



# **USE A API REST DO S3**

## **StorageGRID**

NetApp  
October 03, 2025

# Índice

Use S3	1
Suporte para a API REST do S3	1
Alterações ao suporte à API REST do S3	1
Versões suportadas	4
Suporte para serviços de plataforma StorageGRID	4
Configurando contas de locatário e conexões	5
Criação e configuração de contas de locatário do S3	5
Como as conexões do cliente podem ser configuradas	6
Nomes de domínio de endpoint para solicitações S3	9
Testando a configuração da API REST do S3	10
Como o StorageGRID implementa a API REST do S3	11
Solicitações de cliente conflitantes	11
Controles de consistência	11
Como as regras do StorageGRID ILM gerenciam objetos	15
Controle de versão de objetos	16
Recomendações para a implementação da API REST do S3	17
S3 operações e limitações suportadas pela API REST	18
Tratamento da data	18
Cabeçalhos de solicitação comuns	19
Cabeçalhos de resposta comuns	19
Autenticando solicitações	19
Operações no serviço	20
Operações em baldes	20
Operações personalizadas em buckets	34
Operações em objetos	35
Operações para uploads de várias partes	60
Respostas de erro	68
Operações da API REST do StorageGRID S3	71
OBTENHA pedido de consistência de balde	71
COLOCAR pedido consistência balde	72
OBTENHA último pedido de tempo de acesso do Bucket	74
COLOCAR o último pedido de tempo de acesso do balde	74
EXCLUIR solicitação de configuração de notificação de metadados do bucket	76
OBTENHA solicitação de configuração de notificação de metadados do bucket	76
COLOCAR solicitação de configuração de notificação de metadados do bucket	80
OBTENHA solicitação de uso de armazenamento	87
Solicitações de bucket obsoletas para conformidade legada	88
Políticas de acesso ao bucket e ao grupo	94
Visão geral da política de acesso	94
Configurações de controle de consistência para políticas	96
Usando o ARN nas declarações de política	97
Especificando recursos em uma política	98
Especificando princípios em uma política	98

Especificando permissões em uma política .....	99
Usando a permissão PutOverwriteObject .....	104
Especificando condições em uma política .....	104
Especificando variáveis em uma política .....	107
Criação de políticas que exigem manipulação especial .....	108
Proteção WORM (write-once-read-many) .....	110
S3 exemplos de políticas .....	111
Configurando a segurança para a API REST .....	120
Como o StorageGRID fornece segurança para a API REST .....	120
Algoritmos de hash e criptografia suportados para bibliotecas TLS .....	122
Operações de monitoramento e auditoria .....	123
Monitoramento de taxas de ingestão e recuperação de objetos .....	123
Acesso e revisão de logs de auditoria .....	125
Benefícios de conexões HTTP ativas, ociosas e simultâneas .....	126
Benefícios de manter conexões HTTP ociosas abertas .....	127
Benefícios de conexões HTTP ativas .....	127
Benefícios de conexões HTTP simultâneas .....	128
Separação de pools de conexão HTTP para operações de leitura e gravação .....	129

# Use S3

Saiba como os aplicativos clientes podem usar a API S3 para fazer interface com o sistema StorageGRID.

- ["Suporte para a API REST do S3"](#)
- ["Configurando contas de locatário e conexões"](#)
- ["Como o StorageGRID implementa a API REST do S3"](#)
- ["S3 operações e limitações suportadas pela API REST"](#)
- ["Operações da API REST do StorageGRID S3"](#)
- ["Políticas de acesso ao bucket e ao grupo"](#)
- ["Configurando a segurança para a API REST"](#)
- ["Operações de monitoramento e auditoria"](#)
- ["Benefícios de conexões HTTP ativas, ociosas e simultâneas"](#)

## Suporte para a API REST do S3

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 aplicações orientadas a serviços desenvolvidas para serviços da Web do S3 ao storage de objetos no local que usa o sistema StorageGRID. Isso requer alterações mínimas no uso atual de chamadas de API REST do aplicativo cliente S3.

- ["Alterações ao suporte à API REST do S3"](#)
- ["Versões suportadas"](#)
- ["Suporte para serviços de plataforma StorageGRID"](#)

## Alterações ao suporte à API REST do S3

Você deve estar ciente das alterações no suporte do sistema StorageGRID para a API REST do S3.

Solte	Comentários
11,5	<ul style="list-style-type: none"><li>• Adicionado suporte para gerenciar a criptografia de bucket.</li><li>• Adicionado suporte para S3 Object Lock e solicitações de conformidade legadas obsoletas.</li><li>• Adicionado suporte para o uso DE EXCLUIR vários objetos em buckets versionados.</li><li>• O Content-MD5 cabeçalho de solicitação agora é suportado corretamente.</li></ul>

Solte	Comentários
11,4	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Para buckets criados no StorageGRID 11,4, não é mais necessário restringir nomes de chaves de objeto para atender às práticas recomendadas de desempenho.</li> <li>• Adicionado suporte para notificações de intervalo no <code>s3:ObjectRestore:Post</code> tipo de evento.</li> <li>• 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.</li> <li>• Adicionado suporte para TLS 1,3 e lista atualizada de pacotes de criptografia TLS suportados.</li> <li>• O serviço CLB está obsoleto.</li> </ul>
11,3	<ul style="list-style-type: none"> <li>• Adicionado suporte para criptografia no lado do servidor de dados de objeto com chaves fornecidas pelo cliente (SSE-C).</li> <li>• 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.</li> <li>• PUT Object, put Object - Copy e Multipart Upload atualizados para descrever o impactos das regras ILM que usam o posicionamento síncrono na ingestão.</li> <li>• Lista atualizada dos conjuntos de encriptação TLS suportados. As cifras TLS 1,1 não são mais suportadas.</li> </ul>

Solte	Comentários
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><b>Observação:</b> 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 configuração de controle de 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.

## Versões suportadas

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

Item	Versão
Especificação S3	<i>Referência da API de serviço de armazenamento simples 2006-03-01</i>
HTTP	1,1  Para obter mais informações sobre HTTP, consulte HTTP/1,1 (RFCs 7230-35).  <b>Nota:</b> O StorageGRID não suporta a canalização HTTP/1,1.

### Informações relacionadas

["IETF RFC 2616: Protocolo de transferência de hipertexto \(HTTP/1,1\)"](#)

["Documentação do Amazon Web Services \(AWS\): Referência da API do Amazon Simple Storage Service"](#)

## Suporte para serviços de plataforma StorageGRID

Os serviços da plataforma StorageGRID permitem que as contas de locatários do StorageGRID aproveitem serviços externos, como um bucket remoto do S3, um endpoint do Serviço de notificação simples (SNS) ou um cluster do Elasticsearch para estender os serviços fornecidos por uma grade.

A tabela a seguir resume os serviços de plataforma disponíveis e as APIs do S3 usadas para configurá-los.

Serviço de plataforma	Finalidade	S3 API usada para configurar o serviço
Replicação do CloudMirror	Replica objetos de um bucket do StorageGRID de origem para o bucket do S3 remoto configurado.	COLOQUE a replicação do balde
Notificações	Envia notificações sobre eventos em um bucket do StorageGRID de origem para um endpoint configurado do Serviço de notificação simples (SNS).	COLOCAR notificação de balde
Integração de pesquisa	Envia metadados de objetos para objetos armazenados em um bucket do StorageGRID para um índice Elasticsearch configurado.	NOTIFICAÇÃO DE metadados do Bucket  <b>Observação:</b> esta é uma API S3D personalizada do StorageGRID.

Um administrador de grade deve habilitar o uso de serviços de plataforma para uma conta de locatário antes que eles possam ser usados. Em seguida, um administrador de locatário deve criar um endpoint que represente o serviço remoto na conta de locatário. Esta etapa é necessária antes que um serviço possa ser configurado.

## Recomendações para o uso de serviços de plataforma

Antes de usar os serviços de plataforma, você deve estar ciente das seguintes recomendações:

- A NetApp recomenda que você não permita mais de 100 locatários ativos com solicitações do S3 que exigem replicação, notificações e integração de pesquisa do CloudMirror. Ter mais de 100 inquilinos ativos pode resultar em desempenho mais lento do cliente S3.
- Se um bucket do S3 no sistema do StorageGRID tiver o controle de versão e a replicação do CloudMirror habilitado, a NetApp recomenda que o endpoint de destino também tenha o controle de versão do bucket do S3 habilitado. Isso permite que a replicação do CloudMirror gere versões de objetos semelhantes no endpoint.
- A replicação do CloudMirror não é suportada se o bucket de origem tiver o S3 Object Lock ativado.
- A replicação do CloudMirror falhará com um erro AccessDenied se o intervalo de destino tiver conformidade legada habilitada.

