Usar API REST do S3

StorageGRID software

NetApp
December 03, 2025

Índice

Usar API REST do S3

Versões e atualizações suportadas pela API REST do S3

O StorageGRID oferece suporte à API Simple Storage Service (S3), que é implementada como um conjunto de serviços web Representational State Transfer (REST).

O suporte para a API REST do S3 permite que você conecte aplicativos orientados a serviços desenvolvidos para serviços da Web do S3 com armazenamento de objetos local que usa o sistema StorageGRID . São necessárias alterações mínimas no uso atual de chamadas da API REST do S3 por um aplicativo cliente.

Versões suportadas

O StorageGRID suporta as seguintes versões específicas do S3 e HTTP.

Item	Versão
Especificação da API S3	"Documentação da Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service"
HTTP	1,1 Para obter mais informações sobre HTTP, consulte HTTP/1.1 (RFCs 7230-35). "IETF RFC 2616: Protocolo de Transferência de Hipertexto (HTTP/1.1)" **Observação**: O StorageGRID não oferece suporte a pipeline HTTP/1.1.

Atualizações no suporte à API REST do S3

Liberar	Comentários
11,9	• Adicionado suporte para valores de soma de verificação SHA-256 pré-calculados para as seguintes solicitações e cabeçalhos suportados. Você pode usar este recurso para verificar a integridade dos objetos enviados: ◦ Upload completo de várias partes: `x-amz-checksum-sha256` ◦ CriarMultipartUpload: `x-amz-checksum-algorithm` ◦ ObterObjeto: `x-amz-checksum-mode` ◦ HeadObject: `x-amz-checksum-mode` ◦ ListarPartes ◦ ColocarObjeto: `x-amz-checksum-sha256` ◦ UploadPart: `x-amz-checksum-sha256` • Foi adicionada a capacidade do administrador da grade de controlar as configurações de conformidade e retenção no nível do locatário. Essas configurações afetam as configurações de bloqueio de objeto do S3. ◦ Modo de retenção padrão do bucket e modo de retenção de objeto: Governança ou Conformidade, se permitido pelo administrador da grade. ◦ Período de retenção padrão do bucket e data de retenção do objeto: deve ser menor ou igual ao permitido pelo período máximo de retenção definido pelo administrador da grade. • Suporte aprimorado para `aws-chunked` codificação e streaming de conteúdo `x-amz-content-sha256` valores. Limitações: ◦ Se presente, `chunk-signature` é opcional e não validado ◦ Se presente, `x-amz-trailer` o conteúdo é ignorado
11,8	Atualizou os nomes das operações do S3 para corresponder aos nomes usados no "Documentação da Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service" .
11,7	• Adicionado"Referência rápida: solicitações de API do S3 suportadas" . • Adicionado suporte para usar o modo GOVERNANCE com o S3 Object Lock. • Adicionado suporte para StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta para solicitações GET Object e HEAD Object. Este cabeçalho fornece o status de replicação de um objeto para replicação entre grades. • Solicitações SelectObjectContent agora oferecem suporte a objetos Parquet.

Liberar	Comentários
11,6	• Adicionado suporte para usar o `partNumber` parâmetro de solicitação em solicitações GET Object e HEAD Object. • Adicionado suporte para um modo de retenção padrão e um período de retenção padrão no nível do bucket para o S3 Object Lock. • Adicionado suporte para o `s3:object-lock-remaining-retention-days` chave de condição de política para definir o intervalo de períodos de retenção permitidos para seus objetos. • Foi alterado o tamanho máximo *recomendado* para uma única operação PUT Object para 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multiparte.
11,5	• Adicionado suporte para gerenciamento de criptografia de bucket. • Suporte adicionado para bloqueio de objeto S3 e solicitações de conformidade legadas obsoletas. • Adicionado suporte para usar DELETE Multiple Objects em buckets versionados. • O `Content-MD5` O cabeçalho da solicitação agora é suportado corretamente.
11,4	• Adicionado suporte para marcação de Bucket DELETE, marcação de Bucket GET e marcação de Bucket PUT. Tags de alocação de custos não são suportadas. • Para buckets criados no StorageGRID 11.4, não é mais necessário restringir nomes de chaves de objeto para atender às práticas recomendadas de desempenho. • Adicionado suporte para notificações de bucket no `s3:ObjectRestore:Post` tipo de evento. • Os limites de tamanho da AWS para partes multipartes agora são aplicados. Cada parte em um upload multiparte deve ter entre 5 MiB e 5 GiB. A última parte pode ser menor que 5 MiB. • Adicionado suporte para TLS 1.3
11,3	• Adicionado suporte para criptografia do lado do servidor de dados de objetos com chaves fornecidas pelo cliente (SSE-C). • Adicionado suporte para operações de ciclo de vida de bucket DELETE, GET e PUT (somente ação de expiração) e para `x-amz-expiration` cabeçalho de resposta. • Objeto PUT atualizado, Objeto PUT - Cópia e Upload Multipartes para descrever o impacto das regras do ILM que usam posicionamento síncrono na ingestão. • As cifras TLS 1.1 não são mais suportadas.

Liberar	Comentários
11,2	Adicionado suporte para restauração de objetos POST para uso com pools de armazenamento em nuvem. Adicionado suporte para usar a sintaxe da AWS para ARN, chaves de condição de política e variáveis de política em políticas de grupo e bucket. As políticas de grupo e bucket existentes que usam a sintaxe StorageGRID continuarão a ser suportadas. **Observação:** Os usos de ARN/URN em outras configurações JSON/XML, incluindo aqueles usados em recursos personalizados do StorageGRID , não foram alterados.
11,1	Adicionado suporte para compartilhamento de recursos entre origens (CORS), HTTP para conexões de cliente S3 com nós de grade e configurações de conformidade em buckets.
11,0	Adicionado suporte para configuração de serviços de plataforma (replicação do CloudMirror, notificações e integração de pesquisa do Elasticsearch) para buckets. Também foi adicionado suporte para restrições de localização de marcação de objetos para buckets e consistência disponível.
10,4	Adicionado suporte para alterações de verificação de ILM no controle de versão, atualizações da página Nomes de Domínio de Endpoint, condições e variáveis em políticas, exemplos de políticas e a permissão PutOverwriteObject.
10,3	Adicionado suporte para controle de versão.
10,2	Adicionado suporte para políticas de acesso de grupo e bucket, e para cópia multiparte (Upload Part - Copy).
10,1	Adicionado suporte para upload multiparte, solicitações de estilo de hospedagem virtual e autenticação v4.
10,0	Suporte inicial da API REST do S3 pelo sistema StorageGRID . A versão atualmente suportada da *Simple Storage Service API Reference* é 2006-03-01.

Referência rápida: solicitações de API do S3 suportadas

Esta página resume como o StorageGRID oferece suporte às APIs do Amazon Simple Storage Service (S3).

Esta página inclui apenas as operações do S3 suportadas pelo StorageGRID.

Para ver a documentação da AWS para cada operação, selecione o link no título.

Parâmetros de consulta URI comuns e cabeçalhos de solicitação

A menos que indicado, os seguintes parâmetros comuns de consulta de URI são suportados:

- `versionId`(conforme necessário para operações de objeto)

A menos que indicado, os seguintes cabeçalhos de solicitação comuns são suportados:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informações relacionadas

- "Detalhes da implementação da API REST S3"
- "Referência da API do Amazon Simple Storage Service: Cabeçalhos de solicitação comuns"

"AbortarMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, mais este parâmetro de consulta URI adicional:

- `uploadId`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações para uploads multipartes"

"Upload completo de várias partes"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, mais este parâmetro de consulta URI adicional:

- `uploadId`
- `x-amz-checksum-sha256`

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`

- `Part`
- `PartNumber`

Documentação do StorageGRID

"Upload completo de várias partes"

"CopiarObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes cabeçalhos adicionais:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `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-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"CopiarObjeto"

"CriarBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes cabeçalhos adicionais:

- `x-amz-bucket-object-lock-enabled`

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em baldes"

"CriarMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes cabeçalhos adicionais:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"CriarMultipartUpload"

"ExcluirBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Documentação do StorageGRID

"Operações em baldes"

"ExcluirBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"DeleteBucketEncryption"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Ciclo de vida do DeleteBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

- "Operações em baldes"
- "Criar configuração do ciclo de vida do S3"

"Política de exclusão de balde"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"DeleteBucketReplication"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ExcluirBucketTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ExcluirObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, mais este cabeçalho de solicitação adicional:

- `x-amz-bypass-governance-retention`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"ExcluirObjetos"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, mais este cabeçalho de solicitação adicional:

- `x-amz-bypass-governance-retention`

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em objetos"

"ExcluirMarcaçãoDeObjeto"

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"ObterBucketAcl"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ObterBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Obter criptografia do Bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Obter configuração do ciclo de vida do Bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

- "Operações em baldes"
- "Criar configuração do ciclo de vida do S3"

"ObterBucketLocation"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Obter configuração de notificação de bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ObterBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Obter replicação do Bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Obter marcação de balde"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ObterVersionamento doBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ObterObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

E estes cabeçalhos de solicitação adicionais:

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`

- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"ObterObjeto"

"ObterAclObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"ObterObjetoLegalHold"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

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

"ObterConfiguraçãoObjectLock"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

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

"ObterRetençãoDeObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

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

"Obter marcação de objeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"Balde de cabeça"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"CabeçaObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes cabeçalhos adicionais:

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

- `Range`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"CabeçaObjeto"

"ListBuckets"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

Operações no serviço › ListBuckets

"ListarMultipartUploads"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

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

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"ListarMultipartUploads"

"Objetos de Lista"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`

- `prefix`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ListObjectsV2"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Versões do objeto de lista"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ListarPartes"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

- `max-parts`
- `part-number-marker`
- `uploadId`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"ListarMultipartUploads"

"ColoqueBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em baldes"

"PutBucketEncryption"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

Documentação do StorageGRID

"Operações em baldes"

"Configuração do ciclo de vida do PutBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- `And`
- `Days`
- `Expiration`
- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

Documentação do StorageGRID

- "Operações em baldes"
- "Criar configuração do ciclo de vida do S3"

"Configuração de notificação PutBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- `Event`
- `Filter`
- `FilterRule`
- `Id`

- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

Documentação do StorageGRID

"Operações em baldes"

"PutBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Para obter detalhes sobre os campos de corpo JSON suportados, consulte"Use políticas de acesso a buckets e grupos" .

"PutBucketReplicação"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Tags XML do corpo da solicitação

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

Documentação do StorageGRID

"Operações em baldes"

"Colocar marcação de balde"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em baldes"

"Versão PutBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Parâmetros do corpo da solicitação

O StorageGRID suporta estes parâmetros do corpo da solicitação:

- `VersioningConfiguration`
- `Status`

Documentação do StorageGRID

"Operações em baldes"

"ColocarObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes cabeçalhos adicionais:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corpo da solicitação

- Dados binários do objeto

Documentação do StorageGRID

"ColocarObjeto"

"ColocarObjetoLegalHold"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

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

"PutObjectLockConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

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

"ColocarRetençãoDeObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, mais este cabeçalho adicional:

- `x-amz-bypass-governance-retention`

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

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

"Colocar marcação de objeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em objetos"

"RestaurarObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Para obter detalhes sobre os campos corporais suportados, consulte"RestaurarObjeto" .

