



USE A API REST DO S3

StorageGRID

NetApp

November 04, 2025

Índice

USE A API REST DO S3	1
S3 versões e atualizações suportadas pela API REST	1
Versões suportadas	1
Atualizações para o suporte à API REST do S3	1
Referência rápida: Solicitações de API S3 suportadas	3
Parâmetros comuns de consulta URI e cabeçalhos de solicitação	4
"AbortMultipartUpload"	4
"CompleteMultipartUpload"	4
"CopyObject"	5
"CreateBucket"	6
"CreateMultipartUpload"	6
>DeleteBucket"	7
>DeleteBucketCors"	7
>DeleteBucketEncryption"	7
>DeleteBucketLifecycle"	7
>DeleteBucketPolicy"	8
>DeleteBucketReplication"	8
>DeleteBucketTagging"	8
>DeleteObject"	8
>DeleteObjects"	9
>DeleteObjectTagging"	9
"GetBucketAcl"	9
"GetBucketCors"	9
"GetBucketEncryption"	10
"GetBucketLifecycleConfiguration"	10
"GetBucketlocalização"	10
"GetBucketNotificationConfiguration"	10
"Política de GetBucketPolicy"	10
"GetBucketReplication"	11
"GetBucketTagging"	11
"GetBucketControle de versão"	11
"GetObject"	11
"GetObjectAcl"	12
"GetObjectLegalHod"	12
"GetObjectLockConfiguration"	13
"GetObjectRetention"	13
"GetObjectTagging"	13
"Balde para a cabeça"	13
"HeadObject"	13
>ListBuckets"	14
>ListMultipartUploads"	14
>ListObjects"	15
>ListObjectsV2"	15

"ListObjectVersions"	15
"ListParts"	16
"PutBucketCors"	16
"PutBucketEncryption"	16
"PutBucketLifecycleConfiguration"	17
"PutBucketNotificationConfiguration"	18
"Política de PutBucketPolicy"	18
"PutBucketReplication"	18
"PutBucketTagging"	19
"PutBucketControle de versão"	19
"PutObject"	19
"PutObjectLegalHod"	20
"PutObjectLockConfiguration"	20
"Retenção PutObjectRetention"	20
"Marcação de objetos"	21
"RestoreObject"	21
"Selecione ObjectContent"	21
"UploadPart"	21
"UploadPartCopy"	22
Teste a configuração da API REST do S3	22
Como o StorageGRID implementa a API REST do S3	24
Solicitações de cliente conflitantes	24
Valores de consistência	24
Controle de versão de objetos	27
Use a API REST do S3 para configurar o bloqueio de objetos do S3	28
Crie a configuração do ciclo de vida do S3	33
Recomendações para a implementação da API REST do S3	38
Suporte para API REST do Amazon S3	39
Detalhes da implementação da API REST do S3	40
Autenticar solicitações	41
Operações no serviço	41
Operações em baldes	42
Operações em objetos	49
Operações para uploads de várias partes	77
Respostas de erro	85
Operações personalizadas do StorageGRID	87
Operações personalizadas do StorageGRID: Visão geral	88
OBTENHA consistência de balde	88
COLOQUE a consistência do balde	90
OBTENHA último tempo de acesso do Bucket	91
COLOQUE o último tempo de acesso do balde	92
ELIMINAR configuração de notificação de metadados do bucket	93
OBTENHA configuração de notificação de metadados do bucket	93
COLOQUE a configuração de notificação de metadados do bucket	97
OBTENHA solicitação de uso de armazenamento	103

Solicitações de bucket obsoletas para conformidade legada	104
Políticas de acesso ao bucket e ao grupo	110
Use políticas de acesso de grupo e bucket	110
Exemplo de políticas de bucket	127
Exemplo de políticas de grupo	133
S3 operações rastreadas nos logs de auditoria	136
Operações de bucket rastreadas nos logs de auditoria	136
Operações de objeto rastreadas nos logs de auditoria	137

USE A API REST DO S3

S3 versões e atualizações suportadas pela API REST

O StorageGRID oferece suporte à API Simple Storage Service (S3), que é implementada como um conjunto de serviços da Web de transferência de Estado representacional (REST).

O suporte à API REST do S3 permite conectar aplicativos orientados a serviços desenvolvidos para serviços da Web do S3 ao storage de objetos no local que usa o sistema StorageGRID. São necessárias alterações mínimas no uso atual de chamadas de API REST do aplicativo cliente S3.

Versões suportadas

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

Item	Versão
Especificação da API S3	"Documentação do Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service"
HTTP	<p>1,1</p> <p>Para obter mais informações sobre HTTP, consulte HTTP/1,1 (RFCs 7230-35).</p> <p>"IETF RFC 2616: Protocolo de transferência de hipertexto (HTTP/1,1)"</p> <p>Nota: O StorageGRID não suporta a canalização HTTP/1,1.</p>

Atualizações para o suporte à API REST do S3

Solte	Comentários
11,8	Atualizado os nomes das operações S3 para corresponder aos nomes usados no "Documentação do Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service" .

Solte	Comentários
11,7	<ul style="list-style-type: none"> • Adicionado "Referência rápida: Solicitações de API S3 suportadas". • Adicionado suporte para usar o modo DE GOVERNANÇA com o bloqueio de objetos S3. • Adicionado suporte para o cabeçalho de resposta específico do StorageGRID <code>x-ntap-sg-cgr-replication-status</code> para OBTER solicitações DE objeto e objeto PRINCIPAL. Este cabeçalho fornece o status de replicação de um objeto para replicação entre grade. • As solicitações <code>SelectObjectContent</code> agora suportam objetos Parquet.
11,6	<ul style="list-style-type: none"> • Adicionado suporte para o uso do <code>partNumber</code> parâmetro Request 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 bloqueio de objetos S3. • Adicionado suporte para a <code>s3:object-lock-remaining-retention-days</code> chave de condição de política para definir o intervalo de períodos de retenção permitidos para seus objetos. • Alterado o tamanho máximo <i>recommended</i> 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 multipart.
11,5	<ul style="list-style-type: none"> • Adicionado suporte para gerenciar a criptografia de bucket. • Adicionado suporte para S3 Object Lock e solicitações de conformidade legadas obsoletas. • Adicionado suporte para o uso DE EXCLUIR vários objetos em buckets versionados. • O <code>Content-MD5</code> cabeçalho de solicitação agora é suportado corretamente.
11,4	<ul style="list-style-type: none"> • Adicionado suporte para EXCLUIR marcação de balde, OBTER marcação de balde e COLOCAR marcação de balde. As etiquetas 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 intervalo no <code>s3:ObjectRestore:Post</code> tipo de evento. • Os limites de tamanho da AWS para peças de várias partes agora são aplicados. Cada parte em um upload de várias partes deve estar entre 5 MiB e 5 GiB. A última parte pode ser menor do que 5 MiB. • Adicionado suporte para TLS 1,3

Solte	Comentários
11,3	<ul style="list-style-type: none"> • Adicionado suporte para criptografia no lado do servidor de dados de objeto com chaves fornecidas pelo cliente (SSE-C). • Adicionado suporte para as operações DE ELIMINAÇÃO, OBTENÇÃO e COLOCAÇÃO do ciclo de vida do balde (apenas ação de expiração) e para o <code>x-amz-expiration</code> cabeçalho de resposta. • PUT Object, put Object - Copy e Multipart Upload atualizados para descrever o impactos das regras ILM que usam o posicionamento síncrono na ingestão. • As cifras TLS 1,1 não são mais suportadas.
11,2	<p>Adicionado suporte para restauração PÓS-objeto para uso com Cloud Storage Pools. Adicionado suporte para o uso da 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.</p> <p>Observação: os usos de ARN/URN em outra configuração JSON/XML, incluindo aqueles usados em recursos personalizados do StorageGRID, não foram alterados.</p>
11,1	Adicionado suporte para compartilhamento de recursos entre origens (CORS), HTTP para conexões de clientes S3 para 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 a consistência disponível.
10,4	Adicionado suporte para alterações de verificação de ILM para controle de versão, atualizações de página de nomes de domínio de endpoints, 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 de várias partes (Upload de peça - cópia).
10,1	Adicionado suporte para upload em várias partes, solicitações virtuais de estilo hospedado e autenticação v4.1X.
10,0	Suporte inicial da API REST do S3 pelo sistema StorageGRID. A versão atualmente suportada da <i>Simple Storage Service API Reference</i> é 2006-03-01.

Referência rápida: Solicitações de API S3 suportadas

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

Esta página inclui apenas as operações S3 com suporte do StorageGRID.



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

Parâmetros comuns de consulta URI e cabeçalhos de solicitação

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

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

Salvo indicação em contrário, 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 do S3"](#)
- ["Referência da API do Amazon Simple Storage Service: Cabeçalhos de solicitação comuns"](#)

"AbortMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para esta solicitação, além deste parâmetro de consulta URI adicional:

- `uploadId`

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações para uploads de várias partes"](#)

"CompleteMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para esta solicitação, além deste parâmetro de consulta URI adicional:

- uploadId

Solicitar tags XML do corpo

O StorageGRID suporta essas tags XML do corpo de solicitação:

- CompleteMultipartUpload
- ETag
- Part
- PartNumber

Documentação do StorageGRID

["CompleteMultipartUpload"](#)

"CopyObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além desses 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 do pedido

Nenhum

Documentação do StorageGRID

["CopyObject"](#)

"CreateBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além desses cabeçalhos adicionais:

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

Corpo do pedido

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

Documentação do StorageGRID

["Operações em baldes"](#)

"CreateMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além desses cabeçalhos adicionais:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- 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 do pedido

Nenhum

Documentação do StorageGRID

["CreateMultipartUpload"](#)

"DeleteBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Documentação do StorageGRID

["Operações em baldes"](#)

"DeleteBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"DeleteBucketEncryption"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"DeleteBucketLifecycle"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

- ["Operações em baldes"](#)
- ["Crie a configuração do ciclo de vida do S3"](#)

"DeleteBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"DeleteBucketReplication"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"DeleteBucketTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"DeleteObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além deste cabeçalho de solicitação adicional:

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

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em objetos"](#)

"DeleteObjects"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além deste cabeçalho de solicitação adicional:

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

Corpo do pedido

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

Documentação do StorageGRID

["Operações em objetos"](#)

"DeleteObjectTagging"

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em objetos"](#)

"GetBucketAcl"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"GetBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"GetBucketEncryption"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"GetBucketLifecycleConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

- ["Operações em baldes"](#)
- ["Crie a configuração do ciclo de vida do S3"](#)

"GetBucketlocalização"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"GetBucketNotificationConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"Política de GetBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"GetBucketReplication"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"GetBucketTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"GetBucketControle de versão"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"GetObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros de consulta URI adicionais:

- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding

- response-content-language
- response-content-type
- response-expires

E esses 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 do pedido

Nenhum

Documentação do StorageGRID

["GetObject"](#)

"GetObjectAcl"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em objetos"](#)

"GetObjectLegalHod"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#)

"GetObjectLockConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#)

"GetObjectRetention"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#)

"GetObjectTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em objetos"](#)

"Balde para a cabeça"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"HeadObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além desses cabeçalhos adicionais:

- 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 do pedido

Nenhum

Documentação do StorageGRID

["HeadObject"](#)

"ListBuckets"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Nenhum

Documentação do StorageGRID

[Operações no serviço](#) > [ListBuckets](#)

"ListMultipartUploads"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além desses parâmetros adicionais:

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

Corpo do pedido

Nenhum

Documentação do StorageGRID

["ListMultipartUploads"](#)

"ListObjects"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além desses parâmetros adicionais:

- delimiter
- encoding-type
- marker
- max-keys
- prefix

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ListObjectsV2"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além desses parâmetros adicionais:

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

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ListObjectVersions"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além desses parâmetros adicionais:

- delimiter

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

Corpo do pedido

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ListParts"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além desses parâmetros adicionais:

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

Corpo do pedido

Nenhum

Documentação do StorageGRID

["ListMultipartUploads"](#)

"PutBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de 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 tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Solicitar tags XML do corpo

O StorageGRID suporta essas tags XML do corpo de solicitação:

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentação do StorageGRID

["Operações em baldes"](#)

"PutBucketLifecycleConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Solicitar tags XML do corpo

O StorageGRID suporta essas tags XML do corpo de solicitação:

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

Documentação do StorageGRID

- ["Operações em baldes"](#)
- ["Crie a configuração do ciclo de vida do S3"](#)

"PutBucketNotificationConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Solicitar tags XML do corpo

O StorageGRID suporta essas tags XML do corpo de solicitação:

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

Documentação do StorageGRID

["Operações em baldes"](#)

"Política de PutBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Para obter detalhes sobre os campos de corpo JSON suportados, "[Use políticas de acesso de grupo e bucket](#)" consulte .

"PutBucketReplication"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Solicitar tags XML do corpo

- Bucket
- Destination
- Prefix
- ReplicationConfiguration

- Rule
- Status
- StorageClass

Documentação do StorageGRID

["Operações em baldes"](#)

"PutBucketTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

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

Documentação do StorageGRID

["Operações em baldes"](#)

"PutBucketControle de versão"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Solicitar parâmetros do corpo

O StorageGRID suporta estes parâmetros do corpo do pedido:

- VersioningConfiguration
- Status

Documentação do StorageGRID

["Operações em baldes"](#)

"PutObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação, além desses cabeçalhos adicionais:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- 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 do pedido

- Dados binários do objeto

Documentação do StorageGRID

"PutObject"

"PutObjectLegalHod"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de 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 objetos do S3"

"PutObjectLockConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de 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 objetos do S3"

"Retenção PutObjectRetention"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para esta solicitação, além deste cabeçalho adicional:

- x-amz-bypass-governance-retention

Corpo do pedido

O StorageGRID oferece suporte a todos os parâmetros de corpo de 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 objetos do S3](#)"

"Marcação de objetos"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

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

Documentação do StorageGRID

"[Operações em objetos](#)"

"RestoreObject"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

Para obter detalhes sobre os campos corpo suportados, "[RestoreObject](#)" consulte .

"Selecione ObjectContent"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a tudo [parâmetros e cabeçalhos comuns](#) para essa solicitação.

Corpo do pedido

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

- "[Utilize S3 Select \(Selecionar\)](#)"
- "[Selecione ObjectContent](#)"

"UploadPart"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `partNumber`
- `uploadId`

E esses cabeçalhos de solicitação adicionais:

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

- x-amz-server-side-encryption-customer-key-MD5

Corpo do pedido

- Dados binários da peça

Documentação do StorageGRID

["UploadPart"](#)

"UploadPartCopy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID suporta tudo [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros de consulta URI adicionais:

- partNumber
- uploadId

E esses 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 do pedido

Nenhum

Documentação do StorageGRID

["UploadPartCopy"](#)

Teste a configuração da API REST do S3

Você pode usar a interface de linha de comando (AWS CLI) do Amazon Web Services para testar sua conexão com o sistema e verificar se é possível ler e gravar objetos.

Antes de começar

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

Para obter detalhes sobre essas etapas, ["Configurar conexões de cliente"](#)consulte .