### Informações relacionadas

["Use uma conta de locatário"](#)

["Administrar o StorageGRID"](#)

["Operações em baldes"](#)

["COLOCAR solicitação de configuração de notificação de metadados do bucket"](#)

## Configurando contas de locatário e conexões

Configurar o StorageGRID para aceitar conexões de aplicativos cliente requer a criação de uma ou mais contas de locatário e a configuração das conexões.

### Criação e configuração de contas de locatário do S3

Uma conta de locatário S3 é necessária antes que os clientes API S3D possam armazenar e recuperar objetos no StorageGRID. Cada conta de locatário tem seu próprio ID de conta, grupos e usuários, além de contentores e objetos.

As contas de locatário do S3 são criadas por um administrador de grade do StorageGRID usando o Gerenciador de grade ou a API de gerenciamento de grade. Ao criar uma conta de locatário do S3, o administrador da grade especifica as seguintes informações:

- Nome de exibição para o locatário (o ID da conta do locatário é atribuído automaticamente e não pode ser alterado).
- Se a conta de locatário tem permissão para usar serviços de plataforma. Se o uso de serviços de plataforma for permitido, a grade deve ser configurada para suportar seu uso.
- Opcionalmente, uma cota de armazenamento para a conta de locatário - o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos do locatário. A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco).



- Se a federação de identidade estiver ativada para o sistema StorageGRID, qual grupo federado tem permissão de acesso root para configurar a conta de locatário.
- Se o logon único (SSO) não estiver em uso para o sistema StorageGRID, se a conta do locatário usará sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.

Depois que uma conta de locatário do S3 for criada, os usuários do locatário poderão acessar o Gerenciador do locatário para executar tarefas como as seguintes:

- Configure a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e crie grupos e usuários locais
- Gerenciar S3 chaves de acesso
- Crie e gerencie buckets do S3, incluindo buckets que têm o bloqueio de objetos do S3 ativado
- Usar serviços de plataforma (se ativado)
- Monitorar o uso do storage



Os usuários de locatários do S3 podem criar e gerenciar buckets do S3 com o Tenant Manager, mas precisam ter S3 chaves de acesso e usar a API REST do S3 para ingerir e gerenciar objetos.

#### Informações relacionadas

["Administrar o StorageGRID"](#)

["Use uma conta de locatário"](#)

## Como as conexões do cliente podem ser configuradas

Um administrador de grade faz escolhas de configuração que afetam a forma como os clientes S3 se conectam ao StorageGRID para armazenar e recuperar dados. As informações específicas que você precisa para fazer uma conexão dependem da configuração escolhida.

Os aplicativos clientes podem armazenar ou recuperar objetos conectando-se a qualquer um dos seguintes:

- O serviço Load Balancer em nós de administração ou nós de gateway, ou, opcionalmente, o endereço IP virtual de um grupo de alta disponibilidade (HA) de nós de administração ou nós de gateway
- O serviço CLB em nós de Gateway, ou, opcionalmente, o endereço IP virtual de um grupo de nós de gateway de alta disponibilidade



O serviço CLB está obsoleto. Os clientes configurados antes da versão do StorageGRID 11,3 podem continuar a usar o serviço CLB nos nós de gateway. Todos os outros aplicativos clientes que dependem do StorageGRID para fornecer balanceamento de carga devem se conectar usando o serviço de balanceamento de carga.

- Nós de storage, com ou sem um balanceador de carga externo

Ao configurar o StorageGRID, um administrador de grade pode usar o Gerenciador de grade ou a API de gerenciamento de grade para executar as seguintes etapas, todas opcionais:

1. Configure endpoints para o serviço Load Balancer.

Você deve configurar endpoints para usar o serviço Load Balancer. O serviço Load Balancer em nós de

administração ou nós de gateway distribui conexões de rede recebidas de aplicativos clientes para nós de storage. Ao criar um endpoint de balanceador de carga, o administrador do StorageGRID especifica um número de porta, se o endpoint aceita conexões HTTP ou HTTPS, o tipo de cliente (S3 ou Swift) que usará o endpoint e o certificado a ser usado para conexões HTTPS (se aplicável).

## 2. Configurar redes de clientes não confiáveis.

Se um administrador do StorageGRID configurar a rede cliente de um nó para não ser confiável, o nó só aceita conexões de entrada na rede cliente em portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

## 3. Configurar grupos de alta disponibilidade.

Se um administrador criar um grupo de HA, as interfaces de rede de vários nós de Admin ou nós de Gateway serão colocadas em uma configuração de backup ativo. As conexões de cliente são feitas usando o endereço IP virtual do grupo HA.

Para obter mais informações sobre cada opção, consulte as instruções para administrar o StorageGRID.

### Informações relacionadas

["Administrar o StorageGRID"](#)

### Resumo: Endereços IP e portas para conexões de clientes

Os aplicativos cliente se conectam ao StorageGRID usando o endereço IP de um nó de grade e o número da porta de um serviço nesse nó. Se os grupos de alta disponibilidade (HA) estiverem configurados, os aplicativos clientes poderão se conectar usando o endereço IP virtual do grupo HA.

#### Informações necessárias para fazer conexões com o cliente

A tabela resume as diferentes maneiras pelas quais os clientes podem se conectar ao StorageGRID e os endereços IP e as portas usadas para cada tipo de conexão. Contate o administrador do StorageGRID para obter mais informações ou consulte as instruções de administração do StorageGRID para obter uma descrição de como localizar essas informações no Gerenciador de Grade.

Onde a conexão é feita	Serviço ao qual o cliente se conecta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	<ul style="list-style-type: none"><li>• Porta de extremidade do balanceador de carga</li></ul>
Grupo HA	CLB  <b>Nota:</b> o serviço CLB está obsoleto.	Endereço IP virtual de um grupo HA	Portas S3 padrão: <ul style="list-style-type: none"><li>• HTTPS: 8082</li><li>• HTTP: 8084</li></ul>
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	<ul style="list-style-type: none"><li>• Porta de extremidade do balanceador de carga</li></ul>

Onde a conexão é feita	Serviço ao qual o cliente se conecta	Endereço IP	Porta
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	<ul style="list-style-type: none"> <li>• Porta de extremidade do balanceador de carga</li> </ul>
Nó de gateway	CLB  <b>Nota:</b> o serviço CLB está obsoleto.	Endereço IP do nó de gateway  <b>Nota:</b> por predefinição, as portas HTTP para CLB e LDR não estão ativadas.	Portas S3 padrão: <ul style="list-style-type: none"> <li>• HTTPS: 8082</li> <li>• HTTP: 8084</li> </ul>
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: <ul style="list-style-type: none"> <li>• HTTPS: 18082</li> <li>• HTTP: 18084</li> </ul>

### Exemplo

Para conectar um cliente S3 ao ponto de extremidade do Load Balancer de um grupo de HA de nós de Gateway, use um URL estruturado como mostrado abaixo:

- `https://VIP-of-HA-group:_LB-endpoint-port_`

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.5 e o número da porta de um endpoint do balanceador de carga S3 for 10443, um cliente S3 poderá usar o seguinte URL para se conectar ao StorageGRID:

- `https://192.0.2.5:10443`

É possível configurar um nome DNS para o endereço IP que os clientes usam para se conectar ao StorageGRID. Contacte o administrador da rede local.

### Informações relacionadas

["Administrar o StorageGRID"](#)

### Decidir usar conexões HTTPS ou HTTP

Quando as conexões de cliente são feitas usando um endpoint de Load Balancer, as conexões devem ser feitas usando o protocolo (HTTP ou HTTPS) especificado para esse endpoint. Para usar HTTP para conexões de cliente a nós de armazenamento ou ao serviço CLB em nós de gateway, você deve habilitar seu uso.

Por padrão, quando os aplicativos cliente se conectam a nós de armazenamento ou ao serviço CLB nos nós de Gateway, eles devem usar HTTPS criptografado para todas as conexões. Opcionalmente, você pode habilitar conexões HTTP menos seguras selecionando a opção de grade **Ativar conexão HTTP** no Gerenciador de Grade. Por exemplo, um aplicativo cliente pode usar HTTP ao testar a conexão com um nó de armazenamento em um ambiente que não seja de produção.



Tenha cuidado ao ativar o HTTP para uma grade de produção, já que as solicitações serão enviadas sem criptografia.



O serviço CLB está obsoleto.

Se a opção **Enable HTTP Connection** estiver selecionada, os clientes devem usar portas diferentes para HTTP do que para HTTPS. Consulte as instruções para administrar o StorageGRID.

