



Operações personalizadas do StorageGRID

StorageGRID software

NetApp
December 03, 2025

Índice

Operações personalizadas do StorageGRID	1
Operações personalizadas do StorageGRID	1
Consistência do balde GET	1
Exemplo de solicitação	2
Resposta	2
Exemplo de resposta	2
Consistência do balde PUT	3
Solicitar	3
Exemplo de solicitação	4
Último horário de acesso do Bucket GET	4
Exemplo de solicitação	4
Exemplo de resposta	4
Hora do último acesso ao bucket PUT	5
Exemplos de solicitação	6
EXCLUIR configuração de notificação de metadados do bucket	6
Exemplo de solicitação	6
Configuração de notificação de metadados do GET Bucket	6
Exemplo de solicitação	7
Resposta	7
Exemplo de resposta	9
Configuração de notificação de metadados do PUT Bucket	10
Solicitar	10
Exemplos de solicitação	12
JSON gerado pelo serviço de integração de pesquisa	14
Metadados de objeto incluídos em notificações de metadados	15
Solicitação de uso de armazenamento GET	16
Exemplo de solicitação	16
Exemplo de resposta	16
Controle de versão	17
Solicitações de bucket obsoletas para conformidade legada	17
Solicitações de bucket obsoletas para conformidade legada	17
Obsoleto: modificações na solicitação CreateBucket para conformidade	18
Obsoleto: solicitação de conformidade do GET Bucket	19
Obsoleto: solicitação de conformidade do PUT Bucket	20

Operações personalizadas do StorageGRID

Operações personalizadas do StorageGRID

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

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

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

Consistência do balde GET

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

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

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

Exemplo de solicitação

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

Resposta

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

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

Exemplo de resposta

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

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

Informações relacionadas

["Valores de consistência"](#)

Consistência do balde PUT

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

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

Antes de começar

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

Solicitar

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

Consistência	Descrição
todos	Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
forte-global	Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
site forte	Garante consistência de leitura após gravação para todas as solicitações de clientes em um site.
leitura após nova escrita	(Padrão) Fornece consistência de leitura após gravação para novos objetos e consistência eventual para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.

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

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

Exemplo de solicitação

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

Informações relacionadas

["Valores de consistência"](#)

Último horário de acesso do Bucket GET

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

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

Exemplo de solicitação

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

Exemplo de resposta

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

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

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

Hora do último acesso ao bucket PUT

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

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



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

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

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

Exemplos de solicitação

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

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

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

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

EXCLUIR configuração de notificação de metadados do bucket

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

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

Exemplo de solicitação

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

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

Configuração de notificação de metadados do GET Bucket

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

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

Exemplo de solicitação

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

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

Resposta

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

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

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

Nome	Descrição	Obrigatório
Configuração de Notificação de Metadados	Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos Rule.	Sim

Nome	Descrição	Obrigatório
Regra	<p>Tag de contêiner 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
EU IA	<p>Identificador exclusivo para a regra.</p> <p>Incluído no elemento Rule.</p>	Não
Status	<p>O status pode ser "Habilitado" ou "Desabilitado". Nenhuma ação é tomada para regras que estão desabilitadas.</p> <p>Incluído no elemento Rule.</p>	Sim
Prefixo	<p>Objetos que correspondem ao prefixo são afetados pela regra, e seus metadados são enviados ao destino especificado.</p> <p>Para corresponder a todos os objetos, especifique um prefixo vazio.</p> <p>Incluído no elemento Rule.</p>	Sim
Destino	<p>Tag de contêiner para o destino de uma regra.</p> <p>Incluído no elemento Rule.</p>	Sim

Nome	Descrição	Obrigatório
Urna	<p>URN do destino para onde os metadados do objeto são enviados. Deve ser a URN de um ponto de extremidade StorageGRID com as seguintes propriedades:</p> <ul style="list-style-type: none"> • <code>`es`</code> deve ser o terceiro elemento. • A URN deve terminar com o índice e o tipo onde os metadados são armazenados, no formato <code>domain-name/myindex/mytype</code>. <p>Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. 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 ponto de extremidade deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404.</p> <p>A urna está incluída no elemento Destino.</p>	Sim

Exemplo de resposta

O XML incluído entre o

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

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

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:33333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Informações relacionadas

["Use uma conta de inquilino"](#)

Configuração de notificação de metadados do PUT Bucket

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

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

Solicitar

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

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

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

Os destinos devem ser especificados usando o URN de um ponto de extremidade StorageGRID . O ponto de

extremidade deve existir quando a configuração de notificação de metadados for enviada, ou a solicitação falhará como um 400 Bad Request. A mensagem de erro diz: Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: *URN*.