Passos

1. Configure as configurações da AWS CLI para usar a conta criada no sistema StorageGRID:
 - a. Entre no modo de configuração: `aws configure`
 - b. Introduza a ID da chave de acesso para a conta que criou.
 - c. Introduza a chave de acesso secreta para a conta que criou.
 - d. Introduza a região predefinida a utilizar. 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 tenha configurado um endpoint 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 êxito, a localização do bucket será retornada, como visto no exemplo a seguir:

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

3. Carregue 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, um Etag é retornado 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. Elimine o balde.

```
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 de cliente conflitantes

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

O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Valores de consistência

A consistência fornece um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de storage e locais. 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 seguindo um PUT concluído com sucesso será capaz de ler os dados recém-escritos. As 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 em uma consistência diferente, você pode:

- Especifique uma consistência para [cada baldeio](#) .
- Especifique uma consistência para [Cada operação da API](#)o .
- Altere a consistência padrão em toda a grade executando uma das seguintes tarefas:
 - No Gerenciador de Grade, vá para **CONFIGURATION > System > Storage settings > Default consistency**.
 - .



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

Valores de consistência

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

Você pode definir a consistência de um bucket ou 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.
- **Read-after-novo-write:** (Padrão) fornece consistência de leitura-após-gravação para novos objetos e eventual consistência 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 do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.

Use a consistência "Read-after-new-write" e "Available"

Quando uma operação HEAD ou GET usa a consistência "Read-after-new-write", o StorageGRID realiza a pesquisa em várias etapas, como segue:

- Ele primeiro procura o objeto usando uma baixa consistência.
- Se essa pesquisa falhar, ela repete a pesquisa no próximo valor de consistência até atingir uma consistência equivalente ao comportamento para strong-global.

Se uma operação HEAD ou GET usa a consistência "Read-after-new-write", mas o objeto não existe, a pesquisa de objeto sempre alcançará uma consistência equivalente ao comportamento para strong-global. Como essa consistência exige que várias cópias dos metadados de objetos estejam disponíveis em cada local, você pode receber um número alto de erros de servidor interno do 500 se dois ou mais nós de storage no mesmo local não estiverem disponíveis.

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

Especifique a consistência para a operação da API

Para definir a consistência para 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.

Especifique a consistência para o bucket

Para definir a consistência do bucket, você pode usar a solicitação StorageGRID ["COLOQUE a consistência do balde"](#). Ou você pode ["altere a consistência de um balde"](#) do Gerente do Locatário.

Ao definir a consistência de um balde, tenha em atenção o seguinte:

- Definir a consistência de um bucket determina qual consistência é usada para operações S3D executadas nos objetos no bucket ou na configuração do bucket. Não afeta as operações no próprio balde.
- A consistência de uma operação de API individual substitui a consistência do bucket.
- Em geral, os intervalos devem usar a consistência padrão, "Read-after-new-write". 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 balde apenas como último recurso.

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

Tanto a sua escolha de consistência quanto a sua regra ILM afetam a forma 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 exige acesso aos metadados de um objeto e aos dados para atender às solicitações do cliente, selecionar níveis de proteção correspondentes para o comportamento de consistência e ingestão pode fornecer melhor proteção de dados iniciais e respostas do sistema mais previsíveis.

Estão disponíveis as seguintes ["opções de ingestão"](#) regras para ILM:

Commit duplo

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

Rigoroso

Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja devolvido 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 locais com a seguinte regra ILM e a seguinte consistência:

- **Regra ILM:** Crie duas cópias de objeto, uma no local e outra em um local remoto. Use um comportamento rigoroso de ingestão.
- **Consistência:** Strong-global (metadados de objetos são imediatamente distribuídos para todos os sites).

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

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

Se, em vez disso, você usou a mesma regra ILM e a consistência do site forte, o cliente pode receber uma mensagem de sucesso depois que os dados do objeto são replicados para o site remoto, mas antes que os metadados do objeto sejam distribuídos lá. Nesse caso, o nível de proteção dos metadados de objetos não corresponde ao nível de proteção dos dados de 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. Contacte a NetApp se necessitar de assistência.

Controle de versão de objetos

Você pode definir o estado de controle de versão de um bucket se quiser reter várias versões de cada objeto. Ativar 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 1.000 versões de cada objeto.

O controle de versão de objetos pode ser combinado com o gerenciamento do ciclo de vida das informações do StorageGRID (ILM) 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 ativado 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) Excluir não é compatível.



O controle de versão pode ser ativado somente em buckets criados com o StorageGRID versão 10,3 ou posterior.

ILM e versionamento

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

Para objetos S3 em buckets habilitados para versionamento, o suporte para versionamento permite criar

regras ILM que usam "tempo não atual" como tempo de referência (selecione **Sim** para a pergunta, "aplicar esta regra apenas a versões de objetos mais antigos?" no "[Etapa 1 do assistente criar uma regra ILM](#)"). Quando um objeto é atualizado, suas versões anteriores se tornam não atuais. O uso de um filtro "tempo não atual" permite criar políticas que reduzem o impactos de armazenamento de versões anteriores de objetos.



Quando você carrega uma nova versão de um objeto usando uma operação de upload multipart, o tempo não atual para a versão original do objeto reflete quando o upload multipart foi criado para a nova versão, não quando o upload multipart foi concluído. Em casos limitados, o tempo não atual para a versão original pode ser horas ou dias antes do tempo para a versão atual.

Informações relacionadas

- "[Como objetos com versão S3 são excluídos](#)"
- "[Regras e políticas do ILM para objetos com versão S3 \(exemplo 4\)](#)".

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

Se a configuração global de bloqueio de objetos S3 estiver ativada para o seu sistema StorageGRID, você poderá criar buckets com o bloqueio de objetos S3 ativado. Você pode especificar a retenção padrão para cada bucket ou configurações de retenção para cada versão do objeto.

Como ativar o bloqueio de objetos S3D para um balde

Se a configuração global de bloqueio de objetos S3 estiver ativada para o seu sistema StorageGRID, você poderá ativar opcionalmente o bloqueio de objetos S3 quando criar cada bucket.

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

Para ativar o bloqueio de objetos S3D para um bucket, use um destes métodos:

- Crie o bucket usando o Gerenciador do locatário. "[Crie um balde S3D](#)."Consulte .
- Crie o bucket usando uma solicitação CreateBucket com o `x-amz-bucket-object-lock-enabled` cabeçalho da solicitação. "[Operações em baldes](#)"Consulte .

O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando o bucket é criado. Não é possível suspender o controle de versão para o bucket. "[Controle de versão de objetos](#)"Consulte .

Configurações de retenção padrão para um balde

Quando o bloqueio de objetos S3D está ativado para um bucket, você pode opcionalmente habilitar a retenção padrão para o bucket e especificar um modo de retenção padrão e um período de retenção padrão.

Modo de retenção predefinido

- No modo DE CONFORMIDADE:
 - O objeto não pode ser excluído até que sua data de retenção seja alcançada.
 - O `retent-until-date` do objeto pode ser aumentado, mas não pode ser diminuído.

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

Período de retenção predefinido

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

Como definir a retenção padrão para um balde

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

- Gerencie as configurações do balde a partir do Gerenciador do Locatário. ["Crie um bucket do S3"](#) Consulte e ["Atualização S3 retenção padrão bloqueio Objeto"](#).
- Emita uma solicitação `PutObjectLockConfiguration` para que o bucket especifique 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 com o bloqueio de objetos S3 ativado. Você também pode remover as configurações de retenção padrão configuradas anteriormente.

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

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

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

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

Exemplo de solicitação

Este exemplo habilita o bloqueio de objetos S3 para um bucket e define o modo de retenção padrão para CONFORMIDADE e o período de retenção padrão para 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 balde

Para determinar se o bloqueio de objeto S3 está ativado para um bucket e para ver o modo de retenção e o período de retenção padrão, use um destes métodos:

- Veja o bucket no Gerenciador do Locatário. ["Veja os baldes do S3"](#)Consulte .
- Emita uma solicitação `GetObjectLockConfiguration`.

`GetObjectLockConfiguration`

A solicitação `GetObjectLockConfiguration` permite que você determine se o bloqueio de objeto S3 está ativado para um bucket e, se ele está ativado, veja se há um modo de retenção padrão e período de retenção configurados para o bucket.

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

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

Exemplo de solicitação

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

Exemplo de resposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
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 bloqueio de objetos S3 ativado pode conter uma combinação de objetos com e sem as configurações de retenção do bloqueio de objetos S3.

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 para o bucket.

Você pode especificar as seguintes configurações para cada objeto:

- **Modo de retenção:** CONFORMIDADE ou GOVERNANÇA.
- **Retent-until-date:** Uma data especificando quanto tempo a versão do objeto deve ser mantida pelo StorageGRID.

- No modo DE CONFORMIDADE, se a data de retenção estiver no futuro, o objeto pode ser recuperado, mas não pode ser modificado ou excluído. A data de retenção até pode ser aumentada, mas esta data não pode ser diminuída ou removida.
- No MODO DE GOVERNANÇA, os usuários com permissão especial podem ignorar a configuração reter até a data. Eles podem excluir uma versão de objeto antes que seu período de retenção tenha decorrido. 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 colocar uma retenção legal em um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até que seja explicitamente removida.

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

Para especificar as configurações de bloqueio de objetos do S3 ao adicionar uma versão de objeto a um bucket, emita uma solicitação `"PutObject"`, `"CopyObject"` ou `"CreateMultipartUpload"`.

Você pode usar o seguinte:

- `x-amz-object-lock-mode`, Que pode ser CONFORMIDADE ou GOVERNANÇA (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 ATIVADA (sensível a maiúsculas e minúsculas), o objeto é colocado sob uma retenção legal. Se a retenção legal estiver DESLIGADA, nenhuma retenção legal será colocada. Qualquer outro valor resulta em um erro de 400 Bad Request (InvalidArgument).

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

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

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

Como atualizar as configurações de retenção para um objeto

Se você precisar atualizar as configurações de retenção legal ou retenção para uma versão de objeto existente, poderá executar as seguintes operações de subrecursos de objeto:

- `PutObjectLegalHold`

Se o novo valor de retenção legal estiver ATIVADO, o objeto será colocado sob uma retenção legal. Se o valor de retenção legal estiver DESLIGADO, a retenção legal é levantada.

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

Como usar o modo DE GOVERNANÇA

Os usuários que têm a `s3:BypassGovernanceRetention` permissão podem ignorar as configurações de retenção ativa de um objeto que usa o modo DE GOVERNANÇA. Qualquer operação DE EXCLUSÃO ou `PutObjectRetention` deve incluir o `x-amz-bypass-governance-retention:true` cabeçalho da solicitação. Esses usuários podem executar essas operações adicionais:

- Execute as operações `DeleteObject` ou `DeleteObjects` para excluir uma versão do objeto antes de seu período de retenção ter decorrido.

Os objetos que estão sob uma retenção legal não podem ser excluídos. A retenção legal deve estar DESLIGADA.

- Execute as operações `PutObjectRetention` que alteram o modo DE uma versão DE objeto DE GOVERNANÇA para CONFORMIDADE 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 de objeto.

Informações relacionadas

- ["Gerencie objetos com o S3 Object Lock"](#)
- ["Use o bloqueio de objetos S3D para reter objetos"](#)
- ["Guia do usuário do Amazon Simple Storage Service: Usando o bloqueio de objeto S3"](#)

Crie a configuração do ciclo de vida do S3

Você pode criar uma configuração de ciclo de vida do S3 para controlar quando objetos

específicos são excluídos do sistema StorageGRID.

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

Qual é a configuração do ciclo de vida

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

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

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

Cada objeto segue as configurações de retenção de um ciclo de vida do bucket do S3 ou de uma política de ILM. Quando um ciclo de vida do bucket do S3 é configurado, as ações de expiração do ciclo de vida substituem a política ILM para objetos que correspondam ao filtro do ciclo de vida do bucket. Os objetos que não correspondem ao filtro do ciclo de vida do bucket usam as configurações de retenção da política ILM. Se um objeto corresponder a um filtro do ciclo de vida do bucket e nenhuma ação de expiração for explicitamente especificada, as configurações de retenção da política ILM não serão usadas e está implícito que as versões do objeto serão mantidas para sempre. ["Exemplos de prioridades para o ciclo de vida do bucket do S3 e a política de ILM"](#)Consulte .

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



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

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

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Criar configuração do ciclo de vida

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

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



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

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

```

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

```


Aplique a configuração do ciclo de vida ao bucket

Depois de criar o arquivo de configuração do ciclo de vida, você o aplica a um bucket emitindo uma solicitação `PutBucketLifecycleConfiguration`.

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

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

Para validar que uma configuração de ciclo de vida foi aplicada com sucesso ao bucket, emita uma solicitação `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.

Valide que 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 um `Expiration` parâmetro que indica quando o objeto expira e qual regra de expiração foi correspondida.



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

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

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

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

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

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

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

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

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



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

Recomendações para a implementação da API REST do S3

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

Recomendações para heads to non-existent objects

Se o aplicativo verificar 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 dirigir um local antes DE COLOCÁ-lo.

Caso contrário, se a operação PRINCIPAL não encontrar o objeto, poderá receber um número elevado de erros de servidor interno 500 se dois ou mais nós de armazenamento no mesmo local não estiverem disponíveis ou se um local remoto não estiver acessível.

Você pode definir a consistência "disponível" para cada bucket usando a ["COLOQUE a consistência do balde"](#)

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

Recomendações para chaves de objeto

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

Buckets criados no StorageGRID 11,4 ou anterior

- Não use valores aleatórios como os primeiros quatro caracteres de chaves de objeto. Isso contrasta com a antiga recomendação da AWS para prefixos-chave. Em vez disso, use prefixos não aleatórios e não exclusivos, como `image`.
- Se você seguir a antiga recomendação da AWS para 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 objeto para atender às práticas recomendadas de desempenho. Na maioria dos casos, você pode usar valores aleatórios para os primeiros quatro caracteres de nomes de chave de objeto.



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