#### Informações relacionadas

["Administrar o StorageGRID"](#)

["Benefícios de conexões HTTP ativas, ociosas e simultâneas"](#)

## Nomes de domínio de endpoint para solicitações S3

Antes de poder usar nomes de domínio S3 para solicitações de cliente, um administrador do StorageGRID deve configurar o sistema para aceitar conexões que usam nomes de domínio S3 em solicitações de estilo de caminho S3 e S3 solicitações virtuais de estilo hospedado.

#### Sobre esta tarefa

Para permitir que você use S3 solicitações de estilo hospedadas virtuais, um administrador de grade deve executar as seguintes tarefas:

- Use o Gerenciador de Grade para adicionar os nomes de domínio de endpoint S3 ao sistema StorageGRID.
- Certifique-se de que o certificado que o cliente usa para conexões HTTPS com o StorageGRID está assinado para todos os nomes de domínio que o cliente requer.

Por exemplo, se o endpoint for `s3.company.com`, o administrador de grade deve garantir que o certificado usado para conexões HTTPS inclua o `s3.company.com` endpoint e o nome alternativo (SAN) de assunto universal (Wildcard Subject Alternative Name) do endpoint: `*.s3.company.com`.

- Configure o servidor DNS usado pelo cliente para incluir Registros DNS que correspondam aos nomes de domínio de endpoint, incluindo todos os Registros curinga necessários.

Se o cliente se conectar usando o serviço Load Balancer, o certificado que o administrador da grade configura é o certificado para o ponto de extremidade do balanceador de carga que o cliente usa.



Cada ponto de extremidade do balanceador de carga tem seu próprio certificado e cada ponto de extremidade pode ser configurado para reconhecer nomes de domínio de endpoint diferentes.

Se o cliente conectar nós de armazenamento ou ao serviço CLB nos nós de Gateway, o certificado que o administrador de grade configura é o único certificado de servidor personalizado usado para a grade.



O serviço CLB está obsoleto.

Consulte as instruções para administrar o StorageGRID para obter mais informações.

Depois que essas etapas forem concluídas, você poderá usar solicitações virtuais de estilo hospedado (por exemplo, `bucket.s3.company.com`).

#### Informações relacionadas

["Administrar o StorageGRID"](#)

## Testando 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 no sistema.

### O que você vai precisar

- Você deve ter baixado e instalado a AWS CLI do ["aws.amazon.com/cli"](https://aws.amazon.com/cli).
- Você deve ter criado uma conta de locatário do S3 no sistema StorageGRID.

### Passos

1. Configure as configurações do Amazon Web Services para usar a conta criada no sistema StorageGRID:
  - a. Entre no modo de configuração: `aws configure`
  - b. Insira o ID da chave de acesso da AWS para a conta criada.
  - c. Insira a chave de acesso secreto da AWS para a conta criada.
  - d. Digite a região padrão a ser usada, por exemplo, US-East-1.
  - e. Digite o formato de saída padrão a ser usado ou pressione **Enter** para selecionar JSON.
2. Crie um bucket.

```
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

Um aplicativo cliente pode usar S3 chamadas de API REST para se conectar ao StorageGRID para criar, excluir e modificar buckets, bem como armazenar e recuperar objetos.

- ["Solicitações de cliente conflitantes"](#)
- ["Controles de consistência"](#)
- ["Como as regras do StorageGRID ILM gerenciam objetos"](#)
- ["Controle de versão de objetos"](#)
- ["Recomendações para a implementação da API REST do S3"](#)

### Solicitações de cliente conflitantes

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos".

O calendário 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.

### Controles de consistência

Os controles de consistência fornecem uma troca entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós e sites de storage, conforme exigido pelo 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 um nível de consistência diferente, você pode especificar um controle de consistência para cada bucket ou para cada operação de API.

## Controles de consistência

O controle de 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 o controle de consistência para um bucket ou uma operação de API para um dos seguintes valores:

Controle de 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. Corresponde às garantias de consistência do Amazon S3.  <b>Observação:</b> se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, defina o controle de consistência como "disponível", a menos que você exija garantias de consistência semelhantes ao Amazon S3.
Disponível (eventual consistência para OPERAÇÕES DE CABEÇA)	Comporta-se da mesma forma que o nível de consistência "read-after-novo-write", mas apenas fornece consistência eventual para operações HEAD. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis. Difere das garantias de consistência do Amazon S3 apenas para operações PRINCIPAIS.

## Usando os controles de consistência "read-after-new-write" e "available"

Quando uma operação HEAD ou GET usa o controle de consistência "read-after-novo-write" ou uma operação GET usa o controle de consistência "disponível", 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 nível de consistência até atingir o mais alto

nível de consistência, "All", o que requer que todas as cópias dos metadados do objeto estejam disponíveis.

Se uma operação HEAD ou GET usar o controle de consistência "read-after-novo-write", mas o objeto não existir, a pesquisa de objetos sempre alcançará o nível de consistência "all". Como esse nível de consistência exige que todas as cópias dos metadados do objeto estejam disponíveis, você pode receber um número alto de 500 erros de servidor interno se um ou mais nós de storage não estiverem disponíveis.

A menos que você precise de garantias de consistência semelhantes ao Amazon S3, você pode evitar esses erros para operações HEAD definindo o controle de consistência como "disponível". Quando uma operação HEAD usa o controle de consistência "disponível", o StorageGRID fornece consistência eventual apenas. Ele não tenta novamente uma operação com falha até atingir o nível de consistência "tudo", portanto, não requer que todas as cópias dos metadados do objeto estejam disponíveis.

### Especificando o controle de consistência para uma operação de API

Para definir o controle de consistência para uma operação de API individual, os controles de consistência devem ser suportados para a operação e você deve especificar o controle de consistência no cabeçalho da solicitação. Este exemplo define o controle de consistência como "local-strong" para uma operação GET Object.

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



Você deve usar o mesmo controle de consistência para as operações COLOCAR Objeto e OBTER Objeto.

### Especificando o controle de consistência para um bucket

Para definir o controle de consistência para o bucket, você pode usar a solicitação de consistência do bucket do StorageGRID PUT e a solicitação DE consistência do bucket do GET. Ou você pode usar o Gerenciador do Locatário ou a API de Gerenciamento do Locatário.

Ao definir os controles de consistência para um balde, tenha em atenção o seguinte:

- Definir o controle de consistência para um balde determina qual controle de consistência é usado para operações S3D realizadas nos objetos no balde ou na configuração do balde. Não afeta as operações no próprio balde.
- O controle de consistência para uma operação de API individual substitui o controle de consistência para o bucket.
- Em geral, os buckets devem usar o controle de 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 o controle de consistência para cada solicitação de API. Defina o controle de consistência no nível do balde apenas como último recurso.



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

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

Por exemplo, o controle de consistência usado 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 nível de consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas do sistema mais previsíveis.

Os seguintes comportamentos de ingestão estão disponíveis para regras ILM:

- **Strict:** Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja devolvido ao cliente.
- **Balanced:** O StorageGRID tenta fazer todas as cópias especificadas na regra ILM no ingest; 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.
- **\* Commit duplo\*:** O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.



Antes de selecionar o comportamento de ingestão para uma regra ILM, leia a descrição completa dessas configurações nas instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

### Exemplo de como o controle de consistência e a regra ILM podem interagir

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

- **Regra ILM:** Crie duas cópias de objeto, uma no local e outra em um local remoto. O comportamento de ingestão estrita é selecionado.
- **Nível de consistência:** "Trong-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 o nível de consistência "site-trong", o cliente poderá receber uma mensagem de sucesso depois que os dados do objeto forem 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 níveis de consistência e regras de ILM pode ser complexa. Contacte a NetApp se necessitar de assistência.

### Informações relacionadas

"Gerenciar objetos com ILM"

"OBTER pedido de consistência de balde"

"COLOCAR pedido consistência balde"

## Como as regras do StorageGRID ILM gerenciam objetos

O administrador da grade cria regras de gerenciamento do ciclo de vida das informações (ILM) para gerenciar dados de objetos ingeridos no sistema StorageGRID a partir de aplicativos clientes da API REST do S3. Essas regras são então adicionadas à política ILM para determinar como e onde os dados do objeto são armazenados ao longo do tempo.

As configurações de ILM determinam os seguintes aspectos de um objeto:

- **Geografia**

O local dos dados de um objeto, seja no sistema StorageGRID (pool de storage) ou em um pool de storage de nuvem.

- **Grau de armazenamento**

O tipo de storage usado para armazenar dados de objetos: Por exemplo, flash ou disco giratório.

- **\* Proteção contra perdas\***

Quantas cópias são feitas e os tipos de cópias criadas: Replicação, codificação de apagamento ou ambos.

- **Retenção**

As mudanças ao longo do tempo para como os dados de um objeto são gerenciados, onde são armazenados e como eles são protegidos contra perda.

- **Proteção durante o consumo**

O método usado para proteger dados de objetos durante a ingestão: Colocação síncrona (usando as opções balanceadas ou rigorosas para o comportamento de ingestão) ou fazendo cópias provisórias (usando a opção de confirmação dupla).

As regras do ILM podem filtrar e selecionar objetos. Para objetos ingeridos usando S3, as regras do ILM podem filtrar objetos com base nos seguintes metadados:

- Conta de locatário
- Nome do balde
- Tempo de ingestão
- Chave
- Último tempo de acesso



Por padrão, as atualizações para o último tempo de acesso são desativadas para todos os buckets do S3. Se o seu sistema StorageGRID incluir uma regra ILM que use a opção último tempo de acesso, você deverá habilitar as atualizações para o último tempo de acesso para os buckets do S3 especificados nessa regra. Você pode habilitar as atualizações da última hora de acesso usando a solicitação de última hora de acesso do PUT Bucket, a caixa de seleção **S3 Buckets Configurar último tempo de acesso** no Gerenciador de locatário ou usando a API de Gerenciamento de locatário. Ao ativar as atualizações da última hora de acesso, esteja ciente de que o desempenho do StorageGRID pode ser reduzido, especialmente em sistemas com objetos pequenos.

- Restrição de localização
- Tamanho do objeto
- Metadados do utilizador
- Etiqueta Objeto

Para obter mais informações sobre o ILM, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

#### Informações relacionadas

["Use uma conta de locatário"](#)

["Gerenciar objetos com ILM"](#)

["COLOCAR o último pedido de tempo de acesso do balde"](#)

## Controle de versão de objetos

Você pode usar o controle de versão para reter várias versões de um objeto, o que protege contra a exclusão acidental de objetos e permite recuperar e restaurar 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 para ativar essa funcionalidade para o bucket. Cada objeto no seu 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 ao versionamento permite criar regras ILM que usam o tempo não-atual como o tempo de referência. Quando um objeto é atualizado, suas versões anteriores se tornam não atuais. O uso de um filtro de tempo não atual permite criar políticas que reduzam 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.

Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações para obter um exemplo de política ILM para objetos com versão S3.

#### Informações relacionadas

["Gerenciar objetos com ILM"](#)

## 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 seu aplicativo verifica rotineiramente para ver se um objeto existe em um caminho onde você não espera que o objeto realmente exista, você deve usar o controle de consistência ""disponível"". Por exemplo, você deve usar o controle de consistência "disponível" se seu aplicativo dirigir um local antes DE COLOCÁ-lo.

Caso contrário, se a operação PRINCIPAL não encontrar o objeto, você poderá receber um número alto de 500 erros de servidor interno se um ou mais nós de storage não estiverem disponíveis.

Você pode definir o controle de consistência ""disponível"" para cada bucket usando a solicitação de consistência do PUT Bucket, ou você pode especificar o controle de consistência no cabeçalho da solicitação para uma operação de API individual.

### Recomendações para chaves de objeto

Para buckets criados no StorageGRID 11,4 ou posterior, não é mais necessário restringir nomes de chaves do objeto para atender às práticas recomendadas de desempenho. Por exemplo, agora você pode usar valores aleatórios para os primeiros quatro caracteres de nomes de chave de objeto.

Para buckets que foram criados em versões anteriores ao StorageGRID 11,4, continue seguindo estas recomendações para nomes de chaves de objeto:

- Você não deve usar 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, você deve usar 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, você deve prefixar 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
```