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

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

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

Nome	Descrição	Obrigatório
Status	<p>O status pode ser "Habilitado" ou "Desabilitado". Nenhuma ação é tomada para regras que estão desabilitadas.</p> <p>Incluído no elemento Rule.</p>	Sim
Prefixo	<p>Objetos que correspondem ao prefixo são afetados pela regra, e seus metadados são enviados ao destino especificado.</p> <p>Para corresponder a todos os objetos, especifique um prefixo vazio.</p> <p>Incluído no elemento Rule.</p>	Sim
Destino	<p>Tag de contêiner para o destino de uma regra.</p> <p>Incluído no elemento Rule.</p>	Sim
Urna	<p>URN do destino para onde os metadados do objeto são enviados. Deve ser a URN de um ponto de extremidade StorageGRID com as seguintes propriedades:</p> <ul style="list-style-type: none"> • `es` deve ser o terceiro elemento. • A URN deve terminar com o índice e o tipo onde os metadados são armazenados, no formato <code>domain-name/myindex/mytype</code>. <p>Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. 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 ponto de extremidade deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404.</p> <p>A urna está incluída no elemento Destino.</p>	Sim

Exemplos de solicitação

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

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

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

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

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

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333: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 habilita o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado ao ponto de extremidade de destino sempre que metadados ou tags de objeto são adicionados, atualizados ou excluídos.

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


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

Metadados de objeto incluídos em notificações de metadados

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

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

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

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



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

Informações relacionadas

["Use uma conta de inquilino"](#)

Solicitação de uso de armazenamento GET

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

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

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

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

Exemplo de solicitação

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

Exemplo de resposta

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

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

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

Controle de versão

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

Informações relacionadas

["Valores de consistência"](#)

Solicitações de bucket obsoletas para conformidade legada

Solicitações de bucket obsoletas para conformidade legada

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

Recurso de conformidade obsoleto

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

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

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

Solicitações de conformidade obsoletas:

- ["Obsoleto - Modificações na solicitação do bucket PUT para conformidade"](#)

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

- ["Obsoleto - Conformidade com o GET Bucket"](#)

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

- ["Obsoleto - Conformidade com PUT Bucket"](#)

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

Obsoleto: modificações na solicitação CreateBucket para conformidade

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



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

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

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

The Compliance feature is deprecated.

Contact your StorageGRID administrator if you need to create new Compliant buckets.

Obsoleto: solicitação de conformidade do GET Bucket

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



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

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

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

Exemplo de solicitação

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

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

Exemplo de resposta

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

```

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

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

```

Nome	Descrição
Período de retenção em minutos	A duração do período de retenção para objetos adicionados a este bucket, em minutos. O período de retenção começa quando o objeto é ingerido na grade.
Retenção Legal	<ul style="list-style-type: none"> • Verdadeiro: Este bucket está atualmente sob retenção legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja suspensão, mesmo que o período de retenção tenha expirado. • Falso: Este bucket não está atualmente sob retenção legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Exclusão automática	<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 retenção legal. • Falso: Os objetos neste bucket não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Respostas de erro

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

Obsoleto: solicitação de conformidade do PUT Bucket

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



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

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

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

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

Exemplo de solicitação

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

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

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

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

Nome	Descrição
Retenção Legal	<ul style="list-style-type: none"> • Verdadeiro: Este bucket está atualmente sob retenção legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja suspensa, mesmo que o período de retenção tenha expirado. • Falso: Este bucket não está atualmente sob retenção legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Exclusão automática	<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 retenção legal. • Falso: Os objetos neste bucket não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Consistência para configurações de conformidade

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

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

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



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

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

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


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

Respostas de erro

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

Informações relacionadas

["Obsoleto: modificações na solicitação do bucket PUT para conformidade"](#)

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 SOBRESSALENTE; 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.