autorização: transferindo carga útil em um único bloco (AWS Signature versão 4)" .

Informações relacionadas

- "Gerenciar objetos com ILM"
- "Referência da API do Amazon Simple Storage Service: PutObject"

RestaurarObjeto

Você pode usar a solicitação S3 RestoreObject para restaurar um objeto armazenado em um pool de armazenamento em nuvem.

Tipo de solicitação suportado

O StorageGRID suporta apenas solicitações RestoreObject para restaurar um objeto. Não suporta o `SELECT` tipo de restauração. Selecione solicitações de retorno `XNotImplemented` .

Controle de versão

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

Comportamento de RestoreObject em objetos do Cloud Storage Pool

Se um objeto foi armazenado em um"Pool de armazenamento em nuvem" , uma solicitação RestoreObject tem o seguinte comportamento, com base no estado do objeto. Ver"CabeçaObjeto" para mais detalhes.

> Se um objeto estiver armazenado em um Cloud Storage Pool e uma ou mais cópias do objeto também existirem na grade, não haverá necessidade de restaurar o objeto emitindo uma solicitação RestoreObject. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação GetObject.

Estado do objeto	Comportamento de RestoreObject
Objeto ingerido no StorageGRID , mas ainda não avaliado pelo ILM, ou o objeto não está em um pool de armazenamento em nuvem	`403 Forbidden` , `InvalidObjectState`
Objeto no Cloud Storage Pool, mas ainda não transitado para um estado não recuperável	`200 OK`Nenhuma alteração é feita. **Nota**: Antes que um objeto seja transferido para um estado não recuperável, você não pode alterar sua `expiry-date` .

Estado do objeto	Comportamento de RestoreObject
Objeto transitado para um estado não recuperável	`202 Accepted`Restaura uma cópia recuperável do objeto para o Cloud Storage Pool pelo número de dias especificado no corpo da solicitação. No final desse período, o objeto é devolvido a um estado não recuperável. Opcionalmente, use o `Tier` elemento de solicitação para determinar quanto tempo o trabalho de restauração levará para terminar(`Expedited` , `Standard` , ou `Bulk`). Se você não especificar `Tier` , o `Standard` camada é usada. **Importante**: Se um objeto tiver sido transferido para o S3 Glacier Deep Archive ou o Cloud Storage Pool usar o armazenamento de Blobs do Azure, você não poderá 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 de um estado não recuperável	`409 Conflict` , `RestoreAlreadyInProgress`
Objeto totalmente restaurado no Cloud Storage Pool	`200 OK` **Observação:** Se um objeto foi restaurado para um estado recuperável, você pode alterá-lo `expiry-date` reemitindo a solicitação RestoreObject com um novo valor para `Days` . A data de restauração é atualizada em relação ao horário da solicitação.

SelecionarObjetoConteúdo

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

Para mais informações, consulte "Referência da API do Amazon Simple Storage Service: SelectObjectContent" .

Antes de começar

- A conta do locatário tem a permissão S3 Select.
- Você tem `s3:GetObject` permissão para o objeto que você deseja consultar.
- O objeto que você deseja consultar deve estar em um dos seguintes formatos:
  - **CSV**. Pode ser usado como está ou compactado em arquivos GZIP ou BZIP2.
  - **Parquet**. Requisitos adicionais para objetos Parquet:
    - O S3 Select suporta apenas compactação em colunas usando GZIP ou Snappy. O S3 Select não oferece suporte à compactação de objetos inteiros para objetos Parquet.
    - O S3 Select não suporta saída Parquet. Você deve especificar o formato de saída como CSV ou JSON.

        - O tamanho máximo do grupo de linhas descompactado é 512 MB.
        - Você deve usar os tipos de dados especificados no esquema do objeto.
        - Você não pode usar os tipos lógicos INTERVAL, JSON, LIST, TIME ou UUID.
- Sua expressão SQL tem um comprimento máximo de 256 KB.
- Qualquer registro na entrada ou nos resultados tem um comprimento máximo de 1 MiB.