## Recomendações para "leituras de intervalo"

Se a opção **Compress Stored Objects** estiver selecionada (**Configuration Grid Options**), os aplicativos cliente S3 devem evitar executar operações GET Object que especifiquem um intervalo de bytes serão retornados. Essas operações de leitura de intervalo são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GET Object que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é muito 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.

### Informações relacionadas

["Controles de consistência"](#)

["COLOCAR pedido consistência balde"](#)

["Administrar o StorageGRID"](#)

## S3 operações e limitações suportadas pela API REST

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.

- ["Autenticando solicitações"](#)
- ["Operações no serviço"](#)
- ["Operações em baldes"](#)
- ["Operações personalizadas em buckets"](#)
- ["Operações em objetos"](#)
- ["Operações para uploads de várias partes"](#)
- ["Respostas de erro"](#)

## 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 cabeçalhos de solicitação comuns definidos pela *Simple Storage Service API Reference*, 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"><li>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.</li></ul>
<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

### Informações relacionadas

["Documentação do Amazon Web Services \(AWS\): Referência da API do Amazon Simple Storage Service"](#)

## Autenticando 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.

## Usando 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.

## Usando 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
Serviço GET	Implementado com todo o comportamento da API REST do Amazon S3.
OBTER 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. 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.

### Informações relacionadas

["OBTER solicitação de uso de armazenamento"](#)

## 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"](#)

## "Nomes de domínio de endpoint para solicitação 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.

Operação	Implementação
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.
OBTENHA o controle de versão do Bucket	Essa implementação usa <code>versioning</code> o subrecurso para retornar o estado de controle de versão de um bucket. O estado de versionamento retornado indica se o bucket está "não versionado" ou se o bucket é a versão "habilitado" ou "suspense".
OBTER Configuração bloqueio Objeto	Esta operação determina se o bloqueio de objetos S3D está ativado para um balde. <a href="#">"Usando S3 Object Lock"</a>
Balde DA cabeça	Esta operação determina se existe um intervalo e você tem permissão para acessá-lo.

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 hífen.</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. <b>Nota:</b> Ocorrerá um erro se a solicitação <code>PUT Bucket</code> usar uma região que não foi definida no StorageGRID.</li> <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.</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> <p><a href="#">"Usando S3 Object Lock"</a></p>

Operação	Implementação
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>
COLOQUE a criptografia Bucket	<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>

Operação	Implementação
COLOQUE o ciclo de vida do balde	<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: <ul style="list-style-type: none"> <li>• <b>EventSource</b></li> </ul> <pre>sgws:s3</pre> <li>• <b>AwsRegion</b></li> </li></ul> <pre>não incluído</pre> <ul style="list-style-type: none"> <li>• <b>x-amz-id-2</b></li> </ul> <pre>não incluído</pre> <ul style="list-style-type: none"> <li>• <b>arn</b></li> </ul> <pre>urn:sgws:s3:::bucket_name</pre>
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. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes.</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 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 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>

Operação	Implementação
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>
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>

### Informações relacionadas

["Documentação do Amazon Web Services \(AWS\): Replicação entre regiões"](#)

["Controles de consistência"](#)

["OBTENHA o último pedido de tempo de acesso do Bucket"](#)

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

["Usando S3 Object Lock"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

["Gerenciar objetos com ILM"](#)

["Use uma conta de locatário"](#)

### Criando uma 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 a criação de configurações de ciclo de vida do S3, consulte a seção sobre gerenciamento do ciclo de vida do objeto no *Amazon Simple Storage Service Developer Guide*. Observe que o StorageGRID suporta apenas ações de expiração; ele não oferece suporte a ações de transição.

## "Amazon Simple Storage Service Developer Guide: Gerenciamento do ciclo de vida do objeto"

### O que é uma configuração de 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, consulte "como o ILM opera ao longo da vida de um objeto" nas instruções para gerenciar objetos com gerenciamento do ciclo de vida da informação.



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

### Criando a 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"
    }
  ]
}

```

### Aplicando uma configuração de ciclo de vida a um 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.

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

```
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.

### A validação da expiração do ciclo de vida do bucket se aplica a um 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, consulte `""como a retenção de objetos é determinada""` nas instruções para executar a administração do StorageGRID.