"SelecionarObjetoConteúdo"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Para obter detalhes sobre os campos corporais suportados, consulte o seguinte:

- "Use o S3 Select"
- "SelecionarObjetoConteúdo"

"UploadPart"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `partNumber`
- `uploadId`

E estes cabeçalhos de solicitação adicionais:

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corpo da solicitação

- Dados binários da peça

Documentação do StorageGRID

"UploadPart"

"UploadPartCopy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `partNumber`
- `uploadId`

E estes cabeçalhos de solicitação adicionais:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `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`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"UploadPartCopy"

Testar configuração da API REST do S3

Você pode usar a Amazon Web Services Command Line Interface (AWS CLI) para testar sua conexão com o sistema e verificar se você consegue ler e gravar objetos.

Antes de começar

- Você baixou e instalou o AWS CLI de "aws.amazon.com/cli" .
- Opcionalmente, você tem"criou um ponto de extremidade do balanceador de carga" . Caso contrário, você sabe o endereço IP do nó de armazenamento ao qual deseja se conectar e o número da porta a ser usada. Ver "Endereços IP e portas para conexões de clientes" .
- Você tem"criou uma conta de locatário S3" .
- Você fez login no inquilino e"criou uma chave de acesso" .

Para obter detalhes sobre essas etapas, consulte"Configurar conexões do cliente" .

Passos

1. Configure as definições da AWS CLI para usar a conta que você criou no sistema StorageGRID :
   a. Entrar no modo de configuração: `aws configure`
   b. Digite o ID da chave de acesso da conta que você criou.
   c. Digite a chave de acesso secreta da conta que você criou.
   d. Digite a região padrão a ser usada. Por exemplo, `us-east-1` .
   e. Digite o formato de saída padrão a ser usado ou pressione **Enter** para selecionar JSON.
2. Crie um bucket.

   Este exemplo pressupõe que você configurou um ponto de extremidade do balanceador de carga para usar o endereço IP 10.96.101.17 e a porta 10443.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   Se o bucket for criado com sucesso, o local do bucket será retornado, conforme visto no exemplo a seguir:

   ```
   "Location": "/testbucket"
   ```

3. Carregar um objeto.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   put-object --bucket testbucket --key s3.pdf --body C:\s3-
   test\upload\s3.pdf
   ```

   Se o objeto for carregado com sucesso, uma Etag será retornada, que é um hash dos dados do objeto.

4. Liste o conteúdo do bucket para verificar se o objeto foi carregado.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   list-objects --bucket testbucket
   ```