```
/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg
```

Recomendações para "leituras de intervalo"

Se o ["opção global para comprimir objetos armazenados"](#) estiver ativado, os aplicativos cliente S3 devem evitar executar operações `GetObject` que especificam um intervalo de bytes que sejam retornados. Essas operações de "leitura de intervalo" são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As 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 a partir de objetos compactados, as solicitações do cliente podem expirar.



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

Suporte para API REST do Amazon S3

Detalhes da implementação da API REST do S3

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

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

Tratamento da data

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

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

Cabeçalhos de solicitação comuns

O sistema StorageGRID suporta os cabeçalhos de solicitação comuns definidos pelo ["Referência da API do Amazon Simple Storage Service: Cabeçalhos de solicitação comuns"](#), com uma exceção.

Cabeçalho da solicitação	Implementação
Autorização	Suporte completo para AWS Signature versão 2 Suporte para AWS Signature versão 4, com as seguintes exceções: <ul style="list-style-type: none">• O valor SHA256 não é calculado para o corpo da solicitação. O valor enviado pelo usuário é aceito sem validação, como se o valor <code>UNSIGNED-PAYLOAD</code> tivesse sido fornecido para o <code>x-amz-content-sha256</code> cabeçalho.
<code>x-amz-security-token</code>	Não implementado. Retorna <code>XNotImplemented</code> .

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
<code>x-amz-id-2</code>	Não utilizado

Autenticar solicitações

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

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

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

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

Use o cabeçalho de autorização HTTP

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

Use parâmetros de consulta

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

Operações no serviço

O sistema StorageGRID suporta as seguintes operações no serviço.

Operação	Implementação
ListBuckets (Anteriormente chamado GET Service)	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio.
OBTER uso de armazenamento	A solicitação do StorageGRID " OBTER uso de armazenamento " informa a quantidade total de storage 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 (<code>?x-ntap-sg-usage</code>) adicionado.
OPÇÕES /	Os aplicativos clientes podem emitir <code>OPTIONS</code> / solicitações para a porta S3 em um nó de storage, sem fornecer credenciais de autenticação S3.1X, para determinar se o nó de storage está disponível. Você pode usar essa solicitação para monitoramento ou permitir que balanceadores de carga externos identifiquem quando um nó de storage está inativo.

Operações em baldes

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

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

Consulte o seguinte para obter mais informações:

- ["Guia do usuário do Amazon Simple Storage Service: Restrições e limitações de bucket"](#)
- ["Configurar nomes de domínio de endpoint S3"](#)

As operações ListObjects (GET Bucket) e ListObjectVersions (GET Bucket object versions) suportam StorageGRID ["valores de consistência"](#).

Você pode verificar se as atualizações para a última hora de acesso estão ativadas ou desativadas para buckets individuais. ["OBTENHA o último tempo de acesso do Bucket"](#) Consulte .

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

Operação	Implementação
CreateBucket	<p>Cria um novo balde. Ao criar o balde, você se torna o proprietário do balde.</p> <ul style="list-style-type: none"> Os nomes dos buckets devem estar em conformidade com as seguintes regras: <ul style="list-style-type: none"> Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário). Deve ser compatível com DNS. Deve conter pelo menos 3 e não mais de 63 caracteres. Pode ser uma série de uma ou mais etiquetas, com etiquetas adjacentes separadas por um período. Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens. Não deve se parecer com um endereço IP formatado em texto. Não deve usar períodos em solicitações de estilo hospedadas virtuais. Os períodos causarão problemas com a verificação do certificado curinga do servidor. Por padrão, os intervalos são criados na <code>us-east-1</code> região; no entanto, você pode usar o <code>LocationConstraint</code> elemento de solicitação no corpo da solicitação para especificar uma região diferente. Ao usar o <code>LocationConstraint</code> elemento, você deve especificar o nome exato de uma região que foi definida usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Contacte o administrador do sistema se não souber o nome da região que deve utilizar. <p>Nota: Ocorrerá um erro se a solicitação do CreateBucket usar uma região que não foi definida no StorageGRID.</p> <ul style="list-style-type: none"> Você pode incluir o <code>x-amz-bucket-object-lock-enabled</code> cabeçalho de solicitação para criar um bucket com o bloqueio de objeto S3 ativado. "Use a API REST do S3 para configurar o bloqueio de objetos do S3"Consulte . <p>Você deve ativar o bloqueio de objeto S3 quando você criar o bucket. Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação de um bucket. O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.</p>
DeleteBucket	Elimina o balde.
DeleteBucketCors	Exclui a configuração CORS para o bucket.
DeleteBucketEncryption	Exclui a criptografia padrão do intervalo. Os objetos criptografados existentes permanecem criptografados, mas todos os novos objetos adicionados ao bucket não são criptografados.
DeleteBucketLifecycle	Exclui a configuração do ciclo de vida do bucket. "Crie a configuração do ciclo de vida do S3" Consulte .

Operação	Implementação
DeleteBucketPolicy	Exclui a política anexada ao bucket.
DeleteBucketReplication	Exclui a configuração de replicação anexada ao bucket.
DeleteBucketTagging	<p>Usa o <code>tagging</code> subrecurso para remover todas as tags de um bucket.</p> <p>Atenção: Se uma tag de política ILM não padrão for definida para esse intervalo, haverá uma <code>NTAP-SG-ILM-BUCKET-TAG</code> tag de intervalo com um valor atribuído a ele. Não emita uma solicitação de identificação de <code>DeleteBucketTagging</code> se houver uma <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de intervalo. Em vez disso, emita uma solicitação <code>PutBucketTagging</code> com apenas a <code>NTAP-SG-ILM-BUCKET-TAG</code> tag e seu valor atribuído para remover todas as outras tags do bucket. Não modifique nem remova a <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta do balde.</p>
GetBucketAcl	Retorna uma resposta positiva e a ID, DisplayName e permissão do proprietário do bucket, indicando que o proprietário tem acesso total ao bucket.
GetBucketCors	Retorna a <code>cors</code> configuração para o bucket.
GetBucketEncryption	Retorna a configuração de criptografia padrão para o bucket.
GetBucketLifecycleConfiguration (Anteriormente chamado GET Bucket Lifecycle)	Retorna a configuração do ciclo de vida do bucket. "Crie a configuração do ciclo de vida do S3" Consulte .
GetBucketlocalização	Retorna a região que foi definida usando o <code>LocationConstraint</code> elemento na solicitação <code>CreateBucket</code> . Se a região do bucket for <code>us-east-1</code> , uma string vazia será retornada para a região.
GetBucketNotificationConfiguration (Anteriormente chamado GET Bucket notificação)	Retorna a configuração de notificação anexada ao bucket.
Política de GetBucketPolicy	Retorna a política anexada ao bucket.
GetBucketReplication	Retorna a configuração de replicação anexada ao bucket.

Operação	Implementação
GetBucketTagging	<p>Usa o <code>tagging</code> subrecurso para retornar todas as tags para um bucket.</p> <p>Atenção: Se uma tag de política ILM não padrão for definida para esse intervalo, haverá uma <code>NTAP-SG-ILM-BUCKET-TAG</code> tag de intervalo com um valor atribuído a ele. Não modifique nem remova esta etiqueta.</p>
GetBucketControle de versão	<p>Essa implementação usa <code>versioning</code> o subrecurso para retornar o estado de controle de versão de um bucket.</p> <ul style="list-style-type: none"> • <i>Blank</i>: O controle de versão nunca foi habilitado (bucket é "não versionado") • Habilitado: O controle de versão está habilitado • Suspenso: O controle de versão foi ativado anteriormente e está suspenso
GetObjectLockConfigurati on	<p>Retorna o modo de retenção padrão do bucket e o período de retenção padrão, se configurado.</p> <p>"Use a API REST do S3 para configurar o bloqueio de objetos do S3" Consulte .</p>
Balde para a cabeça	<p>Determina se existe um intervalo e você tem permissão para acessá-lo.</p> <p>Esta operação retorna:</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: O UUID do bucket no formato UUID. • <code>x-ntap-sg-trace-id</code>: O ID de rastreamento exclusivo da solicitação associada.
ListObjects e ListObjectsV2 (Anteriormente chamado GET Bucket)	<p>Retorna alguns ou todos (até 1.000) dos objetos em um bucket. A Classe de armazenamento para objetos pode ter um de dois valores, mesmo que o objeto tenha sido ingerido com a <code>REDUCED_REDUNDANCY</code> opção de classe de armazenamento:</p> <ul style="list-style-type: none"> • <code>STANDARD</code>, Que indica que o objeto está armazenado em um pool de storage que consiste em nós de storage. • <code>GLACIER</code>, Que indica que o objeto foi movido para o bucket externo especificado pelo pool de armazenamento em nuvem. <p>Se o intervalo contiver um grande número de chaves excluídas que tenham o mesmo prefixo, a resposta pode incluir algumas <code>CommonPrefixes</code> que não contêm chaves.</p>
ListObjectVersions (Anteriormente CHAMADO OBTER versões de objetos bucket)	<p>Com <code>ACESSO DE LEITURA</code> em um bucket, o uso dessa operação com o <code>versions</code> subrecurso lista metadados de todas as versões de objetos no bucket.</p>

Operação	Implementação
PutBucketCors	Define a configuração do CORS para um bucket de modo que o bucket possa atender às solicitações de origem cruzada. O compartilhamento de recursos de origem cruzada (CORS) é um mecanismo de segurança que permite que aplicativos da Web do cliente em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket S3 chamado <code>images</code> para armazenar gráficos. Ao definir a configuração CORS para o <code>images</code> intervalo, pode permitir que as imagens nesse intervalo sejam apresentadas no website <code>http://www.example.com</code> .
PutBucketEncryption	<p>Define o estado de encriptação predefinido de um intervalo existente. Quando a criptografia no nível do bucket está ativada, todos os novos objetos adicionados ao bucket são criptografados. O StorageGRID suporta criptografia no lado do servidor com chaves gerenciadas pelo StorageGRID. Ao especificar a regra de configuração de criptografia do lado do servidor, defina o <code>SSEAlgorithm</code> parâmetro como <code>AES256</code>, e não use o <code>KMSMasterKeyID</code> parâmetro.</p> <p>A configuração de criptografia padrão do bucket é ignorada se a solicitação de upload de objeto já especificar criptografia (ou seja, se a solicitação incluir o <code>x-amz-server-side-encryption-*</code> cabeçalho da solicitação).</p>
PutBucketLifecycleConfiguration (Anteriormente chamado PUT Bucket Lifecycle)	<p>Cria uma nova configuração de ciclo de vida para o bucket ou substitui uma configuração de ciclo de vida existente. O StorageGRID dá suporte a até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML:</p> <ul style="list-style-type: none"> • Expiração (dias, Data, ExpiredObjectDeleteMarker) • Não-currentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtro (prefixo, Tag) • Estado • ID <p>O StorageGRID não oferece suporte a essas ações:</p> <ul style="list-style-type: none"> • AbortIncompleteMultipartUpload • Transição <p>"Crie a configuração do ciclo de vida do S3" Consulte . Para entender como a ação de expiração em um ciclo de vida do bucket interage com as instruções de colocação do ILM, "Como o ILM opera ao longo da vida de um objeto" consulte .</p> <p>Nota: A configuração do ciclo de vida do bucket pode ser usada com buckets que têm o S3 Object Lock ativado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis com o legado.</p>

Operação	Implementação
<p>PutBucketNotificationConfiguration</p> <p>(Anteriormente chamada DE NOTIFICAÇÃO PUT Bucket)</p>	<p>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:</p> <ul style="list-style-type: none"> • O StorageGRID oferece suporte a tópicos do Amazon Simple Notification Service (Amazon SNS) ou 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 a URNA de um endpoint do StorageGRID. Os endpoints podem ser criados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário. <p>O endpoint deve existir para que a configuração de notificação seja bem-sucedida. Se o endpoint não existir, um 400 Bad Request erro é retornado com o código InvalidArgument.</p> <ul style="list-style-type: none"> • Não é possível configurar uma notificação para os seguintes tipos de eventos. Esses tipos de eventos são não suportados. <ul style="list-style-type: none"> ◦ <code>s3:ReducedRedundancyLostObject</code> ◦ <code>s3:ObjectRestore:Completed</code> • As notificações de eventos enviadas do StorageGRID usam o formato JSON padrão, exceto que elas não incluem algumas chaves e usam valores específicos para outras, como mostrado na lista a seguir: <ul style="list-style-type: none"> ◦ EventSource <code>sgws:s3</code> ◦ AwsRegion não incluído ◦ x-amz-id-2 não incluído ◦ arn <code>urn:sgws:s3:::bucket_name</code>
<p>Política de PutBucketPolicy</p>	<p>Define a política anexada ao bucket. "Use políticas de acesso de grupo e bucket" Consulte .</p>

Operação	Implementação
PutBucketReplication	<p data-bbox="475 153 1485 296">Configura "Replicação do StorageGRID CloudMirror" para o bucket usando o XML de configuração de replicação fornecido no corpo da solicitação. Para a replicação do CloudMirror, você deve estar ciente dos seguintes detalhes de implementação:</p> <ul data-bbox="500 327 1485 852" style="list-style-type: none"> <li data-bbox="500 327 1485 499">• O StorageGRID suporta apenas V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do <code>Filter</code> elemento para regras e segue convenções V1 para exclusão de versões de objetos. Para obter detalhes, "Guia do usuário do Amazon Simple Storage Service: Configuração de replicação" consulte . <li data-bbox="500 516 1485 583">• A replicação do bucket pode ser configurada em buckets versionados ou não versionados. <li data-bbox="500 600 1485 701">• Você pode especificar um intervalo de destino diferente em cada regra do XML de configuração de replicação. Um bucket de origem pode ser replicado para mais de um bucket de destino. <li data-bbox="500 718 1485 852">• Os buckets de destino devem ser especificados como a URN dos endpoints do StorageGRID, conforme especificado no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. "Configurar a replicação do CloudMirror" Consulte . <p data-bbox="521 884 1485 1062">O endpoint deve existir para que a configuração de replicação seja bem-sucedida. Se o endpoint não existir, a solicitação falhará como um 400 Bad Request. a mensagem de erro indica: Unable to save the replication policy. The specified endpoint URN does not exist: <i>URN</i>.</p> <ul data-bbox="500 1094 1485 1545" style="list-style-type: none"> <li data-bbox="500 1094 1485 1161">• Não é necessário especificar um <code>Role</code> no XML de configuração. Este valor não é usado pelo StorageGRID e será ignorado se enviado. <li data-bbox="500 1178 1485 1245">• Se você omitir a classe de armazenamento do XML de configuração, o StorageGRID usará a <code>STANDARD</code> classe de armazenamento por padrão. <li data-bbox="500 1262 1485 1545">• Se você excluir um objeto do bucket de origem ou excluir o bucket de origem, o comportamento de replicação entre regiões é o seguinte: <ul data-bbox="548 1356 1485 1545" style="list-style-type: none"> <li data-bbox="548 1356 1485 1423">◦ Se você excluir o objeto ou o bucket antes que ele tenha sido replicado, o objeto/bucket não será replicado e você não será notificado. <li data-bbox="548 1440 1485 1545">◦ Se você excluir o objeto ou o bucket depois que ele foi replicado, o StorageGRID segue o comportamento padrão de exclusão do Amazon S3 para V1 TB de replicação entre regiões.

Operação	Implementação
PutBucketTagging	<p>Usa o <code>tagging</code> subrecurso para adicionar ou atualizar um conjunto de tags para um bucket. Ao adicionar etiquetas de bucket, esteja ciente das seguintes limitações:</p> <ul style="list-style-type: none"> • O StorageGRID e o Amazon S3 suportam até 50 tags para cada bucket. • As tags associadas a um bucket devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento. • Os valores de tag podem ter até 256 caracteres Unicode de comprimento. • Chave e valores são sensíveis a maiúsculas e minúsculas. <p>Atenção: Se uma tag de política ILM não padrão for definida para esse intervalo, haverá uma <code>NTAP-SG-ILM-BUCKET-TAG</code> tag de intervalo com um valor atribuído a ele. Certifique-se de que a <code>NTAP-SG-ILM-BUCKET-TAG</code> tag bucket está incluída com o valor atribuído em todas as solicitações <code>PutBucketTagging</code>. Não modifique nem remova esta etiqueta.</p> <p>Nota: Esta operação irá substituir quaisquer tags atuais que o bucket já tenha. Se quaisquer tags existentes forem omitidas do conjunto, essas tags serão removidas para o intervalo.</p>
PutBucketControle de versão	<p>Usa o <code>versioning</code> subrecurso para definir o estado de controle de versão de um bucket existente. Você pode definir o estado de controle de versão com um dos seguintes valores:</p> <ul style="list-style-type: none"> • Habilitado: Permite o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo. • Suspensão: Desativa o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão <code>null</code>.
PutObjectLockConfigurati on	<p>Configura ou remove o modo de retenção padrão do bucket e o período de retenção padrão.</p> <p>Se o período de retenção padrão for modificado, a data de retenção até as versões de objetos existentes permanecerá a mesma e não será recalculada usando o novo período de retenção padrão.</p> <p>"Use a API REST do S3 para configurar o bloqueio de objetos do S3" Consulte para obter informações detalhadas.</p>

Operações em objetos

Operações em objetos

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

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

- Os StorageGRID "[valores de consistência](#)" são suportados por todas as operações em objetos, com exceção dos seguintes:
 - `GetObjectAcl`
 - `OPTIONS /`
 - `PutObjectLegalHod`
 - `Retenção PutObjectRetention`
 - `Selecione ObjectContent`
- As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.
- Todos os objetos em um bucket do StorageGRID são de propriedade do proprietário do bucket, incluindo objetos criados por um usuário anônimo ou por outra conta.
- Os objetos de dados ingeridos para o sistema StorageGRID através do Swift não podem ser acedidos através do S3.

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

Operação	Implementação
DeleteObject	<p data-bbox="591 163 1451 226">Autenticação multifator (MFA) e o cabeçalho de resposta <code>x-amz-mfa</code> não são suportados.</p> <p data-bbox="591 264 1485 499">Ao processar uma solicitação de DeleteObject, o StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais armazenados. Se for bem-sucedido, o StorageGRID retornará uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas dentro de 30 segundos (por exemplo, porque um local está temporariamente indisponível), o StorageGRID coloca as cópias em fila para remoção e, em seguida, indica sucesso para o cliente.</p> <p data-bbox="591 537 841 562">Controle de versão</p> <p data-bbox="631 579 1485 747">Para remover uma versão específica, o solicitante deve ser o proprietário do bucket e usar o <code>versionId</code> subrecurso. O uso deste subrecurso exclui permanentemente a versão. Se o <code>versionId</code> corresponder a um marcador de exclusão, o cabeçalho de resposta <code>x-amz-delete-marker</code> será retornado como <code>true</code>.</p> <ul data-bbox="656 789 1485 1226" style="list-style-type: none"> • Se um objeto for excluído sem o <code>versionId</code> subrecurso em um bucket habilitado para versão, isso resultará na geração de um marcador de exclusão. O <code>versionId</code> para o marcador de exclusão é retornado usando o <code>x-amz-version-id</code> cabeçalho de resposta e o <code>x-amz-delete-marker</code> cabeçalho de resposta é retornado como <code>true</code>. • Se um objeto for excluído sem o <code>versionId</code> sub-recurso em um bucket suspenso de versão, ele resultará em uma exclusão permanente de uma versão 'null' já existente ou um marcador 'null' delete, e a geração de um novo marcador 'null' delete. O <code>x-amz-delete-marker</code> cabeçalho de resposta é retornado definido como <code>true</code>. <p data-bbox="680 1268 1451 1331">Nota: Em certos casos, vários marcadores de exclusão podem existir para um objeto.</p> <p data-bbox="591 1373 1485 1478">"Use a API REST do S3 para configurar o bloqueio de objetos do S3" Consulte para saber como excluir versões de objetos no MODO DE GOVERNANÇA.</p>
DeleteObjects (Anteriormente CHAMADO EXCLUIR vários objetos)	<p data-bbox="591 1539 1451 1602">Autenticação multifator (MFA) e o cabeçalho de resposta <code>x-amz-mfa</code> não são suportados.</p> <p data-bbox="591 1640 1354 1703">Vários objetos podem ser excluídos na mesma mensagem de solicitação.</p> <p data-bbox="591 1745 1485 1850">"Use a API REST do S3 para configurar o bloqueio de objetos do S3" Consulte para saber como excluir versões de objetos no MODO DE GOVERNANÇA.</p>

Operação	Implementação
DeleteObjectTagging	<p>Usa o <code>tagging</code> subrecurso para remover todas as tags de um objeto.</p> <p>Controle de versão</p> <p>Se o <code>versionId</code> parâmetro de consulta não for especificado na solicitação, a operação excluirá todas as tags da versão mais recente do objeto em um bucket com versão. Se a versão atual do objeto for um marcador de exclusão, um status "MethodNotAllowed" é retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.</p>
GetObject	"GetObject"
GetObjectAcl	Se as credenciais de acesso necessárias forem fornecidas para a conta, a operação retornará uma resposta positiva e a ID, DisplayName e permissão do proprietário do objeto, indicando que o proprietário tem acesso total ao objeto.
GetObjectLegalHod	"Use a API REST do S3 para configurar o bloqueio de objetos do S3"
GetObjectRetention	"Use a API REST do S3 para configurar o bloqueio de objetos do S3"
GetObjectTagging	<p>Usa o <code>tagging</code> subrecurso para retornar todas as tags para um objeto.</p> <p>Controle de versão</p> <p>Se o <code>versionId</code> 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" é retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.</p>
HeadObject	"HeadObject"
RestoreObject	"RestoreObject"
PutObject	"PutObject"
CopyObject (Anteriormente chamado PUT Object - Copy)	"CopyObject"
PutObjectLegalHod	"Use a API REST do S3 para configurar o bloqueio de objetos do S3"
Retenção PutObjectRetention	"Use a API REST do S3 para configurar o bloqueio de objetos do S3"

Operação	Implementação
<p>Marcação de objetos</p>	<p>Usa o <code>tagging</code> subrecurso para adicionar um conjunto de tags a um objeto existente.</p> <p>Limites da etiqueta do objeto</p> <p>Você pode adicionar tags a novos objetos ao enviá-los ou adicioná-los a objetos existentes. O StorageGRID e o Amazon S3 suportam até 10 tags para cada objeto. Tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento e os valores de tag podem ter até 256 caracteres Unicode de comprimento. Chave e valores são sensíveis a maiúsculas e minúsculas.</p> <p>Tag atualizações e comportamento de ingestão</p> <p>Quando você usa <code>PutObjectTagging</code> para atualizar as tags de um objeto, o StorageGRID não reingere o objeto. Isso significa que a opção de comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento de objetos que são acionadas pela atualização são feitas quando o ILM é reavaliado por processos normais de ILM em segundo plano.</p> <p>Isso significa que se a regra ILM usar a opção estrita para o comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objeto necessários não puderem ser feitos (por exemplo, porque um local recém-exigido não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível.</p> <p>Resolução de conflitos</p> <p>As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.</p> <p>Controle de versão</p> <p>Se o <code>versionId</code> parâmetro de consulta não for especificado na solicitação, a operação adicionará tags à versão mais recente do objeto em um bucket com versão. Se a versão atual do objeto for um marcador de exclusão, um status <code>"MethodNotAllowed"</code> é retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.</p>
<p>Selecione ObjectContent</p>	<p>"Selecione ObjectContent"</p>

Utilize S3 Select (Selecionar)

O StorageGRID oferece suporte às seguintes cláusulas, tipos de dados e operadores do Amazon S3 Select para o ["SelectObjectContent - comando"](#).



Nenhum item não listado não é suportado.

Para obter a sintaxe, "[Selecione ObjectContent](#)" consulte . Para obter mais informações sobre S3 Select, consulte "[Documentação da AWS para o S3 Select](#)".

Apenas as contas de inquilino que tenham S3 Select ativado podem emitir consultas SelectObjectContent. Consulte "[Considerações e requisitos para usar o S3 Select](#)".

Cláusulas

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

Tipos de dados

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

Operadores

Operadores lógicos

- E
- NÃO
- OU

Operadores de comparação

- *
- >
- <
- >
- .
- .
- >
- !
- ENTRE
- EM

Operadores de correspondência de padrões

- GOSTO
- _
- %

Operadores unitários

- É NULO
- NÃO É NULL

Operadores de matemática

- E
- -
- *
- /
- %

O StorageGRID segue a precedência do operador Amazon S3 Select.

Agregar funções

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

Funções condicionais

- CASO
- COALESCE
- NULLIF

Funções de conversão

- CAST (para tipos de dados suportados)

Funções de data

- DATE_ADD
- DATE_DIFF
- EXTRAIR
- TO_STRING
- TO_TIMESTAMP

- UTCNOW

Funções de cadeia de caracteres

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

Use a criptografia do lado do servidor

A criptografia do lado do servidor permite proteger os dados do objeto em repouso. O StorageGRID criptografa os dados enquanto grava o objeto e descriptografa os dados quando você acessa o objeto.

Se você quiser usar a criptografia do lado do servidor, você pode escolher uma das duas opções mutuamente exclusivas, com base em como as chaves de criptografia são gerenciadas:

- **SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID):** Quando você emite uma solicitação S3 para armazenar um objeto, o StorageGRID criptografa o objeto com uma chave exclusiva. Quando você emite uma solicitação S3 para recuperar o objeto, o StorageGRID usa a chave armazenada para descriptografar o objeto.
- **SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente):** Quando você emite uma solicitação S3 para armazenar um objeto, você fornece sua própria chave de criptografia. Quando você recupera um objeto, você fornece a mesma chave de criptografia como parte de sua solicitação. Se as duas chaves de criptografia corresponderem, o objeto será descriptografado e seus dados de objeto serão retornados.

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



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



Se um objeto for criptografado com SSE ou SSE-C, quaisquer configurações de criptografia no nível de bucket ou no nível de grade serão ignoradas.

Use SSE

Para criptografar um objeto com uma chave exclusiva gerenciada pelo StorageGRID, use o seguinte cabeçalho de solicitação:

```
x-amz-server-side-encryption
```

O cabeçalho de solicitação SSE é suportado pelas seguintes operações de objeto:

- "PutObject"
- "CopyObject"

- ["CreateMultipartUpload"](#)

Use SSE-C

Para criptografar um objeto com uma chave exclusiva que você gerencia, use três cabeçalhos de solicitação:

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

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

- ["GetObject"](#)
- ["HeadObject"](#)
- ["PutObject"](#)
- ["CopyObject"](#)
- ["CreateMultipartUpload"](#)
- ["UploadPart"](#)
- ["UploadPartCopy"](#)

Considerações sobre o uso de criptografia no lado do servidor com chaves fornecidas pelo cliente (SSE-C)

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

- Você deve usar https.



O StorageGRID rejeita quaisquer solicitações feitas por http ao usar SSE-C. Para considerações de segurança, você deve considerar qualquer chave que você enviar acidentalmente usando http para ser comprometida. Elimine a chave e rode-a conforme adequado.

- O ETag na resposta não é o MD5 dos dados do objeto.
- É necessário gerenciar o mapeamento de chaves de criptografia para objetos. O StorageGRID não armazena chaves de criptografia. Você é responsável por rastrear a chave de criptografia fornecida para cada objeto.
- Se seu bucket estiver habilitado para versionamento, cada versão do objeto deve ter sua própria chave de criptografia. Você é responsável por rastrear a chave de criptografia usada para cada versão do objeto.

- Como você gerencia chaves de criptografia no lado do cliente, você também deve gerenciar quaisquer proteções adicionais, como rotação de chaves, no lado do cliente.



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

- Se a replicação entre grade 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 \(SSE-C\)"](#)

CopyObject

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

Resolver conflitos

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Tamanho do objeto

O tamanho máximo *recomendado* para uma única operação PutObject é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use ["carregamento multipart"](#) em vez disso.

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



Se você atualizou do StorageGRID 11,6 ou anterior, o alerta COLOCAR tamanho do objeto muito grande S3 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 com o padrão AWS S3, futuras versões do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

UTF-8 caracteres em metadados do usuário

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

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

- As solicitações são bem-sucedidas se os metadados definidos pelo usuário incluírem caracteres UTF-8 escapados.
- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome ou valor da chave 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 de nome-valor contendo metadados definidos pelo usuário
- x-amz-metadata-directive: O valor padrão é COPY, que permite copiar o objeto e os metadados associados.

Você pode especificar REPLACE para substituir os metadados existentes ao copiar o objeto ou para atualizar os metadados do objeto.

- x-amz-storage-class
- x-amz-tagging-directive: O valor padrão é COPY, que permite copiar o objeto e todas as tags.

Você pode especificar REPLACE para substituir as tags existentes ao copiar o objeto ou para atualizar as tags.

- S3 cabeçalhos de solicitação de bloqueio de objetos:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do intervalo serão usadas para calcular o modo de versão do objeto e manter até a data. ["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#) Consulte .

- Cabeçalhos de pedido SSE:

- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

Consulte [Cabeçalhos de solicitação para criptografia do lado do servidor](#)

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-website-redirect-location

Opções de classe de armazenamento

O `x-amz-storage-class` cabeçalho de solicitação é suportado e afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM correspondente usar o compromisso duplo ou equilibrado "[opção de ingestão](#)".

- STANDARD

(Padrão) especifica uma operação de ingestão de commit duplo quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

- REDUCED_REDUNDANCY

Especifica uma operação de ingestão de commit único quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.



Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a REDUCED_REDUNDANCY opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a REDUCED_REDUNDANCY opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Usando x-amz-copy-source em CopyObject

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

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

- Não é possível usar 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, o StorageGRID rejeita a solicitação e retorna `XNotImplemented`.
- A opção de comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento de objetos que são acionadas pela atualização são feitas quando o ILM é reavaliado por processos normais de ILM em segundo plano.

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

Cabeçalhos de solicitação para criptografia do lado do servidor

Se "[use a criptografia do lado do servidor](#)" você, os cabeçalhos de solicitação fornecidos dependem se o objeto de origem está criptografado e se você planeja criptografar o objeto de destino.

- Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deve incluir os três cabeçalhos a seguir na solicitação CopyObject, para que o objeto possa ser descriptografado e copiado:
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar AES256.
 - `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia fornecida quando você criou o objeto de origem.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu quando criou o objeto de origem.
- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva que você fornece e gerencia, inclua os três cabeçalhos a seguir:
 - `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256.
 - `x-amz-server-side-encryption-customer-key`: Especifique uma nova chave de criptografia para o objeto de destino.
 - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da nova chave de criptografia.



As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações para "[usando criptografia do lado do servidor](#)".

- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva gerenciada pelo StorageGRID (SSE), inclua esse cabeçalho na solicitação de CopyObject:

- `x-amz-server-side-encryption`



O `server-side-encryption` valor do objeto não pode ser atualizado. Em vez disso, faça uma cópia com um novo `server-side-encryption` valor usando `x-amz-metadata-directive: REPLACE`.

Controle de versão

Se o bucket de origem for versionado, você pode usar o `x-amz-copy-source` cabeçalho para copiar a versão mais recente de um objeto. Para copiar uma versão específica de um objeto, você deve especificar explicitamente a versão a ser copiada usando o `versionId` subrecurso. Se o intervalo de destino for versionado, a versão gerada será retornada `x-amz-version-id` no cabeçalho de resposta. Se o controle de versão estiver suspenso para o bucket de destino, `x-amz-version-id` retorna um valor "nulo".

GetObject

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

Objetos GetObject e multipart

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

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

UTF-8 caracteres em metadados do usuário

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

Cabeçalho de pedido não suportado

O seguinte cabeçalho de solicitação não é suportado e retorna `XNotImplemented`:

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

Controle de versão

Se um `versionId` sub-recurso não for especificado, a operação busca a versão mais recente do objeto em um bucket com versão. Se a versão atual do objeto for um marcador de exclusão, um status "não encontrado" é retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Cabeçalhos de solicitação para criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use todos os três cabeçalhos se o objeto for criptografado com uma chave exclusiva que você forneceu.

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



As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações no ["Use a criptografia do lado do servidor"](#).

Comportamento do GetObject para objetos de pool de storage de nuvem

Se um objeto tiver sido armazenado em um ["Cloud Storage Pool"](#), o comportamento de uma solicitação GetObject depende do estado do objeto. ["HeadObject"](#) Consulte para obter mais detalhes.



Se um objeto for armazenado em um pool de armazenamento em nuvem e uma ou mais cópias do objeto também existirem na grade, as solicitações `GetObject` tentarão recuperar dados da grade, antes de recuperá-los do pool de armazenamento em nuvem.

Estado do objeto	Comportamento de <code>GetObject</code>
Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento	200 OK Uma cópia do objeto é recuperada.
Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável	200 OK Uma cópia do objeto é recuperada.
Objeto transicionado para um estado não recuperável	403 Forbidden, InvalidObjectState Use uma "RestoreObject" solicitação para restaurar o objeto para um estado recuperável.
Objeto em processo de restauração a partir de um estado não recuperável	403 Forbidden, InvalidObjectState Aguarde até que a solicitação de <code>RestoreObject</code> seja concluída.
Objeto totalmente restaurado para o Cloud Storage Pool	200 OK Uma cópia do objeto é recuperada.

Objetos segmentados ou multiparte em um pool de armazenamento em nuvem

Se você carregou um objeto multipart ou se o StorageGRID dividir um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no pool de armazenamento em nuvem amostrando um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação `GetObject` pode retornar incorretamente 200 OK quando algumas partes do objeto já tiverem sido transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não tiverem sido restauradas.

Nestes casos:

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

Replicação `GetObject` e cross-grid

Se você estiver usando ["federação de grade"](#) e ["replicação entre grade"](#) 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 cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

Grelha	Estado da replicação
Fonte	<ul style="list-style-type: none"> • SUCESSO: A replicação foi bem-sucedida. • PENDENTE: O objeto ainda não foi replicado. • FAILURE: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	<ul style="list-style-type: none"> • RÉPLICA*: O objeto foi replicado a partir da grade de origem.



O StorageGRID não suporta o `x-amz-replication-status` colhedor.

HeadObject

Você pode usar a solicitação S3 HeadObject para recuperar metadados de um objeto sem retornar o próprio objeto. Se o objeto for armazenado em um pool de armazenamento em nuvem, você poderá usar o HeadObject para determinar o estado de transição do objeto.

Objetos HeadObject e multipart

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

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

UTF-8 caracteres em metadados do usuário

O StorageGRID não analisa nem interpreta caracteres UTF-8 escapados 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 ou valor da chave incluir caracteres não imprimíveis.

Cabeçalho de pedido não suportado

O seguinte cabeçalho de solicitação não é suportado e retorna `XNotImplemented`:

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

Controle de versão

Se um `versionId` sub-recurso não for especificado, a operação busca a versão mais recente do objeto em um bucket com versão. Se a versão atual do objeto for um marcador de exclusão, um status "não encontrado" é retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Cabeçalhos de solicitação para criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use os três cabeçalhos se o objeto for criptografado com uma chave exclusiva que você forneceu.

- `x-amz-server-side-encryption-customer-algorithm`: 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 que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações no ["Use a criptografia do lado do servidor"](#).

Respostas do HeadObject para objetos Pool de storage de nuvem

Se o objeto for armazenado em a ["Cloud Storage Pool"](#), os seguintes cabeçalhos de resposta serão retornados:

- `x-amz-storage-class`: GLACIER
- `x-amz-restore`

Os cabeçalhos de resposta fornecem informações sobre o estado de um objeto à medida que ele é movido para um pool de armazenamento em nuvem, opcionalmente transferido para um estado não recuperável e restaurado.

Estado do objeto	Resposta ao HeadObject
Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento	200 OK (Nenhum cabeçalho de resposta especial é retornado.)
Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável	200 OK <code>x-amz-storage-class</code> : GLACIER "X-amz-restore: Ongoing-request", data de expiração"Sat, 23 de julho de 20 2030 00:00:00 GMT" Até que o objeto seja transferido para um estado não recuperável, o valor para <code>expiry-date</code> é definido para algum tempo distante no futuro. A hora exata da transição não é controlada pelo sistema StorageGRID.

Estado do objeto	Resposta ao HeadObject
O objeto fez a transição para o estado não recuperável, mas pelo menos uma cópia também existe na grade	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>"X-amz-restore: Ongoing-request", data de expiração"Sat, 23 de julho de 20 2030 00:00:00 GMT"</p> <p>O valor para expiry-date é definido para algum tempo distante no futuro.</p> <p>Nota: Se a cópia na grade não estiver disponível (por exemplo, um nó de armazenamento está inativo), você deve emitir uma "RestoreObject" solicitação para restaurar a cópia do pool de armazenamento em nuvem antes de recuperar o objeto com êxito.</p>
Objeto transicionado para um estado não recuperável e nenhuma cópia existe na grade	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
Objeto em processo de restauração a partir de um estado não recuperável	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>"x-amz-restore:</p>
Objeto totalmente restaurado para o Cloud Storage Pool	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>"X-amz-restore: Ongoing-request", data de expiração"Sat, 23 de julho de 20 2018 00:00:00 GMT"</p> <p>O expiry-date indica quando o objeto no pool de armazenamento em nuvem será retornado a um estado não recuperável.</p>

Objetos segmentados ou multiparte no Cloud Storage Pool

Se você carregou um objeto multipart ou se o StorageGRID dividir um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no pool de armazenamento em nuvem amostrando um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação de HeadObject pode retornar incorretamente "x-amz-restore: Ongoing-request" quando algumas partes do objeto já foram transferidas para um estado não-recuperável ou quando algumas partes do objeto ainda não foram restauradas.

Replicação de HeadObject e cross-grid

Se você estiver usando ["federação de grade"](#) e ["replicação entre grade"](#) estiver habilitado para um bucket, o cliente S3 poderá verificar o status de replicação de um objeto emitindo uma solicitação de HeadObject. A

resposta inclui o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

Grelha	Estado da replicação
Fonte	<ul style="list-style-type: none">• SUCESSO: A replicação foi bem-sucedida.• PENDENTE: O objeto ainda não foi replicado.• FAILURE: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	<ul style="list-style-type: none">• RÉPLICA*: O objeto foi replicado a partir da grade de origem.



O StorageGRID não suporta o `x-amz-replication-status` colhedor.

PutObject

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

Resolver conflitos

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Tamanho do objeto

O tamanho máximo *recomendado* para uma única operação PutObject é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use "[carregamento multipart](#)" em vez disso.

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



Se você atualizou do StorageGRID 11,6 ou anterior, o alerta COLOCAR tamanho do objeto muito grande S3 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 com o padrão AWS S3, futuras versões 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 dentro de cada cabeçalho de SOLICITAÇÃO PUT para 2 KB. O StorageGRID limita os metadados do usuário a 24 KiB. O tamanho dos metadados definidos pelo usuário é medido tomando a soma do número de bytes na codificação UTF-8 de cada chave e valor.

UTF-8 caracteres em metadados do usuário

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

O StorageGRID não analisa nem interpreta caracteres UTF-8 escapados incluídos no nome da chave ou no

valor dos metadados definidos pelo usuário. Os caracteres UTF-8 escapados são tratados como caracteres ASCII:

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

Limites da etiqueta do objeto

Você pode adicionar tags a novos objetos ao enviá-los ou adicioná-los a objetos existentes. O StorageGRID e o Amazon S3 suportam até 10 tags para cada objeto. Tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento e os valores de tag podem ter até 256 caracteres Unicode de comprimento. Chave e valores são sensíveis a maiúsculas e minúsculas.

Propriedade do objeto

No StorageGRID, todos os objetos são de propriedade da conta de proprietário do bucket, incluindo objetos criados por uma conta não proprietária ou um usuário anônimo.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- Cache-Control
- Content-Disposition
- Content-Encoding

Quando você especifica `aws-chunked` para Content-Encoding StorageGRID não verifica os seguintes itens:

- O StorageGRID não verifica o `chunk-signature` contra os dados de bloco.
- O StorageGRID não verifica o valor que você fornece `x-amz-decoded-content-length` em relação ao objeto.

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

A codificação de transferência Chunked é suportada se `aws-chunked` a assinatura de payload também for usada.

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

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


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

Se você quiser usar a opção **tempo de criação definido pelo usuário** como tempo de referência para uma regra ILM, você deve usar `creation-time` como o nome dos metadados que Registram quando o objeto foi criado. Por exemplo:

```
x-amz-meta-creation-time: 1443399726
```

O valor para `creation-time` é avaliado em segundos desde 1 de janeiro de 1970.



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

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

Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do intervalo serão usadas para calcular o modo de versão do objeto e manter até a data. ["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#) Consulte .

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

Consulte [Cabeçalhos de solicitação para criptografia do lado do servidor](#)

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- O `x-amz-acl` cabeçalho da solicitação não é suportado.
- O `x-amz-website-redirect-location` cabeçalho da solicitação não é suportado e retorna `XNotImplemented`.

Opções de classe de armazenamento

O `x-amz-storage-class` cabeçalho da solicitação é suportado. O valor enviado para `x-amz-storage-class` afeta a forma como o StorageGRID protege os dados de objetos durante a ingestão e não quantas

cópias persistentes do objeto são armazenadas no sistema StorageGRID (que é determinado pelo ILM).

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

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

- **STANDARD (Predefinição)**
 - *** Commit duplo***: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, assim que um objeto é ingerido, uma segunda cópia desse objeto é criada e distribuída para um nó de armazenamento diferente (commit duplo). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais satisfazem as instruções de colocação na regra. Caso contrário, novas cópias de objetos podem precisar ser feitas em locais diferentes e as cópias provisórias iniciais podem precisar ser excluídas.
 - **Balanced**: Se a regra ILM especificar a opção Balanced e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes nós de storage.

Se o StorageGRID puder criar imediatamente todas as cópias de objeto especificadas na regra ILM (colocação síncrona), `x-amz-storage-class` o cabeçalho não terá efeito.

- **REDUCED_REDUNDANCY**
 - **Commit duplo**: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, o StorageGRID cria uma única cópia provisória à medida que o objeto é ingerido (commit único).
 - **Balanced**: Se a regra ILM especificar a opção Balanced, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito. A `REDUCED_REDUNDANCY` opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso, o uso `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia de objeto extra para cada operação de ingestão.

A utilização da `REDUCED_REDUNDANCY` opção não é recomendada noutras circunstâncias.

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



Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Especificar `REDUCED_REDUNDANCY` apenas afeta quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Ele não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas ativas de ILM e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.



Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a `REDUCED_REDUNDANCY` opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Cabeçalhos de solicitação para criptografia do lado do servidor

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

- **SSE:** Use o seguinte cabeçalho se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID.
 - `x-amz-server-side-encryption`
- **SSE-C:** Use todos os três cabeçalhos se você quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
 - `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256.
 - `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.
 - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.



As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações para ["usando criptografia do lado do servidor"](#).



Se um objeto for criptografado com SSE ou SSE-C, quaisquer configurações de criptografia no nível de bucket ou no nível de grade serão ignoradas.

Controle de versão

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

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

Cálculos de assinatura para o cabeçalho de autorização

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

- O StorageGRID não requer `host` que os cabeçalhos sejam incluídos no `CanonicalHeaders`.
- O StorageGRID não precisa `Content-Type` ser incluído no `CanonicalHeaders`.
- O StorageGRID não requer `x-amz-*` que os cabeçalhos sejam incluídos no `CanonicalHeaders`.



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

Para obter detalhes, "[Cálculos de assinatura para o cabeçalho de autorização: Transferência de carga útil em uma única bloco \(assinatura AWS versão 4\)](#)" consulte .

Informações relacionadas

["Gerenciar objetos com ILM"](#)

RestoreObject

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

Tipo de solicitação suportada

O `StorageGRID` suporta apenas solicitações de `RestoreObject` para restaurar um objeto. Não suporta o `SELECT` tipo de restauração. Selecione `Requests Return` (retornar solicitações `XNotImplemented`).

Controle de versão

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

Comportamento do RestoreObject em objetos de pool de storage de nuvem

Se um objeto tiver sido armazenado em um "[Cloud Storage Pool](#)", uma solicitação de `RestoreObject` tem o seguinte comportamento, com base no estado do objeto. "[HeadObject](#)" Consulte para obter mais detalhes.



Se um objeto for armazenado em um pool de armazenamento em nuvem e uma ou mais cópias do objeto também existirem na grade, não haverá necessidade de restaurar o objeto emitindo uma solicitação de `RestoreObject`. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação `GetObject`.

Estado do objeto	Comportamento do RestoreObject
Objeto ingerido no <code>StorageGRID</code> , mas ainda não avaliado pelo ILM, ou objeto não está em um pool de storage de nuvem	403 Forbidden, InvalidObjectState
Objeto no <code>Cloud Storage Pool</code> , mas ainda não transicionado para um estado não recuperável	200 OK Nenhuma alteração é feita. Nota: Antes de um objeto ser transferido para um estado não recuperável, não é possível alterar o seu <code>expiry-date</code> .

Estado do objeto	Comportamento do RestoreObject
Objeto transicionado para um estado não recuperável	<p>202 Accepted Restaura uma cópia recuperável do objeto para o pool de armazenamento em nuvem pelo número de dias especificado no corpo da solicitação. No final desse período, o objeto é retornado a um estado não recuperável.</p> <p>Opcionalmente, use o <code>Tier</code> elemento de solicitação para determinar quanto tempo o trabalho de restauração levará para concluir (<code>Expedited</code>, <code>Standard</code> ou <code>Bulk</code>). Se você não especificar <code>Tier</code>, o <code>Standard</code> nível será usado.</p> <p>Importante: Se um objeto tiver sido transferido para o S3 Glacier Deep Archive ou se o Cloud Storage Pool usar o armazenamento Azure Blob, não será possível restaurá-lo usando o <code>Expedited</code> nível. O seguinte erro é retornado 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.</p>
Objeto em processo de restauração a partir de um estado não recuperável	409 Conflict, RestoreAlreadyInProgress
Objeto totalmente restaurado para o Cloud Storage Pool	<p>200 OK</p> <p>Nota: se um objeto foi restaurado para um estado recuperável, você pode alterar o mesmo <code>expiry-date</code> reemitindo a solicitação de <code>RestoreObject</code> com um novo valor para <code>Days</code>. A data de restauração é atualizada em relação à hora da solicitação.</p>

Selecione ObjectContent

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

Para obter mais informações, ["Referência da API do Amazon Simple Storage Service: SelectObjectContent"](#) consulte .

Antes de começar

- A conta de locatário tem a permissão S3 Select (Selecionar).
- Você tem `s3:GetObject` permissão para o objeto que deseja consultar.
- O objeto que você deseja consultar deve estar em um dos seguintes formatos:
 - **CSV**. Pode ser usado como está ou comprimido em arquivos GZIP ou bzip2.
 - **Parquet**. Requisitos adicionais para objetos em Parquet:
 - S3 Select suporta apenas compactação colunar usando GZIP ou Snappy. S3 Select não suporta compactação de objetos inteiros para objetos Parquet.
 - S3 a seleção não suporta saída em Parquet. Você deve especificar o formato de saída como CSV ou JSON.
 - O tamanho máximo do grupo de linhas não comprimidas é de 512 MB.

- Você deve usar os tipos de dados especificados no esquema do objeto.
- Você não pode usar os tipos lógicos INTERVALO, JSON, LISTA, HORA ou UUID.
- Sua expressão SQL tem um comprimento máximo de 256 KB.
- Qualquer Registro na entrada ou resultados tem um comprimento máximo de 1 MIB.

Exemplo de sintaxe de solicitação 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 de 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, 2010 populações, 2015 populações estimadas e a porcentagem de mudança dos dados do censo americano. Registros no arquivo que não são estados são ignorados.

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

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

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

Exemplo de uso da AWS-CLI (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, são assim:

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


Exemplo de uso da 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, são assim:

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

Operações para uploads de várias partes

Operações para uploads de várias partes: Visão geral

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

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

- Você não deve exceder 1.000 carregamentos simultâneos de várias partes para um único bucket, porque os resultados das consultas ListMultipartUploads para esse bucket podem retornar resultados incompletos.
- O StorageGRID impõe limites de tamanho da AWS para peças multipeças. S3 os clientes devem seguir estas diretrizes:
 - Cada parte em um upload de várias partes deve estar entre 5 MIB (5.242.880 bytes) e 5 GiB (5.368.709.120 bytes).
 - A última parte pode ser menor que 5 MIB (5.242.880 bytes).
 - Em geral, os tamanhos das peças devem ser tão grandes quanto possível. Por exemplo, use tamanhos de peças de 5 GiB para um objeto de 100 GiB. Como cada peça é considerada um objeto exclusivo, o uso de tamanhos grandes de peças reduz a sobrecarga de metadados do StorageGRID.
 - Para objetos menores que 5 GiB, considere usar upload não multipart.
- O ILM é avaliado para cada parte de um objeto multipart à medida que é ingerido e para o objeto como um todo quando o upload multipart é concluído, se a regra ILM usa o balanced ou strict ["opção de ingestão"](#). Você deve estar ciente de como isso afeta o posicionamento do objeto e da peça:
 - Se o ILM mudar enquanto um upload multipart S3 estiver em andamento, algumas partes do objeto podem não atender aos requisitos atuais do ILM quando o upload multipart for concluído. Qualquer

peça que não seja colocada corretamente está na fila para reavaliação ILM e movida para o local correto mais tarde.

- Ao avaliar o ILM para uma peça, o StorageGRID filtra o tamanho da peça, não o tamanho do objeto. Isso significa que partes de um objeto podem ser armazenadas em locais que não atendem aos requisitos de ILM para o objeto como um todo. Por exemplo, se uma regra especifica que todos os objetos de 10 GB ou maior são armazenados em DC1 enquanto todos os objetos menores são armazenados em DC2, cada parte de 1 GB de um upload multipart de 10 partes é armazenada em DC2 na ingestão. No entanto, quando ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.
- Todas as operações de upload multipart suportam StorageGRID ["valores de consistência"](#).
- Quando um objeto é ingerido utilizando o carregamento em várias partes, o ["Limite de segmentação de objetos \(1 GiB\)"](#) não é aplicado.
- Conforme necessário, você pode usar ["criptografia do lado do servidor"](#) com uploads de várias partes. Para usar SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID), você inclui o `x-amz-server-side-encryption` cabeçalho da solicitação somente na solicitação `CreateMultipartUpload`. Para usar SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente), você especifica os mesmos três cabeçalhos de solicitação de chave de criptografia na solicitação `CreateMultipartUpload` e em cada solicitação de `UploadPart` subsequente.

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

CompleteMultipartUpload

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

Resolver conflitos

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o

sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Cabeçalhos de solicitação

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

- STANDARD

(Padrão) especifica uma operação de ingestão de commit duplo quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

- REDUCED_REDUNDANCY

Especifica uma operação de ingestão de commit único quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.



Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a REDUCED_REDUNDANCY opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a REDUCED_REDUNDANCY opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.



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



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

Controle de versão

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

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

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



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

Falha na replicação, notificação ou notificação de metadados

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

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

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

CreateMultipartUpload

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

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

Se a regra ILM que corresponde a um objeto ingerido usar o strict "opção de ingestão", o `x-amz-storage-class` cabeçalho não terá efeito.

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

- **STANDARD (Predefinição)**
 - *** Commit duplo***: Se a regra ILM especificar a opção ingestão de commit duplo, assim que um objeto é ingerido, uma segunda cópia desse objeto é criada e distribuída para um nó de armazenamento diferente (commit duplo). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais satisfazem as instruções de colocação na regra. Caso contrário, novas cópias de objetos podem precisar ser feitas em locais diferentes e as cópias provisórias iniciais podem precisar ser excluídas.
 - **Balanced**: Se a regra ILM especificar a opção Balanced e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes nós de storage.

Se o StorageGRID puder criar imediatamente todas as cópias de objeto especificadas na regra ILM (colocação síncrona), `x-amz-storage-class` o cabeçalho não terá efeito.

- **REDUCED_REDUNDANCY**
 - **Commit duplo**: Se a regra ILM especificar a opção Commit duplo, o StorageGRID cria uma única cópia provisória à medida que o objeto é ingerido (commit único).
 - **Balanced**: Se a regra ILM especificar a opção Balanced, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito. A **REDUCED_REDUNDANCY** opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso, o uso **REDUCED_REDUNDANCY** elimina a criação e exclusão desnecessárias de uma cópia de objeto extra para cada operação de ingestão.

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



Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Especificar `REDUCED_REDUNDANCY` apenas afeta quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Ele não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas ativas de ILM e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.



Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a `REDUCED_REDUNDANCY` opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Os seguintes cabeçalhos de solicitação são suportados:

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

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

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

Se você quiser usar a opção **tempo de criação definido pelo usuário** como tempo de referência para uma regra ILM, você deve usar `creation-time` como o nome dos metadados que Registram quando o objeto foi criado. Por exemplo:

```
x-amz-meta-creation-time: 1443399726
```

O valor para `creation-time` é avaliado em segundos desde 1 de janeiro de 1970.



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

- S3 cabeçalhos de solicitação de bloqueio de objetos:
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`

- `x-amz-object-lock-legal-hold`

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

["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#)

- Cabeçalhos de pedido SSE:

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

[Cabeçalhos de solicitação para criptografia do lado do servidor](#)



Para obter informações sobre como o StorageGRID lida com caracteres UTF-8, ["PutObject"](#) consulte .

Cabeçalhos de solicitação para criptografia do lado do servidor

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

- **SSE:** Use o seguinte cabeçalho na solicitação `CreateMultipartUpload` se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações `UploadPart`.
 - `x-amz-server-side-encryption`
- **SSE-C:** Use todos esses três cabeçalhos na solicitação `CreateMultipartUpload` (e em cada solicitação `UploadPart` subsequente) se você quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
 - `x-amz-server-side-encryption-customer-algorithm`: 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 que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações para ["usando criptografia do lado do servidor"](#).

Cabeçalhos de solicitação não suportados

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

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

Controle de versão

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

ListMultipartUploads

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

Os seguintes parâmetros de solicitação são suportados:

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

Controle de versão

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

UploadPart

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

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Length`
- `Content-MD5`

Cabeçalhos de solicitação para criptografia do lado do servidor

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

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

you provided in the `CreateMultipartUpload` request.



The encryption keys that you provide are never stored. If you lose an encryption key, you lose the object it corresponds to. Before using keys provided by the client to protect the data of the object, review the considerations in ["Use server-side encryption"](#).

Controle de versão

Uploading multiple parts consists of separate operations to initiate the upload, list uploads, upload parts, assemble the uploaded parts and complete the upload. Objects are created (and versioned, if applicable) when the `CompleteMultipartUpload` operation is executed.

UploadPartCopy

The `UploadPartCopy` operation uploads a part of an object by copying data from an existing object as the source of data.

The `UploadPartCopy` operation is implemented with the same behavior as the Amazon S3 REST API. Subject to changes without notice.

This request reads and writes the data of the object specified in the `x-amz-copy-source-range` header to the StorageGRID.

The following request headers are supported:

- `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

If you specify SSE-C for the `CreateMultipartUpload` request, you must also include the following request headers in each `UploadPartCopy` request:

- `x-amz-server-side-encryption-customer-algorithm`: Specify AES256.
- `x-amz-server-side-encryption-customer-key`: Specify the same encryption key provided in the `CreateMultipartUpload` request.
- `x-amz-server-side-encryption-customer-key-MD5`: Specify the same MD5 checksum that you provided in the `CreateMultipartUpload` request.

If the source object is encrypted using a key provided by the client (SSE-C), you must include the three headers below in the `UploadPartCopy` request, so that the object can be decrypted and copied:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specify AES256.
- `x-amz-copy-source-server-side-encryption-customer-key`: Specify the encryption key provided when you created the source object.

- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu quando criou o objeto de origem.



As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações no ["Use a criptografia do lado do servidor"](#).

Controle de versão

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

Respostas de erro

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

Códigos de erro S3 API suportados

Nome	Status HTTP
<code>AccessDenied</code>	403 proibido
<code>BadDigest</code>	400 pedido incorreto
<code>BucketAlreadyExists</code>	409 conflito
<code>BucketNotEmpty</code>	409 conflito
<code>IncompleteBody</code>	400 pedido incorreto
<code>InternalError</code> (erro internacional)	500 erro interno do servidor
<code>InvalidAccessKeyId</code>	403 proibido
<code>InvalidArgument</code>	400 pedido incorreto
<code>InvalidBucketName</code>	400 pedido incorreto
<code>InvalidBucketState</code>	409 conflito
<code>InvalidDigest</code>	400 pedido incorreto
<code>InvalidEncryptionAlgorithmError</code>	400 pedido incorreto

Nome	Status HTTP
InvalidPart	400 pedido incorreto
InvalidPartOrder	400 pedido incorreto
Intervalo Invalidável	416 intervalo solicitado não satisfatório
InvalidRequest	400 pedido incorreto
InvalidStorageClass	400 pedido incorreto
InvalidTag	400 pedido incorreto
InvalidURI	400 pedido incorreto
KeyTooLong	400 pedido incorreto
MalformedXML	400 pedido incorreto
MetadataTooLarge	400 pedido incorreto
MetodNotAllowed	Método 405 não permitido
MissingContentLength	411 comprimento necessário
MissingRequestBodyError	400 pedido incorreto
MissingSecurityHeader	400 pedido incorreto
NoSuchBucket	404 não encontrado
NoSuchKey	404 não encontrado
NoSuchUpload	404 não encontrado
Sem Implementado	501 não implementado
NoSuchBucketPolicy	404 não encontrado
ObjectLockConfigurationNotFounError	404 não encontrado
Pré-condiçãoFailed	412 Pré-condição falhou
RequestTimeTooSwed	403 proibido

Nome	Status HTTP
Serviço indisponível	503 Serviço indisponível
SignatureDoesNotMatch	403 proibido
TooManyBuckets	400 pedido incorreto
UserKeyMustBeSpecified	400 pedido incorreto

Códigos de erro personalizados do StorageGRID

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

Operações personalizadas do StorageGRID

Operações personalizadas do StorageGRID: Visão geral

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

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

Operação	Descrição
"OBTER consistência de balde"	Retorna a consistência que está sendo aplicada a um balde específico.
"COLOQUE a consistência do balde"	Define a consistência aplicada a um balde específico.
"OBTER último tempo de acesso do Bucket"	Retorna se as atualizações da última hora de acesso estão ativadas ou desativadas para um intervalo específico.
"COLOQUE o último tempo de acesso do balde"	Permite-lhe ativar ou desativar as atualizações da última hora de acesso para um intervalo específico.
"ELIMINAR configuração de notificação de metadados do bucket"	Exclui o XML de configuração de notificação de metadados associado a um bucket específico.
"OBTER configuração de notificação de metadados do bucket"	Retorna o XML de configuração de notificação de metadados associado a um intervalo específico.
"COLOQUE a configuração de notificação de metadados do bucket"	Configura o serviço de notificação de metadados para um bucket.
"OBTER uso de armazenamento"	Indica 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 não suportado: Você não pode mais criar novos buckets com a conformidade ativada.
"Obsoleto: OBTENHA conformidade com Bucket"	Obsoleto, mas suportado: Retorna as configurações de conformidade atualmente em vigor para um bucket compatível com legado existente.
"Obsoleto: COLOQUE a conformidade com Bucket"	Obsoleto, mas suportado: Permite modificar as configurações de conformidade para um bucket compatível com legado existente.

OBTER consistência de balde

A solicitação GET Bucket Consistency permite determinar a consistência que está sendo aplicada a um determinado bucket.

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

Você deve ter a permissão S3:GetBucketConsistency, ou ser raiz 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
tudo	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.
forte local	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 eventual consistência 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 do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.

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"](#)

COLOQUE a consistência do balde

A solicitação de consistência do PUT Bucket permite especificar a consistência a ser aplicada às operações realizadas 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 raiz da conta, para concluir esta operação.

Pedido

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

Consistência	Descrição
tudo	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.
forte local	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 eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.

Consistência	Descrição
disponível	Fornecer consistência eventual para novos objetos e atualizações de objetos. Para buckets do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.

Nota: em geral, você deve usar a consistência "Read-after-new-write". 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 balde apenas 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"](#)

OBTER último tempo de acesso do Bucket

A solicitação de última hora de acesso do GET Bucket permite determinar se as atualizações da última hora de acesso estão ativadas ou desativadas para buckets individuais.

Você deve ter a permissão S3:GetBucketLastAccessTime, ou ser raiz 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 da última hora de acesso estão ativadas para o intervalo.

```
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>
```

COLOQUE o último tempo de acesso do balde

A solicitação de última hora de acesso do PUT Bucket permite ativar ou desativar as atualizações da última hora de acesso para intervalos individuais. A desativação das atualizações da última hora 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 raiz da conta, para concluir esta operação.



A partir da versão 10,3 do StorageGRID, as atualizações da última hora de acesso são desativadas por padrão para todos os novos buckets. Se você tiver buckets criados usando uma versão anterior do StorageGRID e quiser corresponder ao novo comportamento padrão, desative explicitamente as atualizações da última hora de acesso para cada um desses buckets anteriores. Você pode ativar ou desativar as atualizações para o último tempo de acesso usando a solicitação de última hora de acesso do PUT Bucket ou a partir da página de detalhes de um bucket no Gerenciador do Locatário. ["Ative ou desative as atualizações da última hora de acesso"](#) Consulte .

Se as atualizações da última hora de acesso estiverem desativadas para um bucket, o seguinte comportamento é aplicado às operações no bucket:

- As solicitações `GetObject`, `GetObjectAcl`, `GetObjectTagging` e `HeadObject` não atualizam o último tempo 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 a última hora de acesso. O objeto é adicionado às filas para avaliação ILM.
- Se as atualizações para a última hora de acesso estiverem desativadas para o intervalo de origem, as solicitações de `CopyObject` não atualizam a última hora de acesso para o intervalo de origem. O objeto que foi copiado não é adicionado às filas para avaliação ILM para o bucket de origem. No entanto, para o destino, as solicitações de `CopyObject` sempre atualizam a última hora de acesso. A cópia do objeto é adicionada às filas para avaliação ILM.
- `CompleteMultipartUpload Requests` atualizam o último tempo de acesso. O objeto concluído é adicionado às filas para avaliação ILM.

Exemplos de pedidos

Este exemplo permite o último tempo de acesso para um bucket.

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

Este exemplo desativa a última hora de acesso para um bucket.

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

ELIMINAR configuração de notificação de metadados do bucket

A solicitação de configuração de notificação de metadados DELETE Bucket permite desativar 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 raiz de 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
```

OBTER configuração de notificação de metadados do bucket

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

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

Exemplo de solicitação

Essa solicitação recupera a configuração de notificação de metadados para o bucket chamado `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 determinar como o intervalo é configurado para integração de pesquisa. Ou seja, ele permite determinar quais objetos são indexados e 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 onde o StorageGRID deve enviar metadados de objeto. Os destinos devem ser especificados usando a URNA de um endpoint StorageGRID.