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": {}
}
```

## Informações relacionadas

["Operações em baldes"](#)

["Gerenciar objetos com ILM"](#)

## 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.

Operação	Descrição	Para mais informações
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>

<b>Operação</b>	<b>Descrição</b>	<b>Para mais informações</b>
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 modificações no balde para conformidade	Obsoleto e não suportado: Você não pode mais criar novos buckets com a conformidade ativada.	<a href="#">"Obsoleto: Modificações de solicitação de Bucket para 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"](#)

## Operações em objetos

Esta seção descreve como o sistema StorageGRID implementa S3 operações de API

## REST para objetos.

- "Usando S3 Object Lock"
- "Usando criptografia do lado do servver"
- "Objeto GET"
- "Objeto HEAD"
- "Restauração PÓS-objeto"
- "Objeto PUT"
- "COLOCAR Objeto - Copiar"

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

- Os controles de consistência do StorageGRID são suportados por todas as operações em objetos, com exceção do seguinte:
  - OBTER ACL Objeto
  - OPTIONS /
  - COLOCAR guarda legal Objeto
  - COLOCAR retenção Objeto
- As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário 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
Objeto DELETE	<p data-bbox="818 155 1481 226">Autenticação multifator (MFA) e o cabeçalho de resposta <code>x-amz-mfa</code> não são suportados.</p> <p data-bbox="818 260 1481 604">Ao processar uma solicitação DE EXCLUSÃO de objetos, 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="818 638 1070 667"><b>Controle de versão</b></p> <p data-bbox="818 701 1481 945">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="844 978 1481 1528" style="list-style-type: none"> <li>• 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>.</li> <li>• Se um objeto for excluído sem o <code>versionId</code> subrecurso 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>.</li> </ul> <p data-bbox="818 1562 1481 1633"><b>Nota:</b> Em certos casos, vários marcadores de exclusão podem existir para um objeto.</p>
Excluir vários objetos	<p data-bbox="818 1680 1481 1751">Autenticação multifator (MFA) e o cabeçalho de resposta <code>x-amz-mfa</code> não são suportados.</p> <p data-bbox="818 1785 1481 1856">Vários objetos podem ser excluídos na mesma mensagem de solicitação.</p>



Operação	Implementação
ELIMINAR marcação Objeto	<p>Usa o <code>tagging</code> subrecurso para remover todas as tags de um objeto. Implementado com todo o comportamento da API REST do Amazon S3.</p> <p><b>Controle de versão</b></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 <code>"MethodNotAllowed"</code> será retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.</p>
Objeto GET	"Objeto GET"
OBTER ACL Objeto	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.
OBTER retenção legal Objeto	"Usando S3 Object Lock"
OBTER retenção de objetos	"Usando S3 Object Lock"
OBTER marcação de objetos	<p>Usa o <code>tagging</code> subrecurso para retornar todas as tags para um objeto. Implementado com todo o comportamento da API REST do Amazon S3</p> <p><b>Controle de versão</b></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 <code>"MethodNotAllowed"</code> será retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.</p>
Objeto HEAD	"Objeto HEAD"
Restauração PÓS-objeto	"Restauração PÓS-objeto"
Objeto PUT	"Objeto PUT"

Operação	Implementação
COLOCAR Objeto - Copiar	"COLOCAR Objeto - Copiar"
COLOCAR guarda legal Objeto	"Usando S3 Object Lock"
COLOCAR retenção Objeto	"Usando S3 Object Lock"

Operação	Implementação
COLOQUE a marcação Objeto	<p>Usa o <code>tagging</code> subrecurso para adicionar um conjunto de tags a um objeto existente. Implementado com todo o comportamento da API REST do Amazon S3</p> <p><b>Atualizações de tags e comportamento de ingestão</b></p> <p>Quando você usa a marcação "COLOCAR objeto" 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><b>Resolução de conflitos</b></p> <p>As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário 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><b>Controle de versão</b></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> será retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.</p>

#### Informações relacionadas

["Controles de consistência"](#)

## Usando S3 Object Lock

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 e, em seguida, especificar as configurações de retenção legal e de retenção para cada versão de objeto adicionada a esse bucket.

O bloqueio de objetos S3 permite especificar configurações no nível do objeto para impedir que objetos sejam excluídos ou substituídos por um período fixo de tempo ou indefinidamente.

O recurso bloqueio de objetos do StorageGRID S3 fornece um modo de retenção único equivalente ao modo de conformidade do Amazon S3. Por padrão, uma versão de objeto protegido não pode ser substituída ou excluída por nenhum usuário. O recurso bloqueio de objetos do StorageGRID S3 não suporta um modo de governança e não permite que usuários com permissões especiais ignorem as configurações de retenção ou excluam objetos protegidos.

### 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. Você pode usar qualquer um destes métodos:

- Crie o bucket usando o Gerenciador do locatário.

#### "Use uma conta de locatário"

- Crie o bucket usando uma solicitação DE COLOCAR balde com o `x-amz-bucket-object-lock_enabled` cabeçalho de solicitação.

#### "Operações em baldes"

Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação do bucket. O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.

Um bucket com S3 Object Lock ativado pode conter uma combinação de objetos com e sem configurações de bloqueio de objeto S3. O StorageGRID não suporta retenção padrão para os objetos nos buckets do bloqueio de objetos do S3, portanto, a operação do bucket Configuração do bloqueio de objetos do PUT não é suportada.

### Determinar se o bloqueio de objeto S3 está ativado para um bucket

Para determinar se o bloqueio de objeto S3 está ativado, use a solicitação DE configuração OBTENHA bloqueio de objeto.

#### "Operações em baldes"

### Criando um objeto com S3 configurações de bloqueio de objeto

Para especificar as configurações de bloqueio de objeto S3 ao adicionar uma versão de objeto a um intervalo que tenha o bloqueio de objeto S3 ativado, emita um Objeto PUT, COLOCAR Objeto - Copiar ou inicie uma solicitação de upload de várias partes. Use os cabeçalhos de solicitação a seguir.



Você deve habilitar o bloqueio de objeto S3 quando criar um bucket. Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação de um intervalo.

- `x-amz-object-lock-mode`, Que deve ser CONFORMIDADE (sensível a maiúsculas e 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 DE Objeto PUT. `Content-MD5` Não é necessário para COLOCAR Objeto - Copiar ou iniciar carregamento Multipart.
- 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 put Object 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 DE GET ou HEAD Object 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*`.
- Uma solicitação DE versão DE EXCLUSÃO de objeto subsequente ou versões de EXCLUSÃO de objetos falhará se for antes da data de retenção ou se uma retenção legal estiver ativada.

### A atualizar as definições de bloqueio de objetos do S3

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:

- `PUT Object legal-hold`

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.

- `PUT Object retention`
  - O valor do modo deve ser CONFORMIDADE (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 retida-até-data existente, você só poderá aumentá-la. O novo valor deve estar no futuro.

## Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Use uma conta de locatário"](#)

["Objeto PUT"](#)

["COLOCAR Objeto - Copiar"](#)

["Inicie o carregamento de várias peças"](#)

["Controle de versão de objetos"](#)

["Guia do usuário do Amazon Simple Storage Service: Usando o bloqueio de objeto S3"](#)

## Usando 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.

## Usando 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:

- Objeto PUT
- COLOCAR Objeto - Copiar
- Inicie o carregamento de várias peças

## Usando 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:

- Objeto GET
- Objeto HEAD
- Objeto PUT
- COLOCAR Objeto - Copiar
- Inicie o carregamento de várias peças
- Carregar artigo
- Carregar artigo - Copiar

## 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 do CloudMirror estiver configurada para o bucket, você não poderá ingerir objetos SSE-C. A operação de ingestão falhará.

## Informações relacionadas

["Objeto GET"](#)

["Objeto HEAD"](#)

["Objeto PUT"](#)

["COLOCAR Objeto - Copiar"](#)

["Inicie o carregamento de várias peças"](#)

["Carregar artigo"](#)

["Carregar artigo - Copiar"](#)

["Guia do desenvolvedor do Amazon S3: Protegendo dados usando criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente \(SSE-C\)"](#)

## Objeto GET

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

### O parâmetro pedido de número de peça não é suportado

O `partNumber` parâmetro Request não é suportado para OBTER solicitações Objeto. Não é possível executar uma SOLICITAÇÃO GET para recuperar uma parte específica de um objeto multipart. Um erro 501 não implementado é retornado com a seguinte mensagem:


```
GET Object by partNumber is not implemented
```



**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 em "usar criptografia do lado do servidor".

**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" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

**Comportamento DO GET Object para objetos Pool de storage de nuvem**

Se um objeto tiver sido armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), o comportamento de uma SOLICITAÇÃO GET Object depende do estado do objeto. Consulte "Objeto PRINCIPAL" 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 DE OBTENÇÃO de objetos tentarão recuperar dados da grade, antes de recuperá-los do pool de armazenamento em nuvem.

Estado do objeto	Comportamento de GET Object
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.

Estado do objeto	Comportamento de GET Object
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 solicitação de restauração PÓS-objeto 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 restauração PÓS-objeto 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 GET Object 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 GET Object pode retornar alguns dados, mas parar no meio da transferência.
- Uma solicitação OBTER Objeto subsequente pode retornar 403 Forbidden.

#### Informações relacionadas

["Usando criptografia do lado do servidor"](#)

["Gerenciar objetos com ILM"](#)

["Restauração PÓS-objeto"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

#### Objeto HEAD

Você pode usar a solicitação de Objeto S3 HEAD 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 Objeto HEAD para determinar o estado de transição do objeto.

## 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`: 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 em "usar criptografia do lado do servidor".

### 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`

### Cabeçalhos de resposta para objetos Pool de armazenamento em nuvem

Se o objeto for armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), 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 objeto PRINCIPAL
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.)

Estado do objeto	Resposta ao objeto PRINCIPAL
Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>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.</p>
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="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>O valor para <code>expiry-date</code> é definido para algum tempo distante no futuro.</p> <p><b>Nota:</b> Se a cópia na grade não estiver disponível (por exemplo, um nó de armazenamento está inativo), você deve emitir uma solicitação de restauração PÓS-Objeto 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: ongoing-request="true"</p>

Estado do objeto	Resposta ao objeto PRINCIPAL
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="false", expiry-date="Sat, 23 July 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 multipart 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 de objeto PRINCIPAL pode retornar incorretamente `x-amz-restore: ongoing-request="false"` 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.

### 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" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

### Informações relacionadas

["Usando criptografia do lado do servidor"](#)

["Gerenciar objetos com ILM"](#)

["Restauração PÓS-objeto"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

### Restauração PÓS-objeto

Você pode usar a solicitação de restauração PÓS-objeto S3 para restaurar um objeto armazenado em um pool de storage de nuvem.

### Tipo de solicitação suportada

O StorageGRID suporta apenas solicitações de restauração PÓS-objeto 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 da restauração PÓS-objeto em objetos do Cloud Storage Pool

Se um objeto tiver sido armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), uma solicitação de restauração PÓS-objeto terá o seguinte comportamento, com base no estado do objeto. Consulte "Objeto PRINCIPAL" 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 será necessário restaurar o objeto emitindo uma solicitação de restauração PÓS-objeto. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma SOLICITAÇÃO GET Object.

Estado do objeto	Comportamento da restauração PÓS-objeto
Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto não está em um pool de storage de nuvem	403 Forbidden, InvalidObjectState
Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável	200 OK Nenhuma alteração é feita.  <b>Nota:</b> Antes de um objeto ser transferido para um estado não recuperável, não é possível alterar o seu expiry-date.
Objeto transicionado para um estado não recuperável	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.  Opcionalmente, use o Tier elemento de solicitação para determinar quanto tempo o trabalho de restauração levará para concluir (Expedited, Standard ou Bulk ). Se você não especificar Tier, o Standard nível será usado.  <b>Atenção:</b> Se um objeto tiver sido transferido para o S3 Glacier Deep Archive ou se o Cloud Storage Pool usar o armazenamento Blob do Azure, não será possível restaurá-lo usando o Expedited nível. O seguinte erro é retornado 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.
Objeto em processo de restauração a partir de um estado não recuperável	409 Conflict, RestoreAlreadyInProgress

Estado do objeto	Comportamento da restauração PÓS-objeto
Objeto totalmente restaurado para o Cloud Storage Pool	200 OK  <b>Observação:</b> se um objeto foi restaurado para um estado recuperável, você pode alterar o mesmo <code>expiry-date</code> reemitindo a solicitação de restauração PÓS-objeto com um novo valor para <code>Days</code> . A data de restauração é atualizada em relação à hora da solicitação.

### Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Objeto HEAD"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

### Objeto PUT

Você pode usar a solicitação de objetos S3D PUT para adicionar um objeto a um bucket.

### Resolução de conflitos

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário 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 StorageGRID suporta objetos de até 5 TB de tamanho.

### 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 PUT, PUT Object-Copy, GET e HEAD 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 as opções balanceadas ou rigorosas para o comportamento de ingestão. 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`

### "Usando S3 Object Lock"

- 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`

### "S3 operações e limitações suportadas pela API REST"

#### 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 que corresponde a um objeto ingerido usar a opção estrita para comportamento 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 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 nós de storage diferentes.

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.

**Atenção:** 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 pela política ILM ativa e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

**Nota:** 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.

**Atenção:** 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 em "usar criptografia do lado do servidor".

**Nota:** Se um objeto for criptografado com SSE ou SSE-C, qualquer configuração de criptografia em nível de bucket ou em nível de grade será ignorada.

### 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.

### Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Operações em baldes"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

["Usando criptografia do lado do servidor"](#)

["Como as conexões do cliente podem ser configuradas"](#)

### COLOCAR Objeto - Copiar

Você pode usar a solicitação S3 PUT Object - Copy para criar uma cópia de um objeto que já está armazenado no S3. Uma operação PUT Object - Copy é a mesma que executar um GET e depois um PUT.

### Resolução de conflitos

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário 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 StorageGRID suporta objetos de até 5 TB de tamanho.

## 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`

## "Usando S3 Object Lock"

- 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`

## "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 especificar um comportamento de ingestão de confirmação dupla ou equilibrada.

- `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 `PUT Object - Copy`

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 COLOCAR Objeto - Copiar para criptografar um objeto existente no lugar ou para alterar a criptografia de um objeto existente no lugar. 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 você usar criptografia no lado do servidor, 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 PUT Object - Copy, para que o objeto possa ser descriptografado e copiado:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` AES256 Especifique .
  - `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.

**Atenção:** 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 em "usar 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 no pedido COLOCAR Objeto - Copiar:
  - `x-amz-server-side-encryption`

**Nota:** 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` então retornará um valor `"null"`.

## Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Usando criptografia do lado do servidor"](#)

["S3 operações rastreadas nos logs de auditoria"](#)

["Objeto PUT"](#)

## Operações para uploads de várias partes

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

- ["Listar carregamentos de várias partes"](#)
- ["Inicie o carregamento de várias peças"](#)
- ["Carregar artigo"](#)
- ["Carregar artigo - Copiar"](#)
- ["Concluir carregamento Multipart"](#)

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

- Você não deve exceder 1.000 uploads simultâneos de várias partes para um único bucket, porque os resultados das consultas de uploads de várias partes para esse bucket podem retornar resultados incompletos.
- O StorageGRID impõe limites de tamanho da AWS para peças multipartes. 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 de peças grandes 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 comportamento de ingestão rigoroso ou equilibrado. 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, quando o upload multipart concluir algumas partes do objeto talvez não atendam aos requisitos atuais do ILM. Qualquer peça que não seja colocada corretamente está na fila para reavaliação ILM e é 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, na ingestão cada parte de 1 GB de um upload multipart de 10 partes é armazenado em DC2. Quando ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.

- Todas as operações de upload em várias partes suportam controles de consistência do StorageGRID.
- Conforme necessário, você pode usar a criptografia do lado do servidor com uploads de várias partes. Para usar o 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 de upload de múltiplas partes. 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 de carregamento de múltiplas partes. Iniciar e em cada solicitação de peça de carregamento subsequente.

Operação	Implementação
Listar carregamentos Multipart	Consulte <a href="#">"Listar carregamentos Multipart"</a>
Inicie o carregamento de várias peças	Consulte <a href="#">"Inicie o carregamento de várias peças"</a>
Carregar artigo	Consulte <a href="#">"Carregar artigo"</a>
Carregar artigo - Copiar	Consulte <a href="#">"Carregar artigo - Copiar"</a>
Concluir carregamento Multipart	Consulte <a href="#">"Concluir carregamento Multipart"</a>
Abortar carregamento Multipart	Implementado com todo o comportamento da API REST do Amazon S3
Listar peças	Implementado com todo o comportamento da API REST do Amazon S3

## Informações relacionadas

["Controles de consistência"](#)

["Usando criptografia do lado do servidor"](#)

## Listar carregamentos Multipart

A operação List Multipart uploads lista uploads em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

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



- `upload-id-marker`

O `delimiter` parâmetro Request não é suportado.

### 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. Quando a operação completa de Upload Multipart é executada, esse é o ponto em que os objetos são criados (e versionados, se aplicável).

### Inicie o carregamento de várias peças

A operação 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 a opção estrita para comportamento 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 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 nós de storage diferentes.

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,

you can lose data if the only copy is initially stored in a storage node that fails before the ILM evaluation can occur.

**Atenção:** 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 pela política ILM ativa e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

**Nota:** 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`

## "Usando S3 Object Lock"

- 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`

## "S3 operações e limitações suportadas pela API REST"



Para obter informações sobre como o StorageGRID lida com caracteres UTF-8, consulte a documentação do PUT Object.

### 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 de carregamento de múltiplas partes se você quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações de Upload Part.
  - `x-amz-server-side-encryption`
- **SSE-C:** Use todos esses três cabeçalhos na solicitação de Upload Multipart iniciada (e em cada solicitação de Upload Part 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.

**Atenção:** 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 em "usar 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 completa de Upload Multipart é executada.

### Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Usando criptografia do lado do servidor"](#)

## "Objeto PUT"

### Carregar artigo

A operação Upload Part carrega uma peça 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 a criptografia SSE-C para a solicitação de carregamento de múltiplas peças iniciada, você também deve incluir os seguintes cabeçalhos de solicitação em cada solicitação de Upload de peça:

- 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 Iniciar carregamento Multipart.
- x-amz-server-side-encryption-customer-key-MD5: Especifique o mesmo resumo MD5 que você forneceu na solicitação de Envio de Multipart Iniciar.



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 em "usar 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 completa de Upload Multipart é executada.

#### Informações relacionadas

["Usando criptografia do lado do servidor"](#)

### Carregar artigo - Copiar

A operação Upload Part - Copy carrega uma parte de um objeto copiando dados de um objeto existente como fonte de dados.

A operação Upload Part - Copy é implementada com todo o comportamento da API REST do Amazon S3.

Essa solicitação lê e grava os dados de objeto especificados no x-amz-copy-source-range sistema StorageGRID.

Os seguintes cabeçalhos de solicitação são suportados:

- x-amz-copy-source-if-match

- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since

### Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação de carregamento de múltiplas partes, você também deve incluir os seguintes cabeçalhos de solicitação em cada peça de carregamento - solicitação de cópia:

- 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 Iniciar carregamento Multipart.
- x-amz-server-side-encryption-customer-key-MD5: Especifique o mesmo resumo MD5 que você forneceu na solicitação de Envio de Multipart Iniciar.

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 de Upload Part - Copy, 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.



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 em "usar 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 completa de Upload Multipart é executada.

### Concluir carregamento Multipart

A operação completa de Upload Multipart completa um upload multipart de um objeto, montando as peças carregadas anteriormente.

### Resolução de conflitos

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O calendário 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 StorageGRID suporta objetos de até 5 TB de tamanho.

## Cabeçalhos de solicitação

O `x-amz-storage-class` cabeçalho de solicitação é suportado e afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM correspondente especificar um comportamento de ingestão de confirmação dupla ou equilibrada.

- 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 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.

## Informações relacionadas

["Gerenciar objetos com ILM"](#)

## 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
AccessDenied	403 proibido
BadDigest	400 pedido incorreto
BucketAlreadyExists	409 conflito
BucketNotEmpty	409 conflito
IncompleteBody	400 pedido incorreto
InternalServerError (erro internacional)	500 erro interno do servidor
InvalidAccessKeyId	403 proibido
InvalidArgument	400 pedido incorreto
InvalidBucketName	400 pedido incorreto
InvalidBucketState	409 conflito
InvalidDigest	400 pedido incorreto

<b>Nome</b>	<b>Status HTTP</b>
InvalidEncryptionAlgorithmError	400 pedido incorreto
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



Nome	Status HTTP
RequestTimeTooSwed	403 proibido
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
XComplianceReducedRedundancy Forbidden	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 da API REST do StorageGRID S3

Há operações adicionadas à API REST do S3 que são específicas do sistema StorageGRID.

## OBTER pedido de consistência de balde

A solicitação GET Bucket Consistency permite determinar o nível de consistência que está sendo aplicado a um determinado bucket.

Os controles de consistência padrão são definidos 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

### Resposta

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

Controle de 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.

Controle de consistência	Descrição
leitura-após-nova-gravação	<p>(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. Corresponde às garantias de consistência do Amazon S3.</p> <p><b>Observação:</b> se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, defina o controle de consistência como "disponível", a menos que você exija garantias de consistência semelhantes ao Amazon S3.</p>
Disponível (eventual consistência para OPERAÇÕES DE CABEÇA)	<p>Comporta-se da mesma forma que o nível de consistência "read-after-novo-write", mas apenas fornece consistência eventual para operações HEAD. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis. Difere das garantias de consistência do Amazon S3 apenas para operações PRINCIPAIS.</p>

### 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

["Controles de consistência"](#)

## COLOCAR pedido consistência balde

A solicitação de consistência do PUT Bucket permite especificar o nível de consistência a ser aplicado às operações realizadas em um bucket.

Os controles de consistência padrão são definidos para garantir leitura após gravação para objetos recém-criados.

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:

Controle de 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	<p>(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. Corresponde às garantias de consistência do Amazon S3.</p> <p><b>Observação:</b> se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, defina o controle de consistência como "disponível", a menos que você exija garantias de consistência semelhantes ao Amazon S3.</p>
Disponível (eventual consistência para OPERAÇÕES DE CABEÇA)	Comporta-se da mesma forma que o nível de consistência "read-after-novo-write", mas apenas fornece consistência eventual para operações HEAD. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis. Difere das garantias de consistência do Amazon S3 apenas para operações PRINCIPAIS.

**Nota:** em geral, você deve usar o valor de controle de 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 o controle de consistência para cada solicitação de API. Defina o controle de consistência no nível do balde apenas como último recurso.

## Exemplo de solicitação

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

## Informações relacionadas

["Controles de consistência"](#)

## OBTER último pedido de 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

## 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>
```

