



# Operações em baldes

## StorageGRID

NetApp  
March 12, 2025

# Índice

- Operações em baldes ..... 1
  - Crie a configuração do ciclo de vida do S3 ..... 8
    - Qual é a configuração do ciclo de vida ..... 8
    - Criar configuração do ciclo de vida ..... 9
    - Aplique a configuração do ciclo de vida ao bucket ..... 11
    - Valide que a expiração do ciclo de vida do bucket se aplica ao objeto ..... 11
  - Use retenção padrão do bucket do bloqueio de objetos S3 ..... 12
    - OBTER Configuração bloqueio Objeto ..... 12
    - COLOCAR Configuração bloqueio Objeto ..... 13
- Operações personalizadas em buckets ..... 14

# Operações em baldes

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

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

["Documentação do Amazon Web Services \(AWS\): Restrições e limitações do bucket"](#)

[Configure os nomes de domínio de endpoint da API S3](#)

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

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

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

Operação	Implementação
ELIMINAR balde	Implementado com todo o comportamento da API REST do Amazon S3.
ELIMINAR Cors balde	Esta operação exclui a configuração CORS para o bucket.
ELIMINAR encriptação Bucket	Esta operação exclui a criptografia padrão do intervalo. Os objetos criptografados existentes permanecem criptografados, mas todos os novos objetos adicionados ao bucket não são criptografados.
ELIMINAR ciclo de vida do balde	Esta operação exclui a configuração do ciclo de vida do bucket.
ELIMINAR política de balde	Esta operação exclui a política anexada ao bucket.
ELIMINAR replicação de balde	Esta operação exclui a configuração de replicação anexada ao bucket.
ELIMINAR marcação de intervalo	Esta operação usa o <code>tagging</code> subrecurso para remover todas as tags de um bucket.

Operação	Implementação
GET Bucket (List Objects), versão 1 e versão 2	<p>Esta operação retorna alguns ou todos (até 1.000) dos objetos em um balde. A Classe de armazenamento para objetos pode ter um de dois valores, mesmo que o objeto tenha sido ingerido com a <code>REDUCED_REDUNDANCY</code> opção de classe de armazenamento:</p> <ul style="list-style-type: none"> <li>• <code>STANDARD</code>, Que indica que o objeto está armazenado em um pool de storage que consiste em nós de storage.</li> <li>• <code>GLACIER</code>, Que indica que o objeto foi movido para o bucket externo especificado pelo pool de armazenamento em nuvem.</li> </ul> <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>
OBTER acl balde	Esta operação retorna uma resposta positiva e a ID, <code>DisplayName</code> e permissão do proprietário do bucket, indicando que o proprietário tem acesso total ao bucket.
OBTER Bucket Cors	Esta operação retorna a <code>cors</code> configuração do balde.
OBTER criptografia Bucket	Esta operação retorna a configuração de criptografia padrão para o bucket.
OBTENHA o ciclo de vida do Bucket	Esta operação retorna a configuração do ciclo de vida do bucket.
OBTER localização do balde	Esta operação retorna a região que foi definida usando o <code>LocationConstraint</code> elemento na solicitação <code>PUT Bucket</code> . Se a região do bucket for <code>us-east-1</code> , uma string vazia será retornada para a região.
OBTER notificação Bucket	Esta operação retorna a configuração de notificação anexada ao bucket.
OBTER versões Objeto balde	Com <code>ACESSO DE LEITURA</code> em um bucket, essa operação com o <code>versions</code> subrecurso lista metadados de todas as versões de objetos no bucket.
OBTER política Bucket	Esta operação retorna a política anexada ao bucket.
OBTER replicação do bucket	Esta operação retorna a configuração de replicação anexada ao bucket.
OBTER marcação Bucket	Esta operação usa o <code>tagging</code> subrecurso para retornar todas as tags para um bucket.