Exemplo de sintaxe de solicitação CSV

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

Exemplo de sintaxe de solicitação Parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemplo de consulta SQL

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

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

As primeiras linhas do arquivo a ser consultado, `SUB-EST2020_ALL.csv` , fica 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 do AWS-CLI (CSV)

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

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

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Exemplo de uso do AWS-CLI (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

As primeiras linhas do arquivo de saída, changes.csv, se parecem com isto:

```
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 multipartes

Operações para uploads multipartes

Esta seção descreve como o StorageGRID oferece suporte a operações para uploads multipartes.

As seguintes condições e notas se aplicam a todas as operações de upload multipartes:

- Você não deve exceder 1.000 uploads multipartes simultâneos para um único bucket porque os resultados das consultas ListMultipartUploads para esse bucket podem retornar resultados incompletos.
- O StorageGRID impõe limites de tamanho da AWS para partes multipartes. Os clientes do S3 devem seguir estas diretrizes:
  - Cada parte em um upload multiparte deve ter 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 os maiores possíveis. Por exemplo, use tamanhos de peça de 5 GiB para um objeto de 100 GiB. Como cada parte é considerada um objeto único, o uso de tamanhos de parte grandes reduz a sobrecarga de metadados do StorageGRID .
  - Para objetos menores que 5 GiB, considere usar o upload não multiparte.
- O ILM é avaliado para cada parte de um objeto multiparte à medida que é ingerido e para o objeto como um todo quando o upload multiparte é concluído, se a regra ILM usar o Balanceado ou o Estrito"opção de ingestão" . Você deve estar ciente de como isso afeta o posicionamento de objetos e peças:
  - Se o ILM for alterado enquanto um upload multiparte do S3 estiver em andamento, algumas partes do objeto poderão não atender aos requisitos atuais do ILM quando o upload multiparte for concluído. Qualquer peça que não seja colocada corretamente é colocada na fila para reavaliação do ILM e

movida para o local correto posteriormente.

  - 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 do ILM para o objeto como um todo. Por exemplo, se uma regra especificar que todos os objetos de 10 GB ou maiores sejam armazenados no DC1, enquanto todos os objetos menores sejam armazenados no DC2, cada parte de 1 GB de um upload multiparte de 10 partes será armazenada no DC2 na ingestão. Entretanto, quando o ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.

- Todas as operações de upload multipartes oferecem suporte ao StorageGRID"valores de consistência" .
- Quando um objeto é ingerido usando upload multipartes, o"limite de segmentação de objetos (1 GiB)" não é aplicado.
- Conforme necessário, você pode usar"criptografia do lado do servidor" com uploads multipartes. Para usar SSE (criptografia do lado do servidor com chaves gerenciadas StorageGRID), você inclui o `x-amz-server-side-encryption` cabeçalho de solicitação somente na solicitação CreateMultipartUpload. Para usar SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente), especifique os mesmos três cabeçalhos de solicitação de chave de criptografia na solicitação CreateMultipartUpload e em cada solicitação UploadPart subsequente.

Operação	Implementação
AbortarMultipartUpload	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
Upload completo de várias partes	Ver"Upload completo de várias partes"
CriarMultipartUpload (anteriormente chamado de Iniciar Upload Multipartes)	Ver"CriarMultipartUpload"
ListarMultipartUploads	Ver"ListarMultipartUploads"
ListarPartes	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
UploadPart	Ver"UploadPart"
UploadPartCopy	Ver"UploadPartCopy"

Upload completo de várias partes