## COLOCAR o último pedido de 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, a caixa de seleção **S3 Buckets Change Last Access Setting** no Gerenciador de locatários ou na API de Gerenciamento do locatário.

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

- **OBTER Objeto**, **OBTER ACL Objeto**, **OBTER marcação Objeto** e solicitações **Objeto HEAD** não atualizam a última hora de acesso. O objeto não é adicionado às filas para avaliação do gerenciamento do ciclo de vida das informações (ILM).
- **COLOCAR Objeto - Copiar e COLOCAR** solicitações de marcação de objetos 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 o último tempo de acesso estiverem desativadas para o intervalo de origem, as solicitações **COLOCAR Objeto - cópia** não atualizam o último tempo 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, **COLOCAR Objeto - solicitações de cópia** sempre atualizam o último tempo de acesso. A cópia do objeto é adicionada às filas para avaliação ILM.
- Concluir a atualização de pedidos de carregamento de várias peças da última vez 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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

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

## Informações relacionadas

["Use uma conta de locatário"](#)

## EXCLUIR solicitação de 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

## OBTER solicitação de 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

### 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 URN de um endpoint StorageGRID.

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



Nome	Descrição	Obrigatório
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"> <li>• es deve ser o terceiro elemento.</li> <li>• A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário <code>domain-name/myindex/mytype</code>.</li> </ul> <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"> <li>• <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code></li> <li>• <code>urn:mysite:es:::mydomain/myindex/mytype</code></li> </ul> <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-
1:33333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

#### Informações relacionadas

["Use uma conta de locatário"](#)

## COLOCAR solicitação de 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
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
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

<b>Nome</b>	<b>Descrição</b>	<b>Obrigatório</b>
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"> <li>• es deve ser o terceiro elemento.</li> <li>• A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário domain-name/myindex/mytype.</li> </ul> <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"> <li>• arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</li> <li>• urn:mysite:es:::mydomain/myindex/mytype</li> </ul> <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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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>
```

### Informações relacionadas

["Use uma conta de locatário"](#)

### 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

**Observação:** 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.

## 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 GET Service 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

### 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

["Controles de consistência"](#)

## 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 automaticamente quando você atualizar para o StorageGRID 11,5. 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.

["Usando S3 Object Lock"](#)

["Gerenciar objetos com ILM"](#)

["Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"](#)

### **Obsoleto: Modificações de solicitação de Bucket 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.



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.

["Usando S3 Object Lock"](#)

["Gerenciar objetos com ILM"](#)

["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 as modificações de solicitação DE armazenamento 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.
```

### **Informações relacionadas**

["Gerenciar objetos com ILM"](#)

["Use uma conta de locatário"](#)

### **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.

["Usando S3 Object Lock"](#)

["Gerenciar objetos com ILM"](#)

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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

#### 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: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
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.

Nome	Descrição
LegalHod	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Falso: Este balde não está atualmente sob um guarda legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.</li> </ul>
Autodelete	<ul style="list-style-type: none"> <li>• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob uma retenção legal.</li> <li>• 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.</li> </ul>

### 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.

### Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Use uma conta de locatário"](#)

### 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.

["Usando S3 Object Lock"](#)

["Gerenciar objetos com ILM"](#)

["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: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
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><b>Atenção:</b> 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. Após o período de retenção do balde ser definido, não é possível diminuir esse valor; só é possível aumentá-lo.</p>
LegalHod	<ul style="list-style-type: none"><li>• 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.</li><li>• Falso: Este balde não está atualmente sob um guarda legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.</li></ul>

Nome	Descrição
Autodelete	<ul style="list-style-type: none"> <li>• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob uma retenção legal.</li> <li>• 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.</li> </ul>

### Nível de 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 o nível de 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 atingir o nível de 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 o nível de consistência **strong-site**.