Operação	Implementação
OBTENHA o controle de versão do Bucket	<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"> <li>• <i>Blank</i>: O controle de versão nunca foi habilitado (o bucket é "não versionado")</li> <li>• <i>Habilitado</i>: O controle de versão está habilitado</li> <li>• <i>Suspensão</i>: O controle de versão foi ativado anteriormente e está suspenso</li> </ul>
OBTENHA Configuração bloqueio Objeto	<p>Esta operação retorna o modo de retenção padrão do bucket e o período de retenção padrão, se configurado.</p> <p><a href="#">OBTENHA Configuração bloqueio Objeto</a> Consulte para obter informações detalhadas.</p>
Balde DA cabeça	<p>Esta operação determina se existe um intervalo e você tem permissão para acessá-lo.</p> <p>Esta operação retorna:</p> <ul style="list-style-type: none"> <li>• <code>x-ntap-sg-bucket-id</code>: O UUID do bucket no formato UUID.</li> <li>• <code>x-ntap-sg-trace-id</code>: O ID de rastreamento exclusivo da solicitação associada.</li> </ul>

Operação	Implementação
COLOQUE o balde	<p>Esta operação cria um novo balde. Ao criar o balde, você se torna o proprietário do balde.</p> <ul style="list-style-type: none"> <li>• Os nomes dos buckets devem estar em conformidade com as seguintes regras: <ul style="list-style-type: none"> <li>◦ Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário).</li> <li>◦ Deve ser compatível com DNS.</li> <li>◦ Deve conter pelo menos 3 e não mais de 63 caracteres.</li> <li>◦ 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.</li> <li>◦ Não deve se parecer com um endereço IP formatado em texto.</li> <li>◦ Não deve usar períodos em solicitações de estilo hospedadas virtuais. Os períodos causarão problemas com a verificação do certificado curinga do servidor.</li> </ul> </li> <li>• 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.</li> </ul> <p><b>Nota:</b> Ocorrerá um erro se a solicitação PUT Bucket usar uma região que não foi definida no StorageGRID.</p> <ul style="list-style-type: none"> <li>• 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. <a href="#">Use o bloqueio de objetos S3D</a>. Consulte .</li> </ul> <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 intervalo. O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.</p>
COLOQUE cors de balde	<p>Esta operação define a configuração do CORS para um bucket de modo que o bucket possa atender às solicitações de origem cruzada. O compartilhamento de recursos de origem cruzada (CORS) é um mecanismo de segurança que permite que aplicativos da Web do cliente em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket S3 chamado <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>.</p>

Operação	Implementação
<p>COLOQUE a criptografia Bucket</p>	<p>Esta operação define o estado de criptografia padrão de um bucket existente. Quando a criptografia no nível do bucket está ativada, todos os novos objetos adicionados ao bucket são criptografados. O StorageGRID suporta criptografia no lado do servidor com chaves gerenciadas pelo StorageGRID. Ao especificar a regra de configuração de criptografia do lado do servidor, defina o <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>
<p>COLOQUE o ciclo de vida do balde</p>	<p>Essa operação cria uma nova configuração de ciclo de vida para o bucket ou substitui uma configuração de ciclo de vida existente. O StorageGRID dá suporte a até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML:</p> <ul style="list-style-type: none"> <li>• Validade (dias, Data)</li> <li>• Não-currentVersionExpiration (não-currentDays)</li> <li>• Filtro (prefixo, Tag)</li> <li>• Estado</li> <li>• ID</li> </ul> <p>O StorageGRID não oferece suporte a essas ações:</p> <ul style="list-style-type: none"> <li>• AbortIncompleteMultipartUpload</li> <li>• ExpiredObjectDeleteMarker</li> <li>• Transição</li> </ul> <p>Para entender como a ação Expiration em um ciclo de vida de um bucket interage com as instruções de colocação do ILM, consulte "como o ILM opera ao longo da vida de um objeto" nas instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.</p> <p><b>Nota:</b> 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
COLOCAR notificação de balde	<p>Esta operação configura notificações para o bucket usando o XML de configuração de notificação incluído no corpo da solicitação. Você deve estar ciente dos seguintes detalhes de implementação:</p> <ul style="list-style-type: none"> <li>• O StorageGRID oferece suporte a tópicos do Serviço de notificação simples (SNS) como destinos. Os endpoints do Simple Queue Service (SQS) ou do Amazon Lambda não são suportados.</li> <li>• 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.</li> </ul> <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 <code>InvalidArgument</code>.</p> <ul style="list-style-type: none"> <li>• Não é possível configurar uma notificação para os seguintes tipos de eventos. Esses tipos de eventos são <b>não</b> suportados. <ul style="list-style-type: none"> <li>◦ <code>s3:ReducedRedundancyLostObject</code></li> <li>◦ <code>s3:ObjectRestore:Completed</code></li> </ul> </li> <li>• As notificações de eventos enviadas do StorageGRID usam o formato JSON padrão, exceto que elas não incluem algumas chaves e usam valores específicos para outras, como mostrado na seguinte listagem:</li> </ul> <ul style="list-style-type: none"> <li>• <b>EventSource</b> <pre>sgws:s3</pre> </li> <li>• <b>AwsRegion</b> <pre>não incluído</pre> </li> <li>• <b>x-amz-id-2</b> <pre>não incluído</pre> </li> <li>• <b>arn</b> <pre>urn:sgws:s3:::bucket_name</pre> </li> </ul>
Política COLOCAR balde	Esta operação define a política anexada ao balde.