5. Exclua o objeto.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   delete-object --bucket testbucket --key s3.pdf
   ```

6. Exclua o bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Como o StorageGRID implementa a API REST do S3

Solicitações conflitantes de clientes

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.

Valores de consistência

A consistência fornece um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de armazenamento e sites. Você pode alterar a consistência conforme exigido pelo seu aplicativo.

Por padrão, o StorageGRID garante consistência de leitura após gravação para objetos recém-criados. Qualquer GET após um PUT concluído com sucesso poderá ler os dados recém-gravados. Substituições de objetos existentes, atualizações de metadados e exclusões são eventualmente consistentes. As substituições geralmente levam segundos ou minutos para se propagar, mas podem levar até 15 dias.

Se você quiser executar operações de objeto com uma consistência diferente, você pode:

- Especifique uma consistência paracada balde .
- Especifique uma consistência paracada operação de API .
- Altere a consistência padrão em toda a grade executando uma das seguintes tarefas:
  - No Grid Manager, vá para **CONFIGURAÇÃO** > **Sistema** > **Configurações de armazenamento** > **Consistência padrão**.
  - .

> Uma alteração na consistência de toda a grade se aplica somente aos buckets criados após a configuração ter sido alterada. Para determinar os detalhes de uma alteração, consulte o log de auditoria localizado em `/var/local/log` (pesquise por **consistencyLevel**).

Valores de consistência

A consistência afeta como os metadados que o StorageGRID usa para rastrear objetos são distribuídos entre os nós e, portanto, a disponibilidade dos objetos para solicitações do cliente.

Você pode definir a consistência de um bucket ou de uma operação de API para um dos seguintes valores:

- **Todos**: Todos os nós recebem os dados imediatamente, ou a solicitação falhará.

- **Strong-global**: Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
- **Strong-site**: Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.
- **Leitura após nova gravação**: (Padrão) Fornece consistência de leitura após gravação para novos objetos e consistência eventual para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
- **Disponível**: Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que raramente são lidos ou para operações HEAD ou GET em chaves que não existem). Não suportado para buckets do S3 FabricPool .

Use a consistência "Leitura após nova gravação" e "Disponível"

Quando uma operação HEAD ou GET usa a consistência "Leitura após nova gravação", o StorageGRID executa a pesquisa em várias etapas, da seguinte maneira:

- Primeiro, ele procura o objeto usando uma consistência baixa.
- Se essa pesquisa falhar, ela será repetida no próximo valor de consistência até atingir uma consistência equivalente ao comportamento de strong-global.

Se uma operação HEAD ou GET usar a consistência "Leitura após nova gravação", mas o objeto não existir, a pesquisa de objetos sempre alcançará uma consistência equivalente ao comportamento de strong-global. Como essa consistência exige que várias cópias dos metadados do objeto estejam disponíveis em cada site, você poderá receber um alto número de erros 500 do servidor interno se dois ou mais nós de armazenamento no mesmo site estiverem indisponíveis.

A menos que você precise de garantias de consistência semelhantes às do Amazon S3, você pode evitar esses erros para operações HEAD e GET definindo a consistência como "Disponível". Quando uma operação HEAD ou GET usa a consistência "Disponível", o StorageGRID fornece apenas consistência eventual. Ele não tenta novamente uma operação com falha para aumentar a consistência, portanto, não exige que várias cópias dos metadados do objeto estejam disponíveis.

Especificar consistência para operação de API

Para definir a consistência de uma operação de API individual, os valores de consistência devem ser suportados para a operação e você deve especificar a consistência no cabeçalho da solicitação. Este exemplo define a consistência como "Strong-site" para uma operação GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

Você deve usar a mesma consistência para as operações PutObject e GetObject.

Especificar consistência para bucket

Para definir a consistência do bucket, você pode usar o StorageGRID"Consistência do balde PUT" solicitar. Ou você pode"alterar a consistência de um balde" do gerente do inquilino.

Ao definir a consistência de um bucket, esteja ciente do seguinte:

- Definir a consistência de um bucket determina qual consistência será usada para operações do S3 executadas nos objetos no bucket ou na configuração do bucket. Não afeta as operações no próprio bucket.
- A consistência de uma operação de API individual substitui a consistência do bucket.
- Em geral, os buckets devem usar a consistência padrão, "Leitura após nova gravação". Se as solicitações não estiverem funcionando corretamente, altere o comportamento do cliente do aplicativo, se possível. Ou configure o cliente para especificar a consistência para cada solicitação de API. Defina a consistência no nível do bucket somente como último recurso.

Como a consistência e as regras de ILM interagem para afetar a proteção de dados

Tanto sua escolha de consistência quanto sua regra de ILM afetam como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, a consistência usada quando um objeto é armazenado afeta o posicionamento inicial dos metadados do objeto, enquanto o comportamento de ingestão selecionado para a regra ILM afeta o posicionamento inicial das cópias do objeto. Como o StorageGRID requer acesso aos metadados de um objeto e seus dados para atender às solicitações do cliente, selecionar níveis correspondentes de proteção para consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas do sistema mais previsíveis.

A seguir"opções de ingestão" estão disponíveis para regras ILM:

Comprometimento duplo
: O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

Estrito
: Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja retornado ao cliente.

Equilibrado
: O StorageGRID tenta fazer todas as cópias especificadas na regra ILM na ingestão; se isso não for possível, cópias provisórias são feitas e o sucesso é retornado ao cliente. As cópias especificadas na regra ILM são feitas quando possível.

Exemplo de como a consistência e a regra ILM podem interagir

Suponha que você tenha uma grade de dois sites com a seguinte regra ILM e a seguinte consistência:

- **Regra do ILM**: Crie duas cópias de objetos, uma no site local e outra em um site remoto. Use o comportamento de ingestão estrito.
- **consistência**: Forte-global (os metadados do objeto são imediatamente distribuídos para todos os sites).

Quando um cliente armazena um objeto na grade, o StorageGRID faz cópias do objeto e distribui metadados para ambos os sites antes de retornar o sucesso ao cliente.

O objeto é totalmente protegido contra perda no momento da ingestão bem-sucedida da mensagem. Por exemplo, se o site local for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existirão no site remoto. O objeto é totalmente recuperável.

Se, em vez disso, você usasse a mesma regra de ILM e a consistência de site forte, o cliente poderia receber uma mensagem de sucesso depois que os dados do objeto fossem replicados para o site remoto, mas antes que os metadados do objeto fossem distribuídos lá. Nesse caso, o nível de proteção dos metadados do objeto não corresponde ao nível de proteção dos dados do objeto. Se o site local for perdido logo após a ingestão, os metadados do objeto serão perdidos. O objeto não pode ser recuperado.

A inter-relação entre consistência e regras de ILM pode ser complexa. Entre em contato com a NetApp se precisar de assistência.

Controle de versão de objetos

Você pode definir o estado de controle de versão de um bucket se quiser manter várias versões de cada objeto. Habilitar o controle de versão para um bucket pode ajudar a proteger contra a exclusão acidental de objetos e permite que você recupere e restaure versões anteriores de um objeto.

O sistema StorageGRID implementa o controle de versão com suporte para a maioria dos recursos e com algumas limitações. O StorageGRID suporta até 10.000 versões de cada objeto.

O controle de versão de objetos pode ser combinado com o gerenciamento do ciclo de vida das informações (ILM) do StorageGRID ou com a configuração do ciclo de vida do bucket do S3. Você deve habilitar explicitamente o controle de versão para cada bucket. Quando o controle de versão é habilitado para um bucket, cada objeto adicionado ao bucket recebe um ID de versão, que é gerado pelo sistema StorageGRID .

O uso de MFA (autenticação multifator) não é suportado.

> O controle de versão pode ser habilitado somente em buckets criados com o StorageGRID versão 10.3 ou posterior.

ILM e controle de versão

As políticas de ILM são aplicadas a cada versão de um objeto. Um processo de verificação de ILM verifica continuamente todos os objetos e os reavalia em relação à política de ILM atual. Quaisquer alterações feitas nas políticas do ILM serão aplicadas a todos os objetos ingeridos anteriormente. Isso inclui versões ingeridas anteriormente se o controle de versão estiver habilitado. A verificação de ILM aplica novas alterações de ILM a objetos ingeridos anteriormente.

Para objetos S3 em buckets habilitados para controle de versão, o suporte ao controle de versão permite que você crie regras ILM que usam "Tempo não atual" como o Tempo de referência (selecione **Sim** para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas?" em"Etapa 1 do assistente Criar uma regra ILM"). Quando um objeto é atualizado, suas versões anteriores se tornam obsoletas. Usar um filtro "Tempo não atual" permite criar políticas que reduzem o impacto de armazenamento de versões anteriores de objetos.

> Ao carregar uma nova versão de um objeto usando uma operação de upload multipartes, o tempo não atual para a versão original do objeto reflete quando o upload multipartes foi criado para a nova versão, não quando o upload multipartes foi concluído. Em casos limitados, o horário não atual da versão original pode ser horas ou dias anterior ao horário da versão atual.

Informações relacionadas

- "Como objetos versionados do S3 são excluídos"
- "Regras e políticas do ILM para objetos versionados do S3 (Exemplo 4)" .

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

Se a configuração global do S3 Object Lock estiver habilitada para seu sistema StorageGRID , você poderá criar buckets com o S3 Object Lock habilitado. Você pode especificar a retenção padrão para cada bucket ou configurações de retenção para cada versão do objeto.

Como habilitar o bloqueio de objeto S3 para um bucket

Se a configuração global S3 Object Lock estiver habilitada para seu sistema StorageGRID , você poderá habilitar o S3 Object Lock ao criar cada bucket.

O bloqueio de objeto do S3 é uma configuração permanente que só pode ser ativada quando você cria um bucket. Não é possível adicionar ou desabilitar o S3 Object Lock após a criação de um bucket.

Para habilitar o bloqueio de objeto S3 para um bucket, use um destes métodos:

- Crie o bucket usando o Tenant Manager. Ver "Criar bucket S3" .
- Crie o bucket usando uma solicitação CreateBucket com o `x-amz-bucket-object-lock-enabled` cabeçalho da solicitação. Ver "Operações em baldes" .

O S3 Object Lock requer controle de versão do bucket, que é ativado automaticamente quando o bucket é criado. Não é possível suspender o controle de versão do bucket. Ver "Controle de versão de objetos" .

Configurações de retenção padrão para um bucket

Quando o Bloqueio de Objeto S3 estiver habilitado para um bucket, você poderá, opcionalmente, habilitar a retenção padrão para o bucket e especificar um modo de retenção padrão e um período de retenção padrão.

Modo de retenção padrão

- No modo CONFORMIDADE:
  - O objeto não pode ser excluído até que sua data de retenção seja atingida.
  - A data de retenção do objeto pode ser aumentada, mas não diminuída.
  - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- No modo GOVERNANÇA:
  - Usuários com o `s3:BypassGovernanceRetention` permissão pode usar o `x-amz-bypass-governance-retention: true` cabeçalho de solicitação para ignorar as configurações de retenção.
  - Esses usuários podem excluir uma versão do objeto antes que sua data de retenção seja atingida.
  - Esses usuários podem aumentar, diminuir ou remover a data de retenção de um objeto.

Período de retenção padrão

Cada bucket pode ter um período de retenção padrão especificado em anos ou dias.

Como definir a retenção padrão para um bucket

Para definir a retenção padrão para um bucket, use um destes métodos:

- Gerencie as configurações do bucket no Gerenciador de locatários. Ver"Criar um bucket S3" e"Atualizar retenção padrão do bloqueio de objeto S3" .
- Emita uma solicitação PutObjectLockConfiguration para o bucket para especificar o modo padrão e o número padrão de dias ou anos.

PutObjectLockConfiguration

A solicitação PutObjectLockConfiguration permite que você defina e modifique o modo de retenção padrão e o período de retenção padrão para um bucket que tenha o S3 Object Lock habilitado. Você também pode remover as configurações de retenção padrão configuradas anteriormente.

Quando novas versões de objetos são ingeridas no bucket, o modo de retenção padrão é aplicado se `x-amz-object-lock-mode` e `x-amz-object-lock-retain-until-date` não são especificados. O período de retenção padrão é usado para calcular a data de retenção se `x-amz-object-lock-retain-until-date` não é especificado.

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

Você deve ter o `s3:PutBucketObjectLockConfiguration` permissão, ou ser root da conta, para concluir esta operação.

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

Exemplo de solicitação

Este exemplo habilita o S3 Object Lock para um bucket e define o modo de retenção padrão como COMPLIANCE e o período de retenção padrão como 6 anos.

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

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

Como determinar a retenção padrão para um bucket

Para determinar se o S3 Object Lock está habilitado para um bucket e para ver o modo de retenção padrão e o período de retenção, use um destes métodos:

- Visualize o bucket no Gerenciador de locatários. Ver "Exibir buckets S3" .
- Emita uma solicitação GetObjectLockConfiguration.

ObterConfiguraçãoObjectLock

A solicitação GetObjectLockConfiguration permite que você determine se o S3 Object Lock está habilitado para um bucket e, se estiver, veja se há um modo de retenção padrão e um período de retenção configurados para o bucket.

Quando novas versões de objetos são ingeridas no bucket, o modo de retenção padrão é aplicado se `x-amz-object-lock-mode` não é especificado. O período de retenção padrão é usado para calcular a data de retenção se `x-amz-object-lock-retain-until-date` não é especificado.