Nunca force o nível de 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 o nível de consistência é reduzido 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 um nível de consistência inferior, 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 do nível de consistência **strong-site**, reemita 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"](#)

["Use uma conta de locatário"](#)

["Gerenciar objetos com ILM"](#)

# Políticas de acesso ao bucket e ao grupo

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 configuradas usando a política OBTER bucket, COLOCAR bucket e EXCLUIR Bucket policy S3 operações de API. 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.

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 construídas usando esta estrutura para especificar permissões: Conceder efeito para permitir/negar que o principal execute Ação em recurso quando a condição se aplica.

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": "*"
```

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.

#### Informações relacionadas

["Use uma conta de locatário"](#)

## Configurações de controle de consistência para políticas

Por padrão, quaisquer atualizações feitas para políticas de grupo são eventualmente consistentes. Uma vez que 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 também são, eventualmente, 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 se torne efetiva o mais rápido possível por razões de segurança.

Nesse caso, você pode definir o `Consistency-Control` cabeçalho na solicitação de política COLOCAR balde ou usar a solicitação DE consistência COLOCAR balde. Ao alterar o controle de consistência para essa solicitação, você deve usar o valor **All**, que fornece a maior garantia de consistência de leitura após gravação. Se você especificar qualquer outro valor de controle de consistência em um cabeçalho para a solicitação DE consistência de armazenamento PUT, a solicitação será rejeitada. Se você especificar qualquer outro valor para uma solicitação DE política PUT Bucket, o valor será ignorado. Depois que uma política de bucket se tornar consistente, as alterações podem levar mais 8 segundos para entrar em vigor, devido ao armazenamento em cache de políticas.



Se você definir o nível de consistência como **All** para forçar uma nova política de bucket a entrar em vigor mais cedo, certifique-se de definir o controle de nível de bucket de volta ao valor original quando terminar. Caso contrário, todas as futuras solicitações de bucket usarão a configuração **All**.

## Usando o ARN nas 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 de política PUT Bucket deve ser codificado com charset UTF-8.

## Especificando 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.

### Informações relacionadas

["Especificando variáveis em uma política"](#)

## Especificando 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.

## Especificando 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 de replicação `PUT` e `DELETE` Bucket. 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	COLOQUE o balde	
S3>DeleteBucket	ELIMINAR balde	
S3>DeleteBucketMetadataNotification	ELIMINAR configuração de notificação de metadados do bucket	Sim
S3>DeleteBucketPolicy	ELIMINAR política de balde	
S3>DeleteReplicationConfiguration	ELIMINAR replicação de balde	Sim, permissões separadas para COLOCAR e EXCLUIR*
S3:GetBucketAcl	OBTER ACL balde	
S3:GetBucketCompliance	OBTER conformidade com balde (obsoleto)	Sim
S3:GetBucketConsistência	OBTER consistência de balde	Sim
S3:GetBucketCORS	OBTER Bucket Cors	
S3:GetEncryptionConfiguration	OBTER criptografia Bucket	
S3:GetBucketLastAccessTime	OBTER último tempo de acesso do Bucket	Sim
S3:GetBucketLocation	OBTER localização do balde	
S3:GetBucketMetadataNotification	OBTER configuração de notificação de metadados do bucket	Sim
S3:GetBucketNotification	OBTER notificação Bucket	
S3:GetBucketObjectLockConfiguration	OBTER Configuração bloqueio Objeto	
S3:GetBucketPolicy	OBTER política Bucket	
S3:GetBucketTagging	OBTER marcação Bucket	
S3:GetBucketControle de versão	OBTENHA o controle de versão do Bucket	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:GetLifecycleConfiguration	OBTENHA o ciclo de vida do Bucket	
S3:GetReplicationConfiguration	OBTER replicação do bucket	
S3:ListAllMyBuckets	<ul style="list-style-type: none"> <li>• Serviço GET</li> <li>• OBTER uso de armazenamento</li> </ul>	Sim, para OBTER uso de armazenamento
S3: ListBucket	<ul style="list-style-type: none"> <li>• OBTER balde (Listar objetos)</li> <li>• Balde DA cabeça</li> <li>• Restauração PÓS-objeto</li> </ul>	
S3:ListBucketMultipartUploads	<ul style="list-style-type: none"> <li>• Listar carregamentos Multipart</li> <li>• Restauração PÓS-objeto</li> </ul>	
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"> <li>• ELIMINAR Cors Bucket†</li> <li>• COLOQUE cors de balde</li> </ul>	
S3:PutEncryptionConfiguration	<ul style="list-style-type: none"> <li>• ELIMINAR encriptação Bucket</li> <li>• COLOQUE a criptografia Bucket</li> </ul>	
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	COLOCAR notificação de balde	



Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:PutBucketObjectLockConfiguration	COLOCAR balde com o <code>x-amz-bucket-object-lock-enabled: true</code> cabeçalho de pedido (também requer a permissão S3:CreateBucket)	
S3:PutBucketPolicy	Política COLOCAR balde	
S3:PutBucketTagging	<ul style="list-style-type: none"> <li>• ELIMINAR marcação de intervalo†</li> <li>• COLOQUE a marcação de balde</li> </ul>	
S3:PutBucketControle de versão	COLOQUE o controle de versão do Bucket	
S3:PutLifecycleConfiguration	<ul style="list-style-type: none"> <li>• ELIMINAR ciclo de vida do balde†</li> <li>• COLOQUE o ciclo de vida do balde</li> </ul>	
S3:PutReplicationConfiguration	COLOQUE a replicação do balde	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"> <li>• Abortar carregamento Multipart</li> <li>• Restauração PÓS-objeto</li> </ul>	
S3>DeleteObject	<ul style="list-style-type: none"> <li>• Objeto DELETE</li> <li>• Excluir vários objetos</li> <li>• Restauração PÓS-objeto</li> </ul>	
S3>DeleteObjectTagging	ELIMINAR marcação Objeto	
S3>DeleteObjectVersionTagging	EXCLUIR marcação de objetos (uma versão específica do objeto)	
S3>DeleteObjectVersion	DELETE Object (uma versão específica do objeto)	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:GetObject	<ul style="list-style-type: none"> <li>• Objeto GET</li> <li>• Objeto HEAD</li> <li>• Restauração PÓS-objeto</li> </ul>	
S3:GetObjectAcl	OBTER ACL Objeto	
S3:GetObjectLegalHod	OBTER retenção legal Objeto	
S3:GetObjectRetention	OBTER retenção de objetos	
S3:GetObjectTagging	OBTER marcação Objeto	
S3:GetObjectVersionTagging	OBTER marcação de objetos (uma versão específica do objeto)	
S3:GetObjectVersion	OBTER Objeto (uma versão específica do objeto)	
S3:ListMultipartUploadParts	Listar Artigos, PÓS-restauração de objetos	
S3:PutObject	<ul style="list-style-type: none"> <li>• Objeto PUT</li> <li>• COLOCAR Objeto - Copiar</li> <li>• Restauração PÓS-objeto</li> <li>• Inicie o carregamento de várias peças</li> <li>• Concluir carregamento Multipart</li> <li>• Carregar artigo</li> <li>• Carregar artigo - Copiar</li> </ul>	
S3:PutObjectLegalHod	COLOCAR guarda legal Objeto	
S3:retenção de objetos Put	COLOCAR retenção Objeto	
S3:PutObjectTagging	Colocar marcação Objeto	
S3:PutObjectVersionTagging	COLOCAR marcação de objetos (uma versão específica do objeto)	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:PutOverwriteObject	<ul style="list-style-type: none"> <li>• Objeto PUT</li> <li>• COLOCAR Objeto - Copiar</li> <li>• COLOQUE a marcação Objeto</li> <li>• ELIMINAR marcação Objeto</li> <li>• Concluir carregamento Multipart</li> </ul>	Sim
S3:RestoreObject	Restauração PÓS-objeto	

## Usando 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 substituir 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 do S3 estiver ativado, a configuração Negar impede que as operações de marcação DE objetos PUT ou DELETE 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 seleção **Prevent Client Modification** estiver selecionada (**Configuration Grid Options**), essa configuração substituirá a configuração da permissão PutOverwriteObject.

### Informações relacionadas

["S3 exemplos de políticas de grupo"](#)

## Especificando 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: {  
  <em>condition_type</em>: {  
    <em>condition_key</em>: <em>condition_values</em>
```

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.

<b>Operadores de condição</b>	<b>Descrição</b>
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.
NumericGreaterThan	Compara uma chave com um valor numérico baseado na correspondência "maior que".
NumericGreaterThanEquals	Compara uma chave com um valor numérico com base na