A operação CompleteMultipartUpload conclui um upload multiparte de um objeto reunindo as partes carregadas anteriormente.

> O StorageGRID suporta valores não consecutivos em ordem crescente para `partNumber` parâmetro de solicitação com CompleteMultipartUpload. O parâmetro pode começar com qualquer valor.

Resolver conflitos

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  O `x-amz-storage-class` cabeçalho afeta quantas cópias de objeto o StorageGRID cria se a regra ILM correspondente especificar o"Opção de confirmação dupla ou ingestão balanceada" .

- `STANDARD`

  (Padrão) Especifica uma operação de ingestão de confirmação dupla quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

- `REDUCED_REDUNDANCY`

  Especifica uma operação de ingestão de confirmação única quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

  > Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

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

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

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controle de versão

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

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

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

> Quando o controle de versão está habilitado para um bucket, a conclusão de um upload multiparte sempre cria uma nova versão, mesmo que haja uploads multiparte simultâneos concluídos na mesma chave de objeto. Quando o controle de versão não está habilitado para um bucket, é possível iniciar um upload multiparte e, em seguida, fazer com que outro upload multiparte seja iniciado e concluído primeiro na mesma chave de objeto. Em buckets não versionados, o upload multiparte concluído por último tem precedência.

Falha na replicação, notificação ou notificação de metadados

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

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

Consulte "Solucionar problemas de serviços de plataforma" .

CriarMultipartUpload

A operação CreateMultipartUpload (anteriormente chamada de Initiate Multipart Upload) inicia um upload multipart para um objeto e retorna um ID de upload.

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

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

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

- `STANDARD`(Padrão)
  - **Confirmação dupla**: se a regra do ILM especificar a opção de ingestão de confirmação dupla, assim que um objeto for ingerido, uma segunda cópia desse objeto será criada e distribuída para um nó de armazenamento diferente (confirmação dupla). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais atendem às instruções de posicionamento na regra. Caso contrário, talvez seja necessário fazer novas cópias de objetos em locais diferentes e as cópias provisórias iniciais talvez precisem ser excluídas.
  - **Balanceado**: Se a regra do ILM especificar a opção Balanceado e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes Nós de Armazenamento.

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

- `REDUCED_REDUNDANCY`
  - **Confirmação dupla**: se a regra do ILM especificar a opção Confirmação dupla, o StorageGRID criará uma única cópia provisória à medida que o objeto for ingerido (confirmação única).
  - **Balanceado**: Se a regra ILM especificar a opção Balanceado, 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. O `REDUCED_REDUNDANCY` A opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso usando `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia extra do objeto para cada operação de ingestão.

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

> Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se existir apenas uma cópia replicada de um objeto, esse objeto 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.

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

> Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Type`
- `x-amz-checksum-algorithm`

  Atualmente, apenas o valor SHA256 para `x-amz-checksum-algorithm` é suportado.

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

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