Você deve ter o `s3:GetBucketObjectLockConfiguration` permissão, ou ser root da conta, para concluir esta operação.

Exemplo de solicitação

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

Exemplo de resposta

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

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

Como especificar configurações de retenção para um objeto

Um bucket com o S3 Object Lock ativado pode conter uma combinação de objetos com e sem configurações de retenção do S3 Object Lock.

As configurações de retenção no nível do objeto são especificadas usando a API REST do S3. As configurações de retenção de um objeto substituem quaisquer configurações de retenção padrão do bucket.

Você pode especificar as seguintes configurações para cada objeto:

- **Modo de retenção**: CONFORMIDADE ou GOVERNANÇA.
- **Retain-until-date**: Uma data que especifica por quanto tempo a versão do objeto deve ser retida pelo StorageGRID.
    - No modo CONFORMIDADE, se a data de retenção for no futuro, o objeto poderá ser recuperado, mas

não poderá ser modificado ou excluído. A data de retenção pode ser aumentada, mas esta data não pode ser diminuída ou removida.

    - No modo GOVERNANÇA, usuários com permissão especial podem ignorar a configuração de retenção até a data. Eles podem excluir uma versão do objeto antes que seu período de retenção termine. Eles também podem aumentar, diminuir ou até mesmo remover a data de retenção.

- **Retenção legal**: Aplicar uma retenção legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar reter legalmente um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até ser explicitamente removida.

  A configuração de retenção legal para um objeto é independente do modo de retenção e da data de retenção. Se uma versão do objeto estiver sob retenção legal, ninguém poderá excluí-la.

Para especificar as configurações de bloqueio de objeto do S3 ao adicionar uma versão de objeto a um bucket, emita um"ColocarObjeto" ,"CopiarObjeto" , ou"CriarMultipartUpload" solicitar.

Você pode usar o seguinte:

- `x-amz-object-lock-mode`, que pode ser COMPLIANCE ou GOVERNANCE (diferencia maiúsculas de minúsculas).

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

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

  Se a retenção legal estiver LIGADA (diferencia maiúsculas de minúsculas), o objeto será colocado sob retenção legal. Se a retenção legal estiver DESLIGADA, nenhuma retenção legal será aplicada. Qualquer outro valor resulta em um erro 400 Bad Request (InvalidArgument).

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

- O `Content-MD5` o cabeçalho da solicitação é necessário se houver `x-amz-object-lock-*` O cabeçalho da solicitação está presente na solicitação PutObject. `Content-MD5` não é necessário para CopyObject ou CreateMultipartUpload.
- Se o bucket não tiver o S3 Object Lock habilitado e um `x-amz-object-lock-*` Se o cabeçalho da solicitação estiver presente, um erro 400 Bad Request (InvalidRequest) será retornado.
- A solicitação PutObject suporta o uso de `x-amz-storage-class: REDUCED_REDUNDANCY` para corresponder ao comportamento da AWS. No entanto, quando um objeto é ingerido em um bucket com o S3 Object Lock habilitado, o StorageGRID sempre executará uma ingestão de confirmação dupla.
- Uma resposta de versão GET ou HeadObject subsequente incluirá os cabeçalhos `x-amz-object-lock-mode` , `x-amz-object-lock-retain-until-date` , e `x-amz-object-lock-legal-hold` , se configurado e se o remetente da solicitação tiver o correto `s3:Get*` permissões.

Você pode usar o `s3:object-lock-remaining-retention-days` chave de condição de política para limitar os períodos mínimos e máximos de retenção permitidos para seus objetos.

Como atualizar as configurações de retenção de um objeto

Se precisar atualizar as configurações de retenção ou retenção legal para uma versão de objeto existente, você pode executar as seguintes operações de sub-recursos do objeto:

- `PutObjectLegalHold`

  Se o novo valor de retenção legal for LIGADO, o objeto será colocado sob retenção legal. Se o valor de retenção legal estiver DESLIGADO, a retenção legal será suspensa.

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

Como usar o modo GOVERNANÇA

Usuários que possuem o `s3:BypassGovernanceRetention` a permissão pode ignorar as configurações de retenção ativas de um objeto que usa o modo GOVERNANCE. Qualquer operação DELETE ou PutObjectRetention deve incluir o `x-amz-bypass-governance-retention:true` cabeçalho da solicitação. Esses usuários podem executar estas operações adicionais:

- Execute as operações DeleteObject ou DeleteObjects para excluir uma versão do objeto antes que seu período de retenção termine.

  Objetos que estão sob retenção legal não podem ser excluídos. A retenção legal deve estar DESLIGADA.

- Execute operações PutObjectRetention que alterem o modo de versão de um objeto de GOVERNANCE para COMPLIANCE antes que o período de retenção do objeto tenha decorrido.

  Alterar o modo de CONFORMIDADE para GOVERNANÇA nunca é permitido.

- Execute operações PutObjectRetention para aumentar, diminuir ou remover o período de retenção de uma versão do objeto.

Informações relacionadas

- "Gerenciar objetos com o S3 Object Lock"
- "Use o S3 Object Lock para reter objetos"
- "Guia do usuário do Amazon Simple Storage Service: Bloqueio de objetos"

Criar configuração do ciclo de vida do S3

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

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

O que é configuração de ciclo de vida

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

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: Exclua um objeto quando uma data especificada for atingida ou quando um número especificado de dias for atingido, a partir do momento em que o objeto foi ingerido.
- NoncurrentVersionExpiration: Exclui um objeto quando um número especificado de dias é atingido, começando em quando o objeto se tornou não atual.
- Filtro (Prefixo, Tag)
- Status
- EU IA

Cada objeto segue as configurações de retenção de um ciclo de vida de bucket do S3 ou de uma política do ILM. Quando um ciclo de vida de bucket do S3 é configurado, as ações de expiração do ciclo de vida substituem a política do ILM para objetos que correspondem ao filtro de ciclo de vida do bucket. Objetos que não correspondem ao filtro de ciclo de vida do bucket usam as configurações de retenção da política do ILM. Se um objeto corresponder a um filtro de ciclo de vida de bucket e nenhuma ação de expiração for explicitamente especificada, as configurações de retenção da política ILM não serão usadas e ficará implícito que as versões do objeto serão retidas para sempre. Ver "Exemplo de prioridades para o ciclo de vida do bucket S3 e política de ILM" .

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

> ⓘ 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.

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

- Ciclo de vida do DeleteBucket
- Obter configuração do ciclo de vida do Bucket
- Configuração do ciclo de vida do PutBucket

Criar configuração de ciclo de vida

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

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

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

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

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

Aplicar configuração de ciclo de vida ao bucket

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

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

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

Para validar se uma configuração de ciclo de vida foi aplicada com sucesso ao bucket, emita uma solicitação GetBucketLifecycleConfiguration. Por exemplo:

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

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

Validar se a expiração do ciclo de vida do bucket se aplica ao objeto

Você pode determinar se uma regra de expiração na configuração do ciclo de vida se aplica a um objeto específico ao emitir uma solicitação PutObject, HeadObject ou GetObject. Se uma regra se aplicar, a resposta inclui uma `Expiration` parâmetro que indica quando o objeto expira e qual regra de expiração foi correspondida.

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

Por exemplo, esta solicitação PutObject foi emitida em 22 de junho de 2020 e coloca um objeto no `testbucket` balde.

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

A resposta de sucesso indica que o objeto irá expirar em 100 dias (01 de outubro de 2020) e que correspondeu à Regra 2 da configuração do ciclo de vida.

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

Por exemplo, esta solicitação HeadObject foi usada para obter metadados para o mesmo objeto no bucket testbucket.

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

A resposta de sucesso inclui os metadados do objeto e indica que o objeto irá expirar em 100 dias e que correspondeu à Regra 2.

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

Para buckets habilitados para controle de versão, o `x-amz-expiration` O cabeçalho de resposta se aplica somente às versões atuais dos objetos.

Recomendações para implementar a API REST do S3

Você deve seguir estas recomendações ao implementar a API REST do S3 para uso com o StorageGRID.

Recomendações para HEADs para objetos inexistentes

Se o seu aplicativo verifica rotineiramente se um objeto existe em um caminho onde você não espera que o objeto realmente exista, você deve usar o "Disponível""consistência" . Por exemplo, você deve usar a consistência "Disponível" se seu aplicativo fizer HEAD de um local antes de fazer PUT nele.

Caso contrário, se a operação HEAD não encontrar o objeto, você poderá receber um alto número de erros 500 do Servidor Interno se dois ou mais Nós de Armazenamento no mesmo site estiverem indisponíveis ou um site remoto estiver inacessível.

Você pode definir a consistência "Disponível" para cada bucket usando o"Consistência do balde PUT"

solicitação, ou você pode especificar a consistência no cabeçalho da solicitação para uma operação de API individual.

Recomendações para chaves de objeto

Siga estas recomendações para nomes de chaves de objeto, com base em quando o bucket foi criado pela primeira vez.

Buckets criados no StorageGRID 11.4 ou anterior

- Não use valores aleatórios como os quatro primeiros caracteres das chaves do objeto. Isso contrasta com a antiga recomendação da AWS para prefixos de chaves. Em vez disso, use prefixos não aleatórios e não exclusivos, como `image` .
- Se você seguir a antiga recomendação da AWS de usar caracteres aleatórios e exclusivos em prefixos de chave, prefixe as chaves de objeto com um nome de diretório. Ou seja, use este formato:

  `mybucket/mydir/f8e3-image3132.jpg`

  Em vez deste formato:

  `mybucket/f8e3-image3132.jpg`

Buckets criados no StorageGRID 11.4 ou posterior

Não é necessário restringir nomes de chaves de objetos para atender às melhores práticas de desempenho. Na maioria dos casos, você pode usar valores aleatórios para os quatro primeiros caracteres dos nomes das chaves do objeto.

> Uma exceção a isso é uma carga de trabalho do S3 que remove continuamente todos os objetos após um curto período de tempo. Para minimizar o impacto no desempenho deste caso de uso, varie uma parte inicial do nome da chave a cada vários milhares de objetos com algo como a data. Por exemplo, suponha que um cliente S3 normalmente grava 2.000 objetos/segundo e a política de ciclo de vida do ILM ou do bucket remove todos os objetos após três dias. Para minimizar o impacto no desempenho, você pode nomear as chaves usando um padrão como este: `/mybucket/mydir/`*`yyyymmddhhmmss-random_UUID`*`.jpg`

Recomendações para "leituras de intervalo"

Se o"opção global para compactar objetos armazenados" estiver habilitado, os aplicativos cliente S3 devem evitar executar operações GetObject que especifiquem um intervalo de bytes a serem retornados. Essas operações de "leitura de intervalo" são ineficientes porque o StorageGRID precisa descompactar efetivamente os objetos para acessar os bytes solicitados. Operações GetObject que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é ineficiente ler um intervalo de 10 MB de um objeto compactado de 50 GB.

Se os intervalos forem lidos de objetos compactados, as solicitações do cliente poderão expirar.

> Se você precisar compactar objetos e seu aplicativo cliente precisar usar leituras de intervalo, aumente o tempo limite de leitura do aplicativo.

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.
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`

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

Estado do objeto	Resposta ao HeadObject

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` .
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`

Estado do objeto	Comportamento de RestoreObject
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
ChaveMuitoLonga	400 Solicitação Inválida

Nome	Status HTTP
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

Nome	Descrição	Status HTTP
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

Operações personalizadas do StorageGRID

Operações personalizadas do StorageGRID

O sistema StorageGRID suporta operações personalizadas que são adicionadas à API REST do S3.

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

Operação	Descrição
"Consistência do balde GET"	Retorna a consistência que está sendo aplicada a um bucket específico.
"Consistência do balde PUT"	Define a consistência aplicada a um bucket específico.
"Último horário de acesso do Bucket GET"	Retorna se as últimas atualizações de horário de acesso estão habilitadas ou desabilitadas para um bucket específico.

Operação	Descrição
"Hora do último acesso ao bucket PUT"	Permite que você habilite ou desabilite as atualizações do último horário de acesso para um bucket específico.
"EXCLUIR configuração de notificação de metadados do bucket"	Exclui o XML de configuração de notificação de metadados associado a um bucket específico.
"Configuração de notificação de metadados do GET Bucket"	Retorna o XML de configuração de notificação de metadados associado a um bucket específico.
"Configuração de notificação de metadados do PUT Bucket"	Configura o serviço de notificação de metadados para um bucket.
"Uso de armazenamento GET"	Informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta.
"Obsoleto: CreateBucket com configurações de conformidade"	Obsoleto e sem suporte: não é mais possível criar novos buckets com a Conformidade ativada.
"Obsoleto: conformidade com o GET Bucket"	Obsoleto, mas com suporte: retorna as configurações de conformidade atualmente em vigor para um bucket compatível legado existente.
"Obsoleto: conformidade com PUT Bucket"	Obsoleto, mas com suporte: permite modificar as configurações de conformidade de um bucket compatível legado existente.

Consistência do balde GET

A solicitação de consistência GET Bucket permite que você determine a consistência que está sendo aplicada a um bucket específico.

A consistência padrão é definida para garantir leitura após gravação para objetos recém-criados.

Você deve ter a permissão s3:GetBucketConsistency ou ser root da conta para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Resposta

No XML de resposta, `<Consistency>` retornará um dos seguintes valores:

Consistência	Descrição
todos	Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
forte-global	Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
site forte	Garante consistência de leitura após gravação para todas as solicitações de clientes em um site.
leitura após nova escrita	(Padrão) Fornece consistência de leitura após gravação para novos objetos e consistência eventual para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
disponível	Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que raramente são lidos ou para operações HEAD ou GET em chaves que não existem). Não suportado para buckets do S3 FabricPool .

Exemplo de resposta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Informações relacionadas

"Valores de consistência"

Consistência do balde PUT

A solicitação de consistência do PUT Bucket permite que você especifique a consistência a ser aplicada às operações executadas em um bucket.

A consistência padrão é definida para garantir leitura após gravação para objetos recém-criados.

Antes de começar

Você deve ter a permissão s3:PutBucketConsistency ou ser root da conta para concluir esta operação.

Solicitar

O `x-ntap-sg-consistency` o parâmetro deve conter um dos seguintes valores:

Consistência	Descrição
todos	Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
forte-global	Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
site forte	Garante consistência de leitura após gravação para todas as solicitações de clientes em um site.
leitura após nova escrita	(Padrão) Fornece consistência de leitura após gravação para novos objetos e consistência eventual para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
disponível	Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que raramente são lidos ou para operações HEAD ou GET em chaves que não existem). Não suportado para buckets do S3 FabricPool .

Observação: Em geral, você deve usar a consistência "Leitura após nova gravação". Se as solicitações não estiverem funcionando corretamente, altere o comportamento do cliente do aplicativo, se possível. Ou configure o cliente para especificar a consistência para cada solicitação de API. Defina a consistência no nível do bucket somente como último recurso.

Exemplo de solicitação

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informações relacionadas

"Valores de consistência"

Último horário de acesso do Bucket GET

A solicitação de último horário de acesso do GET Bucket permite que você determine se as atualizações de último horário de acesso estão habilitadas ou desabilitadas para buckets individuais.

Você deve ter a permissão s3:GetBucketLastAccessTime ou ser root da conta para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

Este exemplo mostra que as atualizações do último horário de acesso estão habilitadas para o bucket.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

Hora do último acesso ao bucket PUT

A solicitação de último horário de acesso do PUT Bucket permite que você habilite ou desabilite atualizações de último horário de acesso para buckets individuais. Desabilitar as atualizações do último horário de acesso melhora o desempenho e é a configuração padrão para todos os buckets criados com a versão 10.3.0 ou posterior.

Você deve ter a permissão s3:PutBucketLastAccessTime para um bucket ou ser root da conta para concluir esta operação.

> A partir da versão 10.3 do StorageGRID , as atualizações do último horário de acesso são desabilitadas por padrão para todos os novos buckets. Se você tiver buckets que foram criados usando uma versão anterior do StorageGRID e quiser corresponder ao novo comportamento padrão, deverá desabilitar explicitamente as atualizações do último horário de acesso para cada um desses buckets anteriores. Você pode habilitar ou desabilitar atualizações para o último horário de acesso usando a solicitação de último horário de acesso do bucket PUT ou na página de detalhes de um bucket no Gerenciador de locatários. Ver "Habilitar ou desabilitar atualizações do último horário de acesso" .

Se as atualizações do último horário de acesso estiverem desabilitadas para um bucket, o seguinte comportamento será aplicado às operações no bucket:

- As solicitações GetObject, GetObjectAcl, GetObjectTagging e HeadObject não atualizam o último horário de acesso. O objeto não é adicionado às filas para avaliação do gerenciamento do ciclo de vida das informações (ILM).
- As solicitações CopyObject e PutObjectTagging que atualizam apenas os metadados também atualizam o horário do último acesso. O objeto é adicionado às filas para avaliação do ILM.
- Se as atualizações do último horário de acesso estiverem desabilitadas para o bucket de origem, as solicitações CopyObject não atualizarão o último horário de acesso para o bucket de origem. O objeto que foi copiado não é adicionado às filas para avaliação do ILM para o bucket de origem. Entretanto, para o destino, as solicitações CopyObject sempre atualizam o horário do último acesso. A cópia do objeto é adicionada às filas para avaliação do ILM.
- CompleteMultipartUpload solicita atualização do último horário de acesso. O objeto concluído é adicionado às filas para avaliação do ILM.

Exemplos de solicitação

Este exemplo habilita o último horário de acesso para um bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Este exemplo desabilita o último horário de acesso para um bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

EXCLUIR configuração de notificação de metadados do bucket

A solicitação de configuração de notificação de metadados DELETE Bucket permite que você desabilite o serviço de integração de pesquisa para buckets individuais excluindo o XML de configuração.

Você deve ter a permissão s3:DeleteBucketMetadataNotification para um bucket ou ser root da conta para concluir esta operação.

Exemplo de solicitação

Este exemplo mostra a desativação do serviço de integração de pesquisa para um bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configuração de notificação de metadados do GET Bucket

A solicitação de configuração de notificação de metadados do GET Bucket permite que você recupere o XML de configuração usado para configurar a integração de pesquisa para buckets individuais.

Você deve ter a permissão s3:GetBucketMetadataNotification ou ser root da conta para concluir esta operação.

Exemplo de solicitação

Esta solicitação recupera a configuração de notificação de metadados para o bucket denominado `bucket` .

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Resposta

O corpo da resposta inclui a configuração de notificação de metadados para o bucket. A configuração de notificação de metadados permite que você determine como o bucket é configurado para integração de pesquisa. Ou seja, ele permite que você determine quais objetos são indexados e para quais endpoints seus metadados de objeto estão sendo enviados.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Cada configuração de notificação de metadados inclui uma ou mais regras. Cada regra especifica os objetos aos quais se aplica e o destino para onde o StorageGRID deve enviar metadados do objeto. Os destinos devem ser especificados usando o URN de um ponto de extremidade StorageGRID .

Nome	Descrição	Obrigatório
Configuração de Notificação de Metadados	Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos Rule.	Sim
Regra	Tag de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
EU IA	Identificador exclusivo para a regra. Incluído no elemento Rule.	Não
Status	O status pode ser "Habilitado" ou "Desabilitado". Nenhuma ação é tomada para regras que estão desabilitadas. Incluído no elemento Rule.	Sim

Nome	Descrição	Obrigatório
Prefixo	Objetos que correspondem ao prefixo são afetados pela regra, e seus metadados são enviados ao destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento Rule.	Sim
Destino	Tag de contêiner para o destino de uma regra. Incluído no elemento Rule.	Sim
Urna	URN do destino para onde os metadados do objeto são enviados. Deve ser a URN de um ponto de extremidade StorageGRID com as seguintes propriedades: • `es`deve ser o terceiro elemento. • A URN deve terminar com o índice e o tipo onde os metadados são armazenados, no formato `domain-name/myindex/mytype` . Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles assumem a seguinte forma: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O ponto de extremidade deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. A urna está incluída no elemento Destino.	Sim

Exemplo de resposta

O XML incluído entre o `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags mostra como a integração com um ponto de extremidade de integração de pesquisa é configurada para o bucket. Neste exemplo, os metadados do objeto estão sendo enviados para um índice do Elasticsearch denominado `current` e digite nomeado `2017` que está hospedado em um domínio AWS chamado `records` .

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informações relacionadas

"Use uma conta de inquilino"

Configuração de notificação de metadados do PUT Bucket

A solicitação de configuração de notificação de metadados do PUT Bucket permite que você habilite o serviço de integração de pesquisa para buckets individuais. O XML de configuração de notificação de metadados fornecido no corpo da solicitação especifica os objetos cujos metadados são enviados ao índice de pesquisa de destino.

Você deve ter a permissão s3:PutBucketMetadataNotification para um bucket ou ser root da conta para concluir esta operação.

Solicitar

A solicitação deve incluir a configuração de notificação de metadados no corpo da solicitação. Cada configuração de notificação de metadados inclui uma ou mais regras. Cada regra especifica os objetos aos quais se aplica e o destino para onde o StorageGRID deve enviar metadados do objeto.

Os objetos podem ser filtrados pelo prefixo do nome do objeto. Por exemplo, você pode enviar metadados para objetos com o prefixo `/images` para um destino e objetos com o prefixo `/videos` para outro.

Configurações que possuem prefixos sobrepostos não são válidas e são rejeitadas quando enviadas. Por exemplo, uma configuração que incluía uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não seria permitido.

Os destinos devem ser especificados usando o URN de um ponto de extremidade StorageGRID . O ponto de extremidade deve existir quando a configuração de notificação de metadados for enviada, ou a solicitação

falhará como um `400 Bad Request` . A mensagem de erro diz: `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.`

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

A tabela descreve os elementos no XML de configuração de notificação de metadados.

Nome	Descrição	Obrigatório
Configuração de Notificação de Metadados	Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos Rule.	Sim
Regra	Tag de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
EU IA	Identificador exclusivo para a regra. Incluído no elemento Rule.	Não
Status	O status pode ser "Habilitado" ou "Desabilitado". Nenhuma ação é tomada para regras que estão desabilitadas. Incluído no elemento Rule.	Sim

Nome	Descrição	Obrigatório
Prefixo	Objetos que correspondem ao prefixo são afetados pela regra, e seus metadados são enviados ao destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento Rule.	Sim
Destino	Tag de contêiner para o destino de uma regra. Incluído no elemento Rule.	Sim
Urna	URN do destino para onde os metadados do objeto são enviados. Deve ser a URN de um ponto de extremidade StorageGRID com as seguintes propriedades: • `es`deve ser o terceiro elemento. • A URN deve terminar com o índice e o tipo onde os metadados são armazenados, no formato `domain-name/myindex/mytype` . Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles assumem a seguinte forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O ponto de extremidade deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. A urna está incluída no elemento Destino.	Sim

Exemplos de solicitação

Este exemplo mostra como habilitar a integração de pesquisa para um bucket. Neste exemplo, os metadados de todos os objetos são enviados para o mesmo destino.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Neste exemplo, metadados de objetos para objetos que correspondem ao prefixo `/images` é enviado para um destino, enquanto metadados de objeto para objetos que correspondem ao prefixo `/videos` é enviado para um segundo destino.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

JSON gerado pelo serviço de integração de pesquisa

Quando você habilita o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado ao ponto de extremidade de destino sempre que metadados ou tags de objeto são adicionados, atualizados ou excluídos.

Este exemplo mostra um exemplo do JSON que pode ser gerado quando um objeto com a chave `SGWS/Tagging.txt` é criado em um bucket chamado `test` . O `test` o bucket não é versionado, então o `versionId` a tag está vazia.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadados de objeto incluídos em notificações de metadados

A tabela lista todos os campos incluídos no documento JSON que é enviado ao ponto de extremidade de destino quando a integração de pesquisa está habilitada.

O nome do documento inclui o nome do bucket, o nome do objeto e o ID da versão, se presente.

Tipo	Nome do item	Descrição
Informações sobre bucket e objeto	balde	Nome do balde
Informações sobre bucket e objeto	chave	Nome da chave do objeto
Informações sobre bucket e objeto	ID da versão	Versão do objeto, para objetos em buckets versionados
Informações sobre bucket e objeto	região	Região de balde, por exemplo `us-east-1`
Metadados do sistema	tamanho	Tamanho do objeto (em bytes) conforme visível para um cliente HTTP
Metadados do sistema	md5	Hash de objeto
Metadados do usuário	metadados *`key:value`*	Todos os metadados do usuário para o objeto, como pares de chave-valor

Tipo	Nome do item	Descrição
Etiquetas	etiquetas *key:value*	Todas as tags de objeto definidas para o objeto, como pares chave-valor

> Para tags e metadados do usuário, o StorageGRID passa datas e números para o Elasticsearch como strings ou como notificações de eventos do S3. Para configurar o Elasticsearch para interpretar essas strings como datas ou números, siga as instruções do Elasticsearch para mapeamento de campos dinâmicos e para mapeamento de formatos de data. Você deve habilitar os mapeamentos de campos dinâmicos no índice antes de configurar o serviço de integração de pesquisa. Depois que um documento é indexado, você não pode editar os tipos de campo do documento no índice.