Nome	Descrição	Obrigatório
MetadataNotificationConfiguration	Tag de contendor para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos de regra.	Sim

Nome	Descrição	Obrigatório
Regra	<p>Tag container para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado.</p> <p>Regras com prefixos sobrepostos são rejeitadas.</p> <p>Incluído no elemento MetadataNotificationConfiguration.</p>	Sim
ID	<p>Identificador exclusivo para a regra.</p> <p>Incluído no elemento regra.</p>	Não
Estado	<p>O estado pode ser "ativado" ou "Desativado". Nenhuma ação é tomada para regras que são desativadas.</p> <p>Incluído no elemento regra.</p>	Sim
Prefixo	<p>Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado.</p> <p>Para corresponder a todos os objetos, especifique um prefixo vazio.</p> <p>Incluído no elemento regra.</p>	Sim
Destino	<p>Etiqueta de contentor para o destino de uma regra.</p> <p>Incluído no elemento regra.</p>	Sim

Nome	Descrição	Obrigatório
Urna	<p>URNA do destino onde os metadados do objeto são enviados. Deve ser a URNA de um endpoint StorageGRID com as seguintes propriedades:</p> <ul style="list-style-type: none"> • es deve ser o terceiro elemento. • A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário <code>domain-name/myindex/mytype</code>. <p>Os endpoints são configurados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário. Eles assumem a seguinte forma:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>O endpoint deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404.</p> <p>Urna está incluído no elemento destino.</p>	Sim

Exemplo de resposta

O XML incluído entre as

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags mostra como a integração com um endpoint de integração de pesquisa é configurada para o bucket. Neste exemplo, metadados de objeto estão sendo enviados para um índice Elasticsearch nomeado `current` e tipo nomeado `2017` que está hospedado em um domínio da AWS `records` chamado `.`

```
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 locatário"](#)

COLOQUE a configuração de notificação de metadados do bucket

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

Você deve ter a permissão `S3:PutBucketMetadataNotification` para um bucket, ou ser raiz de conta, para concluir esta operação.

Pedido

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 ao qual o StorageGRID deve enviar metadados de objetos.

Os objetos podem ser filtrados no 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.

As configurações que têm prefixos sobrepostos não são válidas e são rejeitadas quando são 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 permitida.

Os destinos devem ser especificados usando a URNA de um endpoint StorageGRID. O endpoint deve existir quando a configuração de notificação de metadados é enviada ou a solicitação falha como um `400 Bad`

Request. **a mensagem de erro afirma:** 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
MetadataNotificationConfi guration	Tag de contendor para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos de regra.	Sim
Regra	Tag container 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
ID	Identificador exclusivo para a regra. Incluído no elemento regra.	Não
Estado	O estado pode ser "ativado" ou "Desativado". Nenhuma ação é tomada para regras que são desativadas. Incluído no elemento regra.	Sim

Nome	Descrição	Obrigatório
Prefixo	<p>Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado.</p> <p>Para corresponder a todos os objetos, especifique um prefixo vazio.</p> <p>Incluído no elemento regra.</p>	Sim
Destino	<p>Etiqueta de contentor para o destino de uma regra.</p> <p>Incluído no elemento regra.</p>	Sim
Urna	<p>URNA do destino onde os metadados do objeto são enviados. Deve ser a URNA de um endpoint StorageGRID com as seguintes propriedades:</p> <ul style="list-style-type: none"> • <code>es</code> deve ser o terceiro elemento. • A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário <code>domain-name/myindex/mytype</code>. <p>Os endpoints são configurados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário. Eles assumem a seguinte forma:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>O endpoint deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404.</p> <p>Urna está incluído no elemento destino.</p>	Sim

Exemplos de pedidos

Este exemplo mostra a ativação da integração de pesquisa para um bucket. Neste exemplo, metadados de objetos para 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` são enviados para um destino, enquanto metadados de objetos para objetos que correspondem ao prefixo `/videos` são enviados 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-1:33333333: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 ativa o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado para o endpoint de destino cada vez 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 intervalo `test` chamado `.`. O `test` bucket não está versionado, então a `versionId` 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 objetos incluídos nas notificações de metadados

A tabela lista todos os campos que estão incluídos no documento JSON que é enviado para o endpoint de destino quando a integração de pesquisa está ativada.

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

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

Tipo	Nome do item	Descrição
Tags	tags <i>key:value</i>	Todas as tags de objeto definidas para o objeto, como pares chave-valor



Para tags e metadados de usuários, 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 os formatos de data de mapeamento. Você deve ativar os mapeamentos de campo 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 locatário"](#)

OBTER solicitação de uso de armazenamento

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

A quantidade de armazenamento usada por uma conta e seus buckets pode ser obtida por uma solicitação de ListBuckets modificada com o `x-ntap-sg-usage` parâmetro de consulta. O uso do armazenamento de buckets é rastreado separadamente das SOLICITAÇÕES DE 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, especialmente 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 de objeto armazenada contribuirá para os `ObjectCount` valores e `DataBytes` na resposta. Excluir marcadores 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 criados com o recurso de conformidade legado.

Funcionalidade de conformidade obsoleta

O recurso de conformidade do StorageGRID que estava disponível nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3.

Se você ativou anteriormente a configuração de conformidade global, a configuração de bloqueio de objeto global S3 será ativada no StorageGRID 11,6. Você não pode mais criar novos buckets com a conformidade ativada. No entanto, conforme necessário, você pode usar a API REST do StorageGRID S3 para gerenciar buckets em conformidade existentes.

- ["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#)
- ["Gerenciar objetos com ILM"](#)
- ["Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"](#)

Solicitações de conformidade obsoletas:

- ["Obsoleto - COLOCAR modificações de solicitação de balde para conformidade"](#)

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

- ["Obsoleto - OBTER conformidade com balde"](#)

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

- ["Obsoleto - COLOCAR conformidade com balde"](#)

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

Obsoleto: CreateBucket solicita modificações para conformidade

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



O recurso de conformidade do StorageGRID que estava disponível nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3. Consulte o seguinte para obter mais detalhes:

- ["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#)
- ["Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"](#)

Você não pode mais criar novos buckets com a conformidade ativada. A seguinte mensagem de erro é retornada se você tentar usar o CreateBucket solicitar modificações 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: OBTER solicitação de conformidade do bucket

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



O recurso de conformidade do StorageGRID que estava disponível nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3. Consulte o seguinte para obter mais detalhes:

- ["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#)
- ["Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"](#)

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

Exemplo de solicitação

Esta solicitação de exemplo permite que você determine as configurações de conformidade para o bucket chamado 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 de um intervalo no qual cada objeto será retido por um ano (525.600 minutos), a partir de quando o objeto é ingerido na grade. Atualmente, não existe qualquer retenção legal neste intervalo. Cada objeto será automaticamente excluído 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
Repetição de PeriodMinutes	A duração do período de retenção para objetos adicionados a este intervalo, em minutos. O período de retenção começa quando o objeto é ingerido na grade.
LegalHod	<ul style="list-style-type: none"> • Verdadeiro: Este balde está atualmente sob uma guarda legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja levantada, mesmo que seu período de retenção tenha expirado. • Falso: Este balde não está atualmente sob um guarda legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Autodelete	<ul style="list-style-type: none"> • Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob uma retenção legal. • Falso: Os objetos neste intervalo 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 intervalo 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: COLOQUE a solicitação de conformidade do bucket

A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar usando essa solicitação para modificar as configurações de conformidade de um bucket em conformidade com o 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 nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3. Consulte o seguinte para obter mais detalhes:

- ["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#)
- ["Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado 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 PUT Bucket.

Exemplo de solicitação

Esta solicitação de exemplo modifica as configurações de conformidade para o bucket `mybucket` chamado . Neste exemplo, os objetos em `mybucket` agora serão retidos por dois anos (1.051.200 minutos) em vez de um ano, a partir de quando o objeto é ingerido na grade. Não há retenção legal neste balde. Cada objeto será automaticamente excluído 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
Repetição de PeriodMinutes	<p>A duração do período de retenção para objetos adicionados a este intervalo, em minutos. O período de retenção começa quando o objeto é ingerido na grade.</p> <p>Importante ao especificar um novo valor para <code>RetentionPeriodMinutes</code>, você deve especificar um valor 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.</p>

Nome	Descrição
LegalHod	<ul style="list-style-type: none"> • Verdadeiro: Este balde está atualmente sob uma guarda legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja levantada, mesmo que seu período de retenção tenha expirado. • Falso: Este balde não está atualmente sob um guarda legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Autodelete	<ul style="list-style-type: none"> • Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob uma retenção legal. • Falso: Os objetos neste intervalo 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 de ARMAZENAMENTO, 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 de data center e todos os nós de storage que contêm metadados de bucket tenham consistência de leitura após gravação para as configurações de conformidade alteradas.

Se o StorageGRID não conseguir obter 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 grade para garantir que os serviços de armazenamento necessários sejam disponibilizados o mais rápido possível. Se o administrador da grade não conseguir disponibilizar o suficiente dos nós de armazenamento em cada local, o suporte técnico pode direcioná-lo a tentar novamente a solicitação com falha, forçando a consistência **strong-site**.



Nunca force a consistência **strong-site** para a conformidade com o bucket, a menos que você tenha sido direcionado a fazê-lo por suporte técnico e a menos que você entenda as possíveis consequências de usar esse nível.

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

Para forçar o uso da consistência **strong-site**, volte a emitir a solicitação de conformidade PUT Bucket e inclua o Consistency-Control cabeçalho de solicitação HTTP, da seguinte forma:

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

Respostas de erro

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

Informações relacionadas

["Obsoleto: Modificações de solicitação de Bucket para conformidade"](#)

Políticas de acesso ao bucket e ao grupo

Use políticas de acesso de grupo e bucket

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 nesses buckets. O sistema StorageGRID implementa um subconjunto da linguagem de política da API REST S3. As políticas de acesso para a API S3 são escritas em JSON.

Visão geral da política de acesso

Existem dois tipos de políticas de acesso suportadas pelo StorageGRID.

- **Políticas de bucket**, que são gerenciadas usando as operações da API `GetBucketPolicy`, `PutBucketPolicy` e `DeleteBucketPolicy` S3. As políticas de bucket são anexadas a buckets, portanto, são configuradas para controlar o acesso dos usuários na conta de proprietário do bucket ou 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 Gerenciador do locatário ou a API de gerenciamento do locatário. As políticas de grupo são anexadas a um grupo na conta, portanto 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 vários buckets.



Não há diferença na prioridade entre as políticas de grupo e bucket.

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

- ID de declaração (Sid) (opcional)
- Efeito
- Principal/NotPrincipal
- Recurso/não recurso

- Ação/não Ação
- Condição (opcional)

As instruções de política são criadas usando essa estrutura para especificar permissões: Grant <Effect> para permitir/negar que o <Principal> execute o <Action> no <Resource> quando o <Condition> se aplicar.

Cada elemento de política é usado para uma função específica:

Elemento	Descrição
SID	O elemento Sid é opcional. O Sid é apenas uma descrição para o usuário. Ele é armazenado, mas não interpretado pelo sistema StorageGRID.
Efeito	Use o elemento efeito para determinar se as operações especificadas são permitidas ou negadas. É necessário identificar operações que você permite (ou nega) em buckets ou objetos usando as palavras-chave do elemento Ação suportado.
Principal/NotPrincipal	<p>Você pode permitir que usuários, grupos e contas acessem recursos específicos e executem ações específicas. Se nenhuma assinatura S3 estiver incluída na solicitação, o acesso anônimo será permitido especificando o caractere curinga (*) como principal. Por padrão, somente a raiz da conta tem acesso aos recursos de propriedade da conta.</p> <p>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.</p>
Recurso/não recurso	O elemento recurso identifica buckets e objetos. Você pode permitir ou negar permissões a buckets e objetos usando o Nome do recurso da Amazon (ARN) para identificar o recurso.
Ação/não Ação	Os elementos Ação e efeito são os dois componentes das permissões. Quando um grupo solicita um recurso, é concedido ou negado o acesso ao recurso. O acesso é negado a menos que você atribua permissões especificamente, mas você pode usar Negar explícito para substituir uma permissão concedida por outra política.
Condição	O elemento de condição 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, o que concede permissão a todos. Por exemplo, você define o caractere curinga (*) como o valor principal.

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

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

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

```
{
  "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:iam:s3::mybucket",
        "arn:aws:iam: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, quaisquer atualizações feitas para políticas de grupo são eventualmente consistentes. Quando uma política de grupo se torna consistente, as alterações podem levar mais 15 minutos para entrar em vigor, devido ao armazenamento em cache de políticas. Por padrão, todas as atualizações feitas às políticas de bucket são altamente 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 falha no local.

Nesse caso, você pode definir o `Consistency-Control` cabeçalho na solicitação `PutBucketPolicy` ou usar a solicitação `DE` consistência de `COLOCAR` bucket. Quando uma política de bucket se torna consistente, as alterações podem levar mais 8 segundos para entrar em vigor, devido ao armazenamento em 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 balde de volta ao valor original quando terminar. Caso contrário, todas as futuras solicitações de bucket usarão a configuração modificada.

Use ARN em declarações de política

Em declarações de política, o ARN é usado em elementos Principal e recursos.

- Use esta sintaxe para especificar o ARN de recursos 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 de objeto.
- Caracteres internacionais, que podem ser especificados na chave do objeto, devem ser codificados usando JSON UTF-8 ou usando sequências de escape JSON. A codificação percentual não é suportada.

["RFC 2141 sintaxe de URNA"](#)

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

Especifique recursos em uma política

Em declarações de política, você pode usar o elemento recurso para especificar o intervalo 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 recursos S3. Por exemplo:

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

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

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

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

Especifique princípios em uma política

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

- Cada declaração de política em uma política de bucket deve incluir um elemento principal. As 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 princípios são denotados pelo elemento "principal" ou, alternativamente, "NotPrincipal" para exclusão.
- As identidades baseadas em contas devem ser especificadas usando um ID ou um ARN:

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

- Este exemplo usa o ID de 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 usuário UUID 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` seja excluído. Se um novo Alex se juntar à organização e receber o mesmo `Alex` nome de usuário, o novo usuário poderá involuntariamente herdar 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.

Especifique permissões em uma política

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

As tabelas lista 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, que corresponde à especificação original do Amazon S3.



Uma exclusão é executada quando uma `put` é usada para substituir um valor existente.