```
x-amz-meta-_name_: `value`
```

  Se você quiser usar a opção **Tempo de criação definido pelo usuário** como o 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 como segundos desde 1º de janeiro de 1970.

> Adicionando `creation-time` pois metadados definidos pelo usuário não são permitidos se você estiver adicionando um objeto a um bucket que tenha a Conformidade legada habilitada. Um erro será retornado.

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

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular a versão do objeto retain-until-date.

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

- Cabeçalhos de solicitação SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Cabeçalhos de solicitação para criptografia do lado do servidor

> Para obter informações sobre como o StorageGRID lida com caracteres UTF-8, consulte"ColocarObjeto" .

Cabeçalhos de solicitação para criptografia do lado do servidor

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

- **SSE**: Use o seguinte cabeçalho na solicitação CreateMultipartUpload se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações UploadPart.
  - `x-amz-server-side-encryption`
- **SSE-C**: Use todos esses três cabeçalhos na solicitação CreateMultipartUpload (e em cada solicitação UploadPart subsequente) se quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
  - `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256` .

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

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

Cabeçalhos de solicitação não suportados

O seguinte cabeçalho de solicitação não é suportado:

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

  O `x-amz-website-redirect-location` retornos de cabeçalho `XNotImplemented` .

Controle de versão

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

ListarMultipartUploads

A operação ListMultipartUploads lista uploads multipartes em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Controle de versão

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

UploadPart

A operação UploadPart carrega uma parte em um upload multiparte para um objeto.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação CreateMultipartUpload, também deverá incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPart:

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

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

Se você especificou uma soma de verificação SHA-256 durante a solicitação CreateMultipartUpload, também deverá incluir o seguinte cabeçalho de solicitação em cada solicitação UploadPart:

- `x-amz-checksum-sha256`: Especifique a soma de verificação SHA-256 para esta parte.

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controle de versão

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

UploadPartCopy

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

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

Esta solicitação lê e grava os dados do objeto especificados em `x-amz-copy-source-range` dentro do 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 CreateMultipartUpload, também deverá incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPartCopy:

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

Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deverá incluir os três cabeçalhos a seguir na solicitação UploadPartCopy para que o objeto possa ser descriptografado e copiado:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especifique `AES256` .
- `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia que você forneceu quando 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 fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em"Use criptografia do lado do servidor" .

Controle de versão

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

Respostas de erro

O sistema StorageGRID suporta todas as respostas de erro padrão da API REST do S3

aplicáveis. Além disso, a implementação do StorageGRID adiciona várias respostas personalizadas.

Códigos de erro da API S3 suportados

Nome	Status HTTP
Acesso negado	403 Proibido
BadDigest	400 Solicitação Inválida
BucketAlreadyExists	409 Conflito
BaldeNãoVazio	409 Conflito
Corpo Incompleto	400 Solicitação Inválida
Erro interno	Erro interno do servidor 500
Id de chave de acesso inválido	403 Proibido
Argumento inválido	400 Solicitação Inválida
Nome de Bucket inválido	400 Solicitação Inválida
Estado de Bucket inválido	409 Conflito
InvalidDigest	400 Solicitação Inválida
Erro de Algoritmo de Criptografia Inválido	400 Solicitação Inválida
Parte inválida	400 Solicitação Inválida
Pedido de peça inválido	400 Solicitação Inválida
Intervalo inválido	416 Intervalo solicitado não satisfatório
Solicitação inválida	400 Solicitação Inválida
Classe de armazenamento inválida	400 Solicitação Inválida
Tag inválida	400 Solicitação Inválida
URI inválido	400 Solicitação Inválida

Nome	Status HTTP
ChaveMuitoLonga	400 Solicitação Inválida
XML malformado	400 Solicitação Inválida
MetadadosMuitoGrandes	400 Solicitação Inválida
MétodoNãoPermitido	Método 405 não permitido
Comprimento do conteúdo ausente	411 Comprimento necessário
Erro de corpo de solicitação ausente	400 Solicitação Inválida
Cabeçalho de segurança ausente	400 Solicitação Inválida
NoSuchBucket	404 Não Encontrado
Nenhuma Chave	404 Não Encontrado
NoSuchUpload	404 Não Encontrado
Não implementado	501 Não Implementado
Política NoSuchBucket	404 Não Encontrado
Erro de configuração de bloqueio de objeto não encontrado	404 Não Encontrado
Pré-condição falhou	412 Pré-condição falhou
RequestTimeTooSkewed	403 Proibido
Serviço não disponível	503 Serviço indisponível
AssinaturaNãoCorresponde	403 Proibido
Muitos Baldes	400 Solicitação Inválida
UserKeyDeveSerEspecificado	400 Solicitação Inválida

Códigos de erro personalizados do StorageGRID

Nome	Descrição	Status HTTP
XBucketLifecycleNãoPermitido	A configuração do ciclo de vida do bucket não é permitida em um bucket compatível legado	400 Solicitação Inválida
XBucketPolicyParseException	Falha ao analisar o JSON da política de bucket recebida.	400 Solicitação Inválida
XComplianceConflito	Operação negada devido a configurações de conformidade legadas.	403 Proibido
XComplianceRedundância ReduzidaProibido	Redundância reduzida não é permitida no bucket compatível legado	400 Solicitação Inválida
Comprimento da política XMaxBucket excedido	Sua apólice excede o comprimento máximo permitido da apólice.	400 Solicitação Inválida
XMissingInternalRequestHeader	Falta um cabeçalho de uma solicitação interna.	400 Solicitação Inválida
Conformidade com XNoSuchBucket	O bucket especificado não tem a conformidade legada habilitada.	404 Não Encontrado
XNãoAceitável	A solicitação contém um ou mais cabeçalhos de aceitação que não puderam ser atendidos.	406 Não aceitável
XNãoImplementado	A solicitação que você forneceu implica uma funcionalidade que não está implementada.	501 Não Implementado

Informações sobre direitos autorais

Informações sobre marcas comerciais