Informações relacionadas

"Use uma conta de inquilino"

Solicitação de uso de armazenamento GET

A solicitação GET Storage Usage informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta.

A quantidade de armazenamento usada por uma conta e seus buckets pode ser obtida por meio de uma solicitação ListBuckets modificada com o `x-ntap-sg-usage` parâmetro de consulta. O uso do armazenamento do bucket é rastreado separadamente das solicitações PUT e DELETE processadas pelo sistema. Pode haver algum atraso antes que os valores de uso correspondam aos valores esperados com base no processamento de solicitações, principalmente se o sistema estiver sob carga pesada.

Por padrão, o StorageGRID tenta recuperar informações de uso usando consistência global forte. Se a consistência global forte não puder ser alcançada, o StorageGRID tentará recuperar as informações de uso em uma consistência de site forte.

Você deve ter a permissão s3:ListAllMyBuckets ou ser root da conta para concluir esta operação.

Exemplo de solicitação

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

Este exemplo mostra uma conta que tem quatro objetos e 12 bytes de dados em dois buckets. Cada bucket contém dois objetos e seis bytes de dados.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Controle de versão

Cada versão do objeto armazenada contribuirá para o `ObjectCount` e `DataBytes` valores na resposta. Os marcadores de exclusão não são adicionados ao `ObjectCount` total.

Informações relacionadas

"Valores de consistência"

Solicitações de bucket obsoletas para conformidade legada

Solicitações de bucket obsoletas para conformidade legada

Talvez seja necessário usar a API REST do StorageGRID S3 para gerenciar buckets que foram criados usando o recurso de conformidade legado.

Recurso de conformidade obsoleto

O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock.

Se você habilitou anteriormente a configuração global de Conformidade, a configuração global de Bloqueio de Objeto S3 será habilitada no StorageGRID 11.6. Não é mais possível criar novos buckets com a Conformidade ativada; no entanto, conforme necessário, você pode usar a API REST do StorageGRID S3 para gerenciar quaisquer buckets compatíveis legados existentes.

- "Use a API REST do S3 para configurar o bloqueio de objeto do S3"
- "Gerenciar objetos com ILM"
- "Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"

Solicitações de conformidade obsoletas:

- "Obsoleto - Modificações na solicitação do bucket PUT para conformidade"

  O elemento XML SGCompliance está obsoleto. Anteriormente, você podia incluir esse elemento personalizado StorageGRID no corpo de solicitação XML opcional de solicitações PUT Bucket para criar um bucket compatível.

- "Obsoleto - Conformidade com o GET Bucket"

  A solicitação de conformidade do GET Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket compatível legado existente.

- "Obsoleto - Conformidade com PUT Bucket"

  A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para modificar as configurações de conformidade de um bucket compatível legado existente. Por exemplo, você pode colocar um bucket existente em retenção legal ou aumentar seu período de retenção.

Obsoleto: modificações na solicitação CreateBucket para conformidade

O elemento XML SGCompliance está obsoleto. Anteriormente, você podia incluir este elemento personalizado StorageGRID no corpo de solicitação XML opcional das solicitações CreateBucket para criar um bucket compatível.

> O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock. Veja o seguinte para mais detalhes:
>
> - "Use a API REST do S3 para configurar o bloqueio de objeto do S3"
> - "Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"

Não é mais possível criar novos buckets com a Conformidade ativada. A seguinte mensagem de erro será retornada se você tentar usar as modificações de solicitação CreateBucket para conformidade para criar um novo bucket compatível:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsoleto: solicitação de conformidade do GET Bucket

A solicitação de conformidade do GET Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket compatível legado existente.

> ⓘ O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock. Veja o seguinte para mais detalhes:
>
> - "Use a API REST do S3 para configurar o bloqueio de objeto do S3"
> - "Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"

Você deve ter a permissão s3:GetBucketCompliance ou ser root da conta para concluir esta operação.

Exemplo de solicitação

Este exemplo de solicitação permite que você determine as configurações de conformidade para o bucket denominado `mybucket` .

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

No XML de resposta, `<SGCompliance>` lista as configurações de conformidade em vigor para o bucket. Este exemplo de resposta mostra as configurações de conformidade para um bucket no qual cada objeto será retido por um ano (525.600 minutos), a partir do momento em que o objeto for ingerido na grade. Atualmente não há retenção legal para este balde. Cada objeto será excluído automaticamente após um ano.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrição
Período de retenção em minutos	A duração do período de retenção para objetos adicionados a este bucket, em minutos. O período de retenção começa quando o objeto é ingerido na grade.
Retenção Legal	• Verdadeiro: Este bucket está atualmente sob retenção legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja suspensa, mesmo que o período de retenção tenha expirado. • Falso: Este bucket não está atualmente sob retenção legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Exclusão automática	• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob retenção legal. • Falso: Os objetos neste bucket não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Respostas de erro

Se o bucket não foi criado para ser compatível, o código de status HTTP para a resposta é `404 Not Found`, com um código de erro S3 de `XNoSuchBucketCompliance`.

Obsoleto: solicitação de conformidade do PUT Bucket

A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para modificar as configurações de conformidade de um bucket compatível legado existente. Por exemplo, você pode colocar um bucket existente em retenção legal ou aumentar seu período de retenção.

O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock. Veja o seguinte para mais detalhes:

- "Use a API REST do S3 para configurar o bloqueio de objeto do S3"
- "Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"

Você deve ter a permissão s3:PutBucketCompliance ou ser root da conta para concluir esta operação.

Você deve especificar um valor para cada campo das configurações de conformidade ao emitir uma solicitação de conformidade do PUT Bucket.

Exemplo de solicitação

Este exemplo de solicitação modifica as configurações de conformidade para o bucket denominado `mybucket` . Neste exemplo, os objetos em `mybucket` agora serão retidos por dois anos (1.051.200 minutos) em vez de um ano, a partir do momento em que o objeto for inserido na grade. Não há retenção legal para este balde. Cada objeto será excluído automaticamente após dois anos.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrição
Período de retenção em minutos	A duração do período de retenção para objetos adicionados a este bucket, em minutos. O período de retenção começa quando o objeto é ingerido na grade. **Importante** Ao especificar um novo valor para RetentionPeriodMinutes, você deve especificar um valor que seja igual ou maior que o período de retenção atual do bucket. Depois que o período de retenção do bucket for definido, você não poderá diminuir esse valor; você só poderá aumentá-lo.

Nome	Descrição
Retenção Legal	• Verdadeiro: Este bucket está atualmente sob retenção legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja suspensa, mesmo que o período de retenção tenha expirado. • Falso: Este bucket não está atualmente sob retenção legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Exclusão automática	• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob retenção legal. • Falso: Os objetos neste bucket não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Consistência para configurações de conformidade

Quando você atualiza as configurações de conformidade de um bucket do S3 com uma solicitação de conformidade do bucket PUT, o StorageGRID tenta atualizar os metadados do bucket na grade. Por padrão, o StorageGRID usa a consistência **Strong-global** para garantir que todos os sites do data center e todos os nós de armazenamento que contêm metadados de bucket tenham consistência de leitura após gravação para as configurações de conformidade alteradas.

Se o StorageGRID não conseguir atingir a consistência **Strong-global** porque um site de data center ou vários nós de armazenamento em um site não estão disponíveis, o código de status HTTP para a resposta é `503 Service Unavailable`.

Se você receber essa resposta, entre em contato com o administrador da rede para garantir que os serviços de armazenamento necessários sejam disponibilizados o mais rápido possível. Se o administrador da grade não conseguir disponibilizar Nós de Armazenamento suficientes em cada site, o suporte técnico poderá instruí-lo a tentar novamente a solicitação com falha, forçando a consistência **Strong-site**.

> Nunca force a consistência **Strong-site** para conformidade com o bucket PUT, a menos que você tenha sido instruído a fazê-lo pelo suporte técnico e a menos que você entenda as potenciais consequências do uso desse nível.

Quando a consistência é reduzida para **Strong-site**, o StorageGRID garante que as configurações de conformidade atualizadas terão consistência de leitura após gravação somente para solicitações de clientes dentro de um site. Isso significa que o sistema StorageGRID pode ter temporariamente várias configurações inconsistentes para esse bucket até que todos os sites e nós de armazenamento estejam disponíveis. Configurações inconsistentes podem resultar em comportamento inesperado e indesejado. Por exemplo, se você estiver colocando um bucket sob retenção legal e forçar uma consistência menor, as configurações de conformidade anteriores do bucket (ou seja, retenção legal) poderão continuar em vigor em alguns sites de data center. Como resultado, objetos que você acha que estão em retenção legal podem ser excluídos quando seu período de retenção expirar, pelo usuário ou pela Exclusão Automática, se habilitada.

Para forçar o uso da consistência **Strong-site**, emita novamente a solicitação de conformidade do PUT Bucket e inclua o `Consistency-Control` Cabeçalho de solicitação HTTP, como segue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Respostas de erro

- Se o bucket não foi criado para ser compatível, o código de status HTTP para a resposta é `404 Not Found`.
- Se `RetentionPeriodMinutes` na solicitação for menor que o período de retenção atual do bucket, o código de status HTTP é `400 Bad Request`.

Informações relacionadas

"Obsoleto: modificações na solicitação do bucket PUT para conformidade"

Políticas de acesso a grupos e buckets

Use políticas de acesso a buckets e grupos

O StorageGRID usa a linguagem de política da Amazon Web Services (AWS) para permitir que os locatários do S3 controlem o acesso a buckets e objetos dentro desses buckets. O sistema StorageGRID implementa um subconjunto da linguagem de política da API REST do S3. As políticas de acesso para a API do S3 são escritas em JSON.

Visão geral da política de acesso

Há dois tipos de políticas de acesso suportadas pelo StorageGRID.

- **Políticas de bucket**, que são gerenciadas usando as operações da API S3 GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy ou a API Tenant Manager ou Tenant Management. As políticas de bucket são anexadas aos buckets, portanto, elas são configuradas para controlar o acesso de usuários na conta do proprietário do bucket ou de outras contas ao bucket e aos objetos nele contidos. Uma política de bucket se aplica a apenas um bucket e possivelmente a vários grupos.
- **Políticas de grupo**, que são configuradas usando o Tenant Manager ou a Tenant Management API. As políticas de grupo são anexadas a um grupo na conta, portanto, elas são configuradas para permitir que esse grupo acesse recursos específicos de propriedade dessa conta. Uma política de grupo se aplica a apenas um grupo e possivelmente a vários buckets.

> Não há diferença de prioridade entre políticas de grupo e de bucket.

As políticas de grupo e bucket do StorageGRID seguem uma gramática específica definida pela Amazon. Dentro de cada política há uma série de declarações de política, e cada declaração contém os seguintes elementos:

- ID da declaração (Sid) (opcional)
- Efeito
- Principal/Não Principal
- Recurso/NãoRecurso

- Ação/NãoAção
- Condição (opcional)

As declarações de política são criadas usando esta estrutura para especificar permissões: Conceder <Efeito> para permitir/negar que <Principal> execute <Ação> em <Recurso> quando <Condição> se aplicar.

Cada elemento de política é usado para uma função específica:

Elemento	Descrição
Sido	O elemento Sid é opcional. O Sid serve apenas como uma descrição para o usuário. Ele é armazenado, mas não interpretado pelo sistema StorageGRID .
Efeito	Use o elemento Efeito para estabelecer se as operações especificadas são permitidas ou negadas. Você deve identificar as operações que permite (ou nega) em buckets ou objetos usando as palavras-chave do elemento Action suportadas.
Principal/Não Principal	Você pode permitir que usuários, grupos e contas acessem recursos específicos e executem ações específicas. Se nenhuma assinatura S3 for incluída na solicitação, o acesso anônimo será permitido especificando o caractere curinga (*) como principal. Por padrão, somente o root da conta tem acesso aos recursos de propriedade da conta. Você só precisa especificar o elemento Principal em uma política de bucket. Para políticas de grupo, o grupo ao qual a política está anexada é o elemento Principal implícito.
Recurso/NãoRecurso	O elemento Resource identifica buckets e objetos. Você pode permitir ou negar permissões para buckets e objetos usando o Amazon Resource Name (ARN) para identificar o recurso.
Ação/NãoAção	Os elementos Ação e Efeito são os dois componentes das permissões. Quando um grupo solicita um recurso, o acesso ao recurso é concedido ou negado. O acesso será negado, a menos que você atribua permissões especificamente, mas você pode usar a negação explícita para substituir uma permissão concedida por outra política.
Doença	O elemento Condition é opcional. As condições permitem que você crie expressões para determinar quando uma política deve ser aplicada.

No elemento Ação, você pode usar o caractere curinga (*) para especificar todas as operações ou um subconjunto de operações. Por exemplo, esta Ação corresponde a permissões como s3:GetObject, s3:PutObject e s3:DeleteObject.