Operação	Implementação
COLOQUE a replicação do balde	<p>Esta operação configura a replicação do StorageGRID CloudMirror para o bucket usando o XML de configuração de replicação fornecido no corpo da solicitação. Para a replicação do CloudMirror, você deve estar ciente dos seguintes detalhes de implementação:</p> <ul style="list-style-type: none"> <li>• 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, consulte <a href="#">"Documentação do Amazon S3 sobre configuração de replicação"</a>.</li> <li>• A replicação do bucket pode ser configurada em buckets versionados ou não versionados.</li> <li>• 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> <li>• 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.</li> </ul> <p>O endpoint deve existir para que a configuração de replicação seja bem-sucedida. Se o endpoint não existir, a solicitação falhará como um <code>400 Bad Request</code>. a mensagem de erro indica: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code></p> <ul style="list-style-type: none"> <li>• 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> <li>• Se você omitir a classe de armazenamento do XML de configuração, o StorageGRID usará a <code>STANDARD</code> classe de armazenamento por padrão.</li> <li>• 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 style="list-style-type: none"> <li>◦ 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> <li>◦ 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.</li> </ul> </li> </ul>
COLOQUE a marcação de balde	<p>Esta operação 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"> <li>• O StorageGRID e o Amazon S3 suportam até 50 tags para cada bucket.</li> <li>• As tags associadas a um bucket devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento.</li> <li>• Os valores de tag podem ter até 256 caracteres Unicode de comprimento.</li> <li>• Chave e valores são sensíveis a maiúsculas e minúsculas.</li> </ul>

Operação	Implementação
COLOQUE o controle de versão do Bucket	<p>Essa implementação usa <code>versioning</code> o subrecurso para definir o estado de controle de versão de um bucket existente. Você pode definir o estado de controle de versão com um dos seguintes valores:</p> <ul style="list-style-type: none"> <li>• <b>Habilitado:</b> Permite o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo.</li> <li>• <b>Suspensão:</b> Desativa o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão <code>null</code>.</li> </ul>
COLOCAR Configuração bloqueio Objeto	<p>Esta operação 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><a href="#">COLOCAR Configuração bloqueio Objeto</a> Consulte para obter informações detalhadas.</p>

### Informações relacionadas

[Controles de consistência](#)

[OBTER último pedido de tempo de acesso do Bucket](#)

[Políticas de acesso ao bucket e ao grupo](#)

[S3 operações rastreadas em logs de auditoria](#)

[Gerenciar objetos com ILM](#)

[Use a conta de locatário](#)

## Crie a configuração do ciclo de vida do S3

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

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

### Qual é a configuração do ciclo de vida

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

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

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

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

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

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

## Criar configuração do ciclo de vida

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

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



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

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

```

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

```

## Aplique a configuração do ciclo de vida ao bucket

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

## Use retenção padrão do bucket do bloqueio de objetos S3

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

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

### OBTER Configuração bloqueio Objeto

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

o bucket.

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

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

### Exemplo de solicitação

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

### Exemplo de resposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/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>
```

## COLOCAR Configuração bloqueio Objeto

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

as configurações de retenção padrão configuradas anteriormente.

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

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

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

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

### Exemplo de solicitação

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

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

## Operações personalizadas em buckets

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

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



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

### **Informações relacionadas**

[S3 operações rastreadas nos logs 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.