Permissões que se aplicam a buckets

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:CreateBucket	CreateBucket	Sim. Nota: Use somente na política de grupo.
S3>DeleteBucket	DeleteBucket	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:DeleteBucketMetadataNotification	ELIMINAR configuração de notificação de metadados do bucket	Sim
S3:DeleteBucketPolicy	DeleteBucketPolicy	
S3:DeleteReplicationConfiguration	DeleteBucketReplication	Sim, permissões separadas para COLOCAR e EXCLUIR
S3:GetBucketAcl	GetBucketAcl	
S3:GetBucketCompliance	OBTER conformidade com balde (obsoleto)	Sim
S3:GetBucketConsistência	OBTER consistência de balde	Sim
S3:GetBucketCORS	GetBucketCors	
S3:GetEncryptionConfiguration	GetBucketEncryption	
S3:GetBucketLastAccessTime	OBTER último tempo de acesso do Bucket	Sim
S3:GetBucketLocation	GetBucketlocalização	
S3:GetBucketMetadataNotification	OBTER configuração de notificação de metadados do bucket	Sim
S3:GetBucketNotification	GetBucketNotificationConfiguration	
S3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
S3:GetBucketPolicy	Política de GetBucketPolicy	
S3:GetBucketTagging	GetBucketTagging	
S3:GetBucketControle de versão	GetBucketControle de versão	
S3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
S3:GetReplicationConfiguration	GetBucketReplication	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:ListAllMyBuckets	<ul style="list-style-type: none"> ListBuckets OBTER uso de armazenamento 	<p>Sim, para OBTER uso de armazenamento.</p> <p>Nota: Use somente na política de grupo.</p>
S3: ListBucket	<ul style="list-style-type: none"> ListObjects Balde para a cabeça RestoreObject 	
S3:ListBucketMultipartUploads	<ul style="list-style-type: none"> ListMultipartUploads RestoreObject 	
S3:ListBucketVersions	OBTER versões Bucket	
S3:PutBucketCompliance	COLOCAR conformidade com balde (obsoleto)	Sim
S3:PutBucketConsistência	COLOQUE a consistência do balde	Sim
S3:PutBucketCORS	<ul style="list-style-type: none"> DeleteBucketCors† PutBucketCors 	
S3:PutEncryptionConfiguration	<ul style="list-style-type: none"> DeleteBucketEncryption PutBucketEncryption 	
S3:PutBucketLastAccessTime	COLOQUE o último tempo de acesso do balde	Sim
S3:PutBucketMetadataNotification	COLOQUE a configuração de notificação de metadados do bucket	Sim
S3:PutBucketNotification	PutBucketNotificationConfiguration	
S3:PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> CreateBucket com o x-amz-bucket-object-lock-enabled: true cabeçalho de solicitação (também requer a permissão S3:CreateBucket) PutObjectLockConfiguration 	
S3:PutBucketPolicy	Política de PutBucketPolicy	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:PutBucketTagging	<ul style="list-style-type: none"> DeleteBucketTagging† PutBucketTagging 	
S3:PutBucketControle de versão	PutBucketControle de versão	
S3:PutLifecycleConfiguration	<ul style="list-style-type: none"> DeleteBucketLifecycle† PutBucketLifecycleConfiguration 	
S3:PutReplicationConfiguration	PutBucketReplication	Sim, permissões separadas para COLOCAR e EXCLUIR

Permissões que se aplicam a objetos

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:AbortMultipartUpload	<ul style="list-style-type: none"> AbortMultipartUpload RestoreObject 	
S3:BypassGovernanceretenção	<ul style="list-style-type: none"> DeleteObject DeleteObjects Retenção PutObjectRetention 	
S3>DeleteObject	<ul style="list-style-type: none"> DeleteObject DeleteObjects RestoreObject 	
S3>DeleteObjectTagging	DeleteObjectTagging	
S3>DeleteObjectVersionTagging	DeleteObjectTagging (uma versão específica do objeto)	
S3>DeleteObjectVersion	DeleteObject (uma versão específica do objeto)	
S3:GetObject	<ul style="list-style-type: none"> GetObject HeadObject RestoreObject Selecione ObjectContent 	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:GetObjectAcl	GetObjectAcl	
S3:GetObjectLegalHod	GetObjectLegalHod	
S3:GetObjectRetention	GetObjectRetention	
S3:GetObjectTagging	GetObjectTagging	
S3:GetObjectVersionTagging	GetObjectTagging (uma versão específica do objeto)	
S3:GetObjectVersion	GetObject (uma versão específica do objeto)	
S3:ListMultipartUploadParts	ListParts, RestoreObject	
S3:PutObject	<ul style="list-style-type: none"> • PutObject • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy 	
S3:PutObjectLegalHod	PutObjectLegalHod	
S3:retenção de objetos Put	Retenção PutObjectRetention	
S3:PutObjectTagging	Marcação de objetos	
S3:PutObjectVersionTagging	PutObjectTagging (uma versão específica do objeto)	
S3:PutOverwriteObject	<ul style="list-style-type: none"> • PutObject • CopyObject • Marcação de objetos • DeleteObjectTagging • CompleteMultipartUpload 	Sim
S3:RestoreObject	RestoreObject	

Use a permissão PutOverwriteObject

A permissão S3:PutOverwriteObject é uma permissão StorageGRID personalizada 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 objeto S3.

As configurações possíveis para essa permissão incluem:

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



Se a política S3 atual permitir a substituição e a permissão PutOverwriteObject estiver definida como Negar, o cliente não poderá substituir os dados de um objeto, metadados definidos pelo usuário ou marcação de objeto. Além disso, se a caixa de verificação **Prevent client modification** estiver selecionada (**CONFIGURATION > Security settings > Network and Objects**), essa configuração substituirá a configuração da permissão PutOverwriteObject.

Especifique condições em uma política

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

Condições Use pares chave-valor para avaliação. Um elemento de condição pode conter várias condições, e cada condição pode conter vários pares de 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 Sourcelp.

```

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

```

Operadores de condição suportados

Os operadores de condição são categorizados da seguinte forma:

- Cadeia de caracteres
- Numérico
- Booleano
- Endereço IP
- Verificação nula

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

Operadores de condição	Descrição
NumericGreaterThan	Compara uma chave com um valor numérico baseado na correspondência "maior que".
NumericGreaterThanEquals	Compara uma chave com um valor numérico baseado na correspondência "maior que ou igual".
NumericLessThan	Compara uma chave com um valor numérico baseado na correspondência "inferior a".
NumericLessThanEquals	Compara uma chave com um valor numérico baseado na correspondência "inferior ou igual".
Bool	Compara uma chave com um valor booleano baseado na correspondência "verdadeiro ou falso".
Endereço IP	Compara uma chave com um endereço IP ou intervalo de endereços IP.
NotIpAddress	Compara uma chave com um endereço IP ou um intervalo de endereços IP com base na correspondência negada.
Nulo	Verifica se uma chave de condição está presente no contexto de solicitação atual.

Teclas de condição suportadas

Teclas de condição	Ações	Descrição
AWS:SourceIp	Operadores IP	<p>Irá comparar com o endereço IP a partir do qual a solicitação foi enviada. Pode ser usado para operações de balde ou objetos.</p> <p>Observação: se a solicitação S3 tiver sido enviada pelo serviço Load Balancer nos nós Admin e Gateways, isso será comparado ao endereço IP upstream do serviço Load Balancer.</p> <p>Nota: Se um balanceador de carga não transparente de terceiros for usado, isso será comparado ao endereço IP desse balanceador de carga. Qualquer X-Forwarded-For cabeçalho será ignorado porque sua validade não pode ser determinada.</p>
aws:nome de usuário	Recurso/identidade	<p>Irá comparar com o nome de usuário do remetente a partir do qual a solicitação foi enviada. Pode ser usado para operações de balde ou objetos.</p>

Teclas de condição	Ações	Descrição
s3:delimitador	S3: ListBucket e. S3:ListBucketVersions Permissions	Irá comparar com o parâmetro delimitador especificado em uma solicitação ListObjects ou ListObjectVersions.
S3: ExistingObjectTag/<tag- key>	S3:DeleteObjectTagging S3:DeleteObjectVersionT agging S3:GetObject S3:GetObjectAcl 3:GetObjectTagging S3:GetObjectVersion S3:GetObjectVersionAcl S3:GetObjectVersionTagg ing S3:PutObjectAcl S3:PutObjectTagging S3:PutObjectVersionAcl S3:PutObjectVersionTagg ing	Exigirá que o objeto existente tenha a chave e o valor específicos da tag.
s3: teclas de max	S3: ListBucket e. S3:ListBucketVersions Permissions	Irá comparar com o parâmetro Max-keys especificado em uma solicitação ListObjects ou ListObjectVersions.
s3: object-lock-resting- retension-days	S3:PutObject	<p>Compara com a data de retenção até especificada no x-amz-object-lock-retain-until-date cabeçalho da solicitação ou calculada a partir do período de retenção padrão do intervalo para garantir que esses valores estejam dentro do intervalo permitido para as seguintes solicitações:</p> <ul style="list-style-type: none"> • PutObject • CopyObject • CreateMultipartUpload

Tecclas de condição	Ações	Descrição
s3: object-lock-resting-retension-days	S3:retenção de objetos Put	Compara com a data de retenção até especificada na solicitação PutObjectRetention para garantir que ela esteja dentro do intervalo permitido.
s3:prefixo	S3: ListBucket e. S3:ListBucketVersions Permissions	Irá comparar com o parâmetro prefix especificado em uma solicitação ListObjects ou ListObjectVersions.
S3:RequestObjectTag/<tag-key>	S3:PutObject S3:PutObjectTagging S3:PutObjectVersionTagging	Exigirá uma chave de tag específica e um valor quando a solicitação de objeto incluir marcação.

Especifique variáveis em uma política

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

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

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

Variável	Descrição
<code>\${s3:max-keys}</code>	Usa a chave de teclas de Max específicas do serviço como a variável fornecida.
<code>\${*}</code>	Caráter especial. Usa o caractere como um caractere * literal.
<code>\${?}</code>	Caráter especial. Usa o caractere como um caractere literal ?.
<code>\${\$}</code>	Caráter especial. Usa o caractere como um caractere literal.

Crie políticas que exijam tratamento especial

Às vezes, uma diretiva pode conceder permissões que são perigosas para a segurança ou perigosas para operações contínuas, como bloquear o usuário raiz 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 de StorageGRID
Negar a si mesmo quaisquer permissões para a conta raiz	Balde	Válida e aplicada, mas a conta de usuário root mantém permissão para todas as operações de política de bucket do S3	O mesmo
Negar auto quaisquer permissões ao usuário/grupo	Grupo	Válido e aplicado	O mesmo
Permita a um grupo de conta estrangeiro qualquer permissão	Balde	Principal inválido	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido quando permitido por uma política
Permitir uma conta estrangeira root ou usuário qualquer permissão	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido quando permitido por uma política	O mesmo

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

Proteção WORM (write-once-read-many)

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

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

- No Gerenciador de Grade, vá para **CONFIGURATION > Security > Security settings > Network and Objects**, e marque a caixa de seleção **Prevent client modification**.
- Aplique as seguintes regras e políticas do S3:
 - Adicione uma operação PutOverwriteObject NEGAR à política S3.
 - Adicione uma operação DeleteObject NEGAR à política S3.
 - Adicione uma operação PutObject PERMITIR à política S3.



A configuração DeleteObject para NEGAR em uma diretiva S3 não impede que o ILM exclua objetos quando uma regra como "zero cópias após 30 dias" existir.



Mesmo quando todas essas regras e políticas são aplicadas, elas não se protegem contra gravações simultâneas (ver situação A). Eles protegem contra substituições concluídas sequenciais (ver situação B).

Situação A: Gravações simultâneas (não protegidas contra)

```
/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"](#)
- ["Exemplo de políticas de bucket"](#)
- ["Exemplo de políticas de grupo"](#)
- ["Gerenciar objetos com ILM"](#)
- ["Use uma conta de locatário"](#)

Exemplo de políticas de bucket

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

As políticas de bucket especificam as permissões de acesso para o bucket ao qual a diretiva está anexada. As políticas de bucket são configuradas usando a API S3 PutBucketPolicy. ["Operações em baldes"](#) Consulte .

Uma política de bucket pode ser configurada usando a AWS CLI de acordo com o seguinte comando:

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

Exemplo: Permita que todos acessem somente leitura a um bucket

Neste exemplo, todos, incluindo anônimos, podem listar objetos no bucket e executar operações GetObject em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que essa política pode não ser particularmente útil porque ninguém, exceto a raiz da conta, tem permissões 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: Permita que todos em uma conta tenham acesso total, e todos em outra conta tenham acesso somente leitura a um intervalo

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



No StorageGRID, os objetos criados por uma conta não proprietária (incluindo contas anônimas) são de propriedade da conta de proprietário do bucket. A política de bucket aplica-se 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: Permita que todos acessem somente leitura a um bucket e o acesso total por grupo especificado

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

```

{
  "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: Permita que todos leiam e gravem o acesso a um bucket se o cliente estiver no intervalo 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 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` bucket e seus objetos. Todos os outros usuários, incluindo "root", são explicitamente negados todas as operações. Note no entanto que "root" nunca é negada permissão para colocar/obter/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 efeito para PutOverwriteObject e DeleteObject garante que ninguém pode substituir ou excluir os dados do objeto, metadados definidos pelo usuário e marcação de objetos 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 ao StorageGRID para grupos.

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

Exemplo: Defina a política de grupo usando o Gerenciador do locatário

Quando você adiciona ou edita um grupo no Gerenciador do locatário, você pode selecionar uma política de grupo para determinar quais permissões de acesso do S3 os membros deste grupo terão. ["Crie grupos para um locatário do S3"](#) Consulte .

- **No S3 Access:** Opção padrão. Os usuários deste grupo não têm acesso a recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar essa opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
- **Acesso somente leitura:** Os usuários deste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos. Quando você seleciona essa opção, a cadeia de caracteres JSON para uma política de grupo somente leitura aparece na caixa de texto. Não é possível editar esta cadeia de caracteres.
- **Acesso total:** Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona essa opção, a cadeia de caracteres JSON para uma política de grupo de acesso total aparece na caixa de texto. Não é possível editar esta cadeia de caracteres.
- **Mitigação de ransomware:** Esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários deste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que têm o controle de versão de objeto habilitado.

Os usuários do Gerenciador de locatários que têm a permissão Gerenciar todos os buckets podem substituir essa política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação multifator (MFA), onde disponível.

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

Exemplo: Permitir o acesso total do grupo a todos os buckets

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

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

Exemplo: Permitir acesso somente leitura de grupo a todos os buckets

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

```

{
  "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: Permita que os membros do grupo tenham acesso total apenas à sua "pasta" em um intervalo

Neste exemplo, os membros do grupo só podem listar e acessar sua pasta específica (prefixo de chave) no intervalo especificado. Observe que as permissões de acesso de outras políticas de grupo e a 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}/*"
    }
  ]
}

```

S3 operações 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 operações de bucket e objetos.

Operações de bucket rastreadas nos logs de auditoria

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- Balde para a cabeça
- ListObjects
- ListObjectVersions
- COLOQUE a conformidade do balde
- PutBucketTagging
- PutBucketControle de versão

Operações de objeto rastreadas nos logs de auditoria

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- HeadObject
- PutObject
- RestoreObject
- Selecionar Objeto
- UploadPart (quando uma regra ILM usa ingestão equilibrada ou rigorosa)
- UploadPartCopy (quando uma regra ILM usa ingestão equilibrada ou rigorosa)

Informações relacionadas

- ["Acessar o arquivo de log de auditoria"](#)
- ["O cliente escreve mensagens de auditoria"](#)
- ["O cliente lê mensagens de auditoria"](#)

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.