```
s3:*Object
```

No elemento Recurso, você pode usar os caracteres curinga (*) e (?). Enquanto o asterisco (*) corresponde a

0 ou mais caracteres, o ponto de interrogação (?) corresponde a qualquer caractere único.

No elemento Principal, caracteres curinga não são suportados, exceto para definir acesso anônimo, que concede permissão a todos. Por exemplo, você define o curinga (*) como o valor Principal.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

No exemplo a seguir, a instrução está usando os elementos Effect, Principal, Action e Resource. Este exemplo mostra uma declaração de política de bucket completa que usa o efeito "Permitir" para dar aos Principais, o grupo de administração `federated-group/admin` e o grupo financeiro `federated-group/finance` , permissões para executar a Ação `s3:ListBucket` no balde chamado `mybucket` e a Ação `s3:GetObject` em todos os objetos dentro desse balde.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

A política de bucket tem um limite de tamanho de 20.480 bytes, e a política de grupo tem um limite de tamanho de 5.120 bytes.

Consistência para políticas

Por padrão, todas as atualizações feitas nas políticas de grupo serão consistentes. Quando uma política de grupo se torna consistente, as alterações podem levar mais 15 minutos para entrar em vigor, devido ao cache de políticas. Por padrão, todas as atualizações feitas nas políticas de bucket são fortemente consistentes.

Conforme necessário, você pode alterar as garantias de consistência para atualizações de política de bucket. Por exemplo, você pode querer que uma alteração em uma política de bucket esteja disponível durante uma interrupção do site.

Neste caso, você pode definir o `Consistency-Control` cabeçalho na solicitação PutBucketPolicy ou você pode usar a solicitação de consistência PUT Bucket. Quando uma política de bucket se torna consistente, as alterações podem levar mais 8 segundos para entrar em vigor, devido ao cache de políticas.

> Se você definir a consistência para um valor diferente para contornar uma situação temporária, certifique-se de definir a configuração do nível do bucket de volta para seu valor original quando terminar. Caso contrário, todas as solicitações futuras de bucket usarão a configuração modificada.

Use ARN em declarações de política

Em declarações de política, o ARN é usado nos elementos Principal e Resource.

- Use esta sintaxe para especificar o ARN do recurso S3:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Use esta sintaxe para especificar o ARN do recurso de identidade (usuários e grupos):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Outras considerações:

- Você pode usar o asterisco (*) como curinga para corresponder a zero ou mais caracteres dentro da chave do objeto.
- Caracteres internacionais, que podem ser especificados na chave do objeto, devem ser codificados usando JSON UTF-8 ou usando sequências de escape JSON \u. A codificação percentual não é suportada.

  "Sintaxe URN RFC 2141"

  O corpo da solicitação HTTP para a operação PutBucketPolicy deve ser codificado com charset=UTF-8.

Especificar recursos em uma política

Em declarações de política, você pode usar o elemento Resource para especificar o bucket ou objeto para o qual as permissões são permitidas ou negadas.

- Cada declaração de política requer um elemento Recurso. Em uma política, os recursos são denotados

pelo elemento `Resource` , ou alternativamente, `NotResource` para exclusão.

- Você especifica recursos com um ARN de recurso S3. Por exemplo:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Você também pode usar variáveis de política dentro da chave do objeto. Por exemplo:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- O valor do recurso pode especificar um bucket que ainda não existe quando uma política de grupo é criada.

Especificar os principais em uma política

Use o elemento Principal para identificar o usuário, grupo ou conta de locatário que tem acesso permitido/negado ao recurso pela declaração de política.

- Cada declaração de política em uma política de bucket deve incluir um elemento Principal. Declarações de política em uma política de grupo não precisam do elemento Principal porque o grupo é entendido como o principal.
- Em uma política, os principais são indicados pelo elemento "Principal" ou, alternativamente, "NotPrincipal" para exclusão.
- Identidades baseadas em conta devem ser especificadas usando um ID ou um ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- Este exemplo usa o ID da conta de locatário 27233906934684427525, que inclui a raiz da conta e todos os usuários na conta:

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Você pode especificar apenas a raiz da conta:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Você pode especificar um usuário federado específico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Você pode especificar um grupo federado específico ("Gerentes"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Você pode especificar um principal anônimo:

```
"Principal": "*"
```

- Para evitar ambiguidade, você pode usar o UUID do usuário em vez do nome de usuário:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Por exemplo, suponha que Alex deixe a organização e o nome de usuário `Alex` é excluído. Se um novo Alex se juntar à organização e for designado para o mesmo `Alex` nome de usuário, o novo usuário pode herdar involuntariamente as permissões concedidas ao usuário original.

- O valor principal pode especificar um nome de grupo/usuário que ainda não existe quando uma política de bucket é criada.

Especificar permissões em uma política

Em uma política, o elemento Ação é usado para permitir/negar permissões para um recurso. Há um conjunto de permissões que você pode especificar em uma política, que são indicadas pelo elemento "Ação" ou, alternativamente, "NãoAção" para exclusão. Cada um desses elementos mapeia operações específicas da API REST do S3.

As tabelas listam as permissões que se aplicam aos buckets e as permissões que se aplicam aos objetos.

O Amazon S3 agora usa a permissão s3:PutReplicationConfiguration para as ações PutBucketReplication e DeleteBucketReplication. O StorageGRID usa permissões separadas para cada ação, o que corresponde à especificação original do Amazon S3.

Uma exclusão é realizada quando um put é usado para substituir um valor existente.

Permissões que se aplicam a buckets

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:CriarBucket	CriarBucket	Sim. **Observação**: Use somente em políticas de grupo.
s3:ExcluirBucket	ExcluirBucket	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:DeleteBucketMetadataNotification	EXCLUIR configuração de notificação de metadados do bucket	Sim
s3:DeleteBucketPolicy	Política de exclusão de balde	
s3:ExcluirConfiguração de Replicação	DeleteBucketReplication	Sim, permissões separadas para PUT e DELETE
s3:ObterBucketAcl	ObterBucketAcl	
s3:ObterConformidade doBucket	Conformidade com o GET Bucket (obsoleto)	Sim
s3:ObterConsistência doBucket	Consistência do balde GET	Sim
s3:ObterBucketCORS	ObterBucketCors	
s3:ObterConfiguração de Criptografia	Obter criptografia do Bucket	
s3:GetBucketÚltimoAcessoHora	Último horário de acesso do Bucket GET	Sim
s3:ObterLocalização do Balde	ObterBucketLocation	
s3:GetBucketMetadataNotification	Configuração de notificação de metadados do GET Bucket	Sim
s3:GetBucketNotification	Obter configuração de notificação de bucket	
s3:GetBucketObjectLockConfiguration	ObterConfiguraçãoObjectLock	
s3:ObterPolítica deBucket	ObterBucketPolicy	
s3:Obter marcação de balde	Obter marcação de balde	
s3:GetBucketVersionamento	ObterVersionamento doBucket	
s3:ObterConfiguração do Ciclo de Vida	Obter configuração do ciclo de vida do Bucket	
s3:ObterConfiguração de Replicação	Obter replicação do Bucket	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:ListarTodosOsMeusBuckets	• ListBuckets • Uso de armazenamento GET	Sim, para uso de armazenamento GET. **Observação**: Use somente em políticas de grupo.
s3:ListBucket	• Objetos de Lista • Balde de cabeça • RestaurarObjeto	
s3:ListBucketMultipartUploads	• ListarMultipartUploads • RestaurarObjeto	
s3:ListBucketVersões	Versões do GET Bucket	
s3:Conformidade com PutBucket	Conformidade com o PUT Bucket (obsoleto)	Sim
s3:ConsistênciaPutBucket	Consistência do balde PUT	Sim
s3:ColocarBucketCORS	• ExcluirBucketCors† • ColoqueBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:ColocarBucketÚltimoAcessoHora	Hora do último acesso ao bucket PUT	Sim
s3:PutBucketMetadataNotification	Configuração de notificação de metadados do PUT Bucket	Sim
s3:NotificaçãoPutBucket	Configuração de notificação PutBucket	
s3:PutBucketObjectLockConfiguração	• CreateBucket com o `x-amz-bucket-object-lock-enabled: true` cabeçalho de solicitação (também requer a permissão s3:CreateBucket) • PutObjectLockConfiguration	
s3:PolíticaPutBucket	PutBucketPolicy	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:PutBucketTagging	• ExcluirBucketTagging† • Colocar marcação de balde	
s3:PutBucketVersionamento	Versão PutBucket	
s3:PutLifecycleConfiguration	• Ciclo de vida do DeleteBucket† • Configuração do ciclo de vida do PutBucket	
s3:PutReplicationConfiguration	PutBucketReplicação	Sim, permissões separadas para PUT e DELETE

Permissões que se aplicam a objetos

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:AbortarUploadMultipart	• AbortarMultipartUpload • RestaurarObjeto	
s3:Ignorar Governança Retenção	• ExcluirObjeto • ExcluirObjetos • ColocarRetençãoDeObjeto	
s3:ExcluirObjeto	• ExcluirObjeto • ExcluirObjetos • RestaurarObjeto	
s3:ExcluirMarcaçãoDeObjeto	ExcluirMarcaçãoDeObjeto	
s3:ExcluirMarcaçãoDeVersãoDoObjeto	DeleteObjectTagging (uma versão específica do objeto)	
s3:ExcluirVersãoDoObjeto	DeleteObject (uma versão específica do objeto)	
s3:ObterObjeto	• ObterObjeto • CabeçaObjeto • RestaurarObjeto • SelecionarObjetoConteúdo	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:ObterAclDeObjeto	ObterAclObjeto	
s3:ObterObjetoLegalHold	ObterObjetoLegalHold	
s3:ObterRetençãoDeObjeto	ObterRetençãoDeObjeto	
s3:ObterMarcaçãoDeObjeto	Obter marcação de objeto	
s3:ObterTag deVersão do Objeto	GetObjectTagging (uma versão específica do objeto)	
s3:ObterVersãoDoObjeto	GetObject (uma versão específica do objeto)	
s3:ListMultipartUploadParts	ListParts, RestaurarObjeto	
s3:ColocarObjeto	• ColocarObjeto • CopiarObjeto • RestaurarObjeto • CriarMultipartUpload • Upload completo de várias partes • UploadPart • UploadPartCopy	
s3:ColocarObjetoLegalHold	ColocarObjetoLegalHold	
s3:PutObjectRetention	ColocarRetençãoDeObjeto	
s3:PutObjectTagging	Colocar marcação de objeto	
s3:PutObjectVersionTagging	PutObjectTagging (uma versão específica do objeto)	
s3:ColocarObjetoSobrescrito	• ColocarObjeto • CopiarObjeto • Colocar marcação de objeto • ExcluirMarcaçãoDeObjeto • Upload completo de várias partes	Sim
s3:RestaurarObjeto	RestaurarObjeto	

Usar permissão PutOverwriteObject

A permissão s3:PutOverwriteObject é uma permissão personalizada do StorageGRID que se aplica a operações que criam ou atualizam objetos. A configuração dessa permissão determina se o cliente pode substituir os dados de um objeto, metadados definidos pelo usuário ou marcação de objetos do S3.

As configurações possíveis para essa permissão incluem:

- **Permitir**: O cliente pode substituir um objeto. Esta é a configuração padrão.
- **Negar**: O cliente não pode substituir um objeto. Quando definida como Negar, a permissão PutOverwriteObject funciona da seguinte maneira:
  - Se um objeto existente for encontrado no mesmo caminho:
    - Os dados do objeto, os metadados definidos pelo usuário ou a marcação de objetos S3 não podem ser substituídos.
    - Todas as operações de ingestão em andamento são canceladas e um erro é retornado.
    - Se o controle de versão do S3 estiver habilitado, a configuração Negar impedirá que as operações PutObjectTagging ou DeleteObjectTagging modifiquem o TagSet de um objeto e suas versões não atuais.
  - Se um objeto existente não for encontrado, esta permissão não terá efeito.
- Quando essa permissão não está presente, o efeito é o mesmo que se Permitir estivesse definido.

> Se a política atual do S3 permitir a substituição e a permissão PutOverwriteObject estiver definida como Negar, o cliente não poderá substituir os dados de um objeto, os metadados definidos pelo usuário ou a marcação de objetos. Além disso, se a caixa de seleção **Impedir modificação do cliente** estiver marcada (**CONFIGURAÇÃO** > **Configurações de segurança** > **Rede e objetos**), essa configuração substituirá a configuração da permissão PutOverwriteObject.

Especificar condições em uma política

As condições definem quando uma política estará em vigor. As condições consistem em operadores e pares chave-valor.

As condições usam pares chave-valor para avaliação. Um elemento Condition pode conter várias condições, e cada condição pode conter vários pares chave-valor. O bloco de condição usa o seguinte formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

No exemplo a seguir, a condição IpAddress usa a chave de condição SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Operadores de condição suportados

Os operadores de condição são categorizados da seguinte forma:

- Corda
- Numérico
- Booleano
- Endereço IP
- Verificação nula

Operadores de condição	Descrição
StringEquals	Compara uma chave a um valor de string com base na correspondência exata (diferencia maiúsculas de minúsculas).
StringNotEquals	Compara uma chave a um valor de string com base na correspondência negada (diferencia maiúsculas de minúsculas).
StringEqualsIgnoreCase	Compara uma chave a um valor de string com base na correspondência exata (ignora maiúsculas e minúsculas).
StringNotEqualsIgnoreCase	Compara uma chave a um valor de string com base na correspondência negada (ignora maiúsculas e minúsculas).
StringLike	Compara uma chave a um valor de string com base na correspondência exata (diferencia maiúsculas de minúsculas). Pode incluir caracteres curinga * e ?.
StringNotLike	Compara uma chave a um valor de string com base na correspondência negada (diferencia maiúsculas de minúsculas). Pode incluir caracteres curinga * e ?.
NumericEquals	Compara uma chave a um valor numérico com base na correspondência exata.
NuméricoNãoIgual	Compara uma chave a um valor numérico com base na correspondência negada.

Operadores de condição	Descrição
NuméricoMaiorQue	Compara uma chave a um valor numérico com base na correspondência "maior que".
NuméricoMaiorQueIgual	Compara uma chave a um valor numérico com base na correspondência "maior ou igual a".
NuméricoMenorQue	Compara uma chave a um valor numérico com base na correspondência "menor que".
NuméricoMenorQueIgual	Compara uma chave a um valor numérico com base na correspondência "menor ou igual a".
Bool	Compara uma chave a um valor booleano com base na correspondência "verdadeiro ou falso".
Endereço IP	Compara uma chave a um endereço IP ou intervalo de endereços IP.
Não Endereço IP	Compara uma chave a um endereço IP ou intervalo de endereços IP com base na correspondência negada.
Nulo	Verifica se uma chave de condição está presente no contexto de solicitação atual.

Chaves de condição suportadas

Chaves de condição	Ações	Descrição
aws:SourceIp	Operadores de IP	Será comparado ao endereço IP de onde a solicitação foi enviada. Pode ser usado para operações de bucket ou objeto. **Observação:** Se a solicitação S3 foi enviada por meio do serviço Load Balancer nos nós de administração e nos nós de gateway, isso será comparado ao endereço IP upstream do serviço Load Balancer. **Observação**: se um balanceador de carga de terceiros não transparente for usado, isso será comparado ao endereço IP desse balanceador de carga. Qualquer `X-Forwarded-For` O cabeçalho será ignorado porque sua validade não pode ser verificada.
aws:nome de usuário	Recurso/Identidade	Será comparado ao nome de usuário do remetente de onde a solicitação foi enviada. Pode ser usado para operações de bucket ou objeto.

Chaves de condição	Ações	Descrição
s3:delimitador	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro delimitador especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:ExistingObjectTag/<chave-tag>	s3:ExcluirMarcaçãoDeObjeto s3:ExcluirMarcaçãoDeVersãoDoObjeto s3:ObterObjeto s3:ObterAclDeObjeto 3: Obter marcação de objeto s3:ObterVersãoDoObjeto s3:ObterVersãoDoObjetoAcl s3:ObterTag deVersão do Objeto s3:ColocarObjetoAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Exigirá que o objeto existente tenha a chave e o valor de tag específicos.
s3:max-chaves	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro max-keys especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:object-lock-remaining-retention-days	s3:ColocarObjeto	Compara com a data de retenção especificada no `x-amz-object-lock-retain-until-date` cabeçalho de solicitação ou calculado a partir do período de retenção padrão do bucket para garantir que esses valores estejam dentro do intervalo permitido para as seguintes solicitações: • ColocarObjeto • CopiarObjeto • CriarMultipartUpload

Chaves de condição	Ações	Descrição
s3:object-lock-remaining-retention-days	s3:PutObjectRetention	Compara com a data de retenção especificada na solicitação PutObjectRetention para garantir que esteja dentro do intervalo permitido.
s3:prefix	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro de prefixo especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:RequestObjectTag/<chave-tag>	s3:ColocarObjeto s3:PutObjectTagging s3:PutObjectVersionTagging	Exigirá uma chave de tag e um valor específicos quando a solicitação de objeto incluir marcação.

Especificar variáveis em uma política

Você pode usar variáveis em políticas para preencher informações de políticas quando elas estiverem disponíveis. Você pode usar variáveis de política no `Resource` elemento e em comparações de strings no `Condition` elemento.

Neste exemplo, a variável `${aws:username}` faz parte do elemento Recurso:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

Neste exemplo, a variável `${aws:username}` faz parte do valor da condição no bloco de condição:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variável	Descrição
`${aws:SourceIp}`	Usa a chave SourceIp como a variável fornecida.
`${aws:username}`	Usa a chave de nome de usuário como a variável fornecida.
`${s3:prefix}`	Usa a chave de prefixo específica do serviço como a variável fornecida.

Variável	Descrição
`${s3:max-keys}`	Usa a chave max-keys específica do serviço como a variável fornecida.
`${*}`	Caractere especial. Usa o caractere como um caractere * literal.
`${?}`	Caractere especial. Usa o caractere como um caractere literal ?.
`${$}`	Caractere especial. Usa o caractere como um caractere $ literal.

Crie políticas que exijam tratamento especial

Às vezes, uma política pode conceder permissões que são perigosas para a segurança ou perigosas para operações contínuas, como bloquear o usuário root da conta. A implementação da API REST do StorageGRID S3 é menos restritiva durante a validação de políticas do que a Amazon, mas igualmente rigorosa durante a avaliação de políticas.

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento do StorageGRID
Negar a si mesmo quaisquer permissões para a conta root	Balde	Válido e aplicado, mas a conta do usuário root mantém a permissão para todas as operações de política do bucket S3	Mesmo
Negar a si mesmo quaisquer permissões para usuário/grupo	Grupo	Válido e aplicado	Mesmo
Permitir qualquer permissão a um grupo de contas estrangeiras	Balde	Principal inválido	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro 405 Método Não Permitido quando permitidas por uma política
Permitir que uma conta estrangeira root ou usuário tenha qualquer permissão	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro 405 Método Não Permitido quando permitidas por uma política	Mesmo

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento do StorageGRID
Permitir que todos tenham permissão para todas as ações	Balde	Válido, mas as permissões para todas as operações de política do bucket S3 retornam um erro 405 Método Não Permitido para a raiz da conta estrangeira e usuários	Mesmo
Negar a todos permissões para todas as ações	Balde	Válido e aplicado, mas a conta do usuário root mantém a permissão para todas as operações de política do bucket S3	Mesmo
Principal é um usuário ou grupo inexistente	Balde	Principal inválido	Válido
O recurso é um bucket S3 inexistente	Grupo	Válido	Mesmo
Principal é um grupo local	Balde	Principal inválido	Válido
A política concede a uma conta não proprietária (incluindo contas anônimas) permissões para colocar objetos.	Balde	Válido. Os objetos são de propriedade da conta do criador e a política de bucket não se aplica. A conta do criador deve conceder permissões de acesso ao objeto usando ACLs de objeto.	Válido. Os objetos são de propriedade da conta do proprietário do bucket. Aplica-se a política de balde.

Proteção WORM (gravação única e leitura múltipla)

Você pode criar buckets WORM (write-once-read-many) para proteger dados, metadados de objetos definidos pelo usuário e marcação de objetos do S3. Configure os buckets WORM para permitir a criação de novos objetos e evitar substituições ou exclusões de conteúdo existente. Use uma das abordagens descritas aqui.

Para garantir que as substituições sejam sempre negadas, você pode:

- No Grid Manager, vá para **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança** > **Rede e objetos** e marque a caixa de seleção **Impedir modificação do cliente**.
- Aplique as seguintes regras e políticas do S3:
  - Adicione uma operação PutOverwriteObject DENY à política S3.
  - Adicione uma operação DeleteObject DENY à política S3.
  - Adicione uma operação PutObject ALLOW à política S3.

Definir DeleteObject como DENY em uma política do S3 não impede que o ILM exclua objetos quando existe uma regra como "zero cópias após 30 dias".

Mesmo quando todas essas regras e políticas são aplicadas, elas não protegem contra gravações simultâneas (veja Situação A). Eles protegem contra sobrescritas sequenciais concluídas (veja Situação B).

Situação A: Gravações simultâneas (não protegidas)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situação B: Substituições sequenciais concluídas (protegidas contra)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Informações relacionadas

- "Como as regras do StorageGRID ILM gerenciam objetos"
- "Exemplos de políticas de bucket"
- "Exemplo de políticas de grupo"
- "Gerenciar objetos com ILM"
- "Use uma conta de inquilino"

Exemplos de políticas de bucket

Use os exemplos nesta seção para criar políticas de acesso do StorageGRID para buckets.

As políticas de bucket especificam as permissões de acesso para o bucket ao qual a política está anexada. Você configura uma política de bucket usando a API PutBucketPolicy do S3 por meio de uma destas ferramentas:

- "Gerente de inquilinos" .
- AWS CLI usando este comando (consulte"Operações em baldes"):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Exemplo: permitir que todos tenham acesso somente leitura a um bucket

Neste exemplo, todos, incluindo anônimos, têm permissão para listar objetos no bucket e executar operações GetObject em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que esta

política pode não ser particularmente útil porque ninguém, exceto o root da conta, tem permissão para gravar no bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Exemplo: permitir que todos em uma conta tenham acesso total e todos em outra conta tenham acesso somente leitura a um bucket

Neste exemplo, todos em uma conta especificada têm permissão para acesso total a um bucket, enquanto todos em outra conta especificada têm permissão apenas para listar o bucket e executar operações GetObject em objetos no bucket começando com o `shared/` prefixo de chave de objeto.

> No StorageGRID, os objetos criados por uma conta não proprietária (incluindo contas anônimas) são de propriedade da conta do proprietário do bucket. A política de bucket se aplica a esses objetos.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Exemplo: permitir que todos tenham acesso somente leitura a um bucket e acesso total ao grupo especificado

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar operações GetObject em todos os objetos no bucket, enquanto apenas os usuários pertencentes ao grupo `Marketing` na conta especificada têm acesso total.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemplo: permitir que todos tenham acesso de leitura e gravação a um bucket se o cliente estiver no intervalo de IP

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar quaisquer operações de objeto em todos os objetos no bucket, desde que as solicitações venham de um intervalo de IP especificado (54.240.143.0 a 54.240.143.255, exceto 54.240.143.188). Todas as outras operações serão negadas, e todas as solicitações fora do intervalo de IP serão negadas.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Exemplo: permitir acesso total a um bucket exclusivamente por um usuário federado especificado

Neste exemplo, o usuário federado Alex tem acesso total ao `examplebucket` balde e seus objetos. Todos os outros usuários, incluindo `root', têm todas as operações explicitamente negadas. Observe, no entanto, que` root' nunca tem permissões negadas para Put/Get/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemplo: permissão PutOverwriteObject

Neste exemplo, o `Deny` O efeito para PutOverwriteObject e DeleteObject garante que ninguém possa substituir ou excluir os dados do objeto, os metadados definidos pelo usuário e a marcação de objetos do S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Exemplo de políticas de grupo

Use os exemplos nesta seção para criar políticas de acesso do StorageGRID para grupos.

As políticas de grupo especificam as permissões de acesso para o grupo ao qual a política está anexada. Não há `Principal` elemento na política porque está implícito. As políticas de grupo são configuradas usando o Gerenciador de Tenants ou a API.

Exemplo: definir política de grupo usando o Gerenciador de Tenants

Ao adicionar ou editar um grupo no Gerenciador de Tenants, você pode selecionar uma política de grupo para determinar quais permissões de acesso ao S3 os membros desse grupo terão. Ver "Criar grupos para um locatário S3" .

- **Sem acesso S3**: opção padrão. Os usuários neste grupo não têm acesso aos recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar esta opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
- **Acesso somente leitura**: os usuários neste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários neste grupo podem listar objetos e ler dados de objetos, metadados e tags. Quando você seleciona esta opção, a string JSON para uma política de grupo somente leitura aparece na caixa de texto. Você não pode editar esta sequência.
- **Acesso total**: os usuários neste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona esta opção, a string JSON para uma política de grupo de acesso total aparece na caixa de texto. Você não pode editar esta sequência.
- **Mitigação de ransomware**: esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários neste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que tenham o controle de versão de objetos habilitado.

  Usuários do Tenant Manager que têm a permissão Gerenciar todos os buckets podem substituir esta política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação Multifator (MFA) quando disponível.

- **Personalizado**: Os usuários do grupo recebem as permissões que você especifica na caixa de texto.

Exemplo: permitir acesso total do grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm permissão de acesso total a todos os buckets de propriedade da conta do locatário, a menos que seja explicitamente negado pela política de bucket.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemplo: permitir acesso somente leitura do grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm acesso somente leitura aos recursos do S3, a menos que explicitamente negado pela política de bucket. Por exemplo, os usuários neste grupo podem listar objetos e ler dados de objetos, metadados e tags.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemplo: permitir que os membros do grupo tenham acesso total apenas à sua "pasta" em um bucket

Neste exemplo, os membros do grupo só têm permissão para listar e acessar sua pasta específica (prefixo de chave) no bucket especificado. Observe que as permissões de acesso de outras políticas de grupo e da política de bucket devem ser consideradas ao determinar a privacidade dessas pastas.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Operações S3 rastreadas nos logs de auditoria

As mensagens de auditoria são geradas pelos serviços do StorageGRID e armazenadas em arquivos de log de texto. Você pode revisar as mensagens de auditoria específicas do S3 no log de auditoria para obter detalhes sobre as operações de bucket e objeto.

Operações de bucket rastreadas nos logs de auditoria

- CriarBucket
- ExcluirBucket
- ExcluirBucketTagging
- ExcluirObjetos
- Obter marcação de balde
- Balde de cabeça
- Objetos de Lista
- Versões do objeto de lista
- Conformidade do PUT Bucket
- Colocar marcação de balde
- Versão PutBucket

Operações de objetos rastreadas nos logs de auditoria

- Upload completo de várias partes
- CopiarObjeto
- ExcluirObjeto
- ObterObjeto
- CabeçaObjeto
- ColocarObjeto
- RestaurarObjeto
- SelecionarObjeto
- UploadPart (quando uma regra ILM usa ingestão balanceada ou restrita)
- UploadPartCopy (quando uma regra ILM usa ingestão balanceada ou estrita)

Informações relacionadas

- "Arquivo de log de auditoria de acesso"
- "O cliente escreve mensagens de auditoria"
- "O cliente leu mensagens de auditoria"

Informações sobre direitos autorais

Informações sobre marcas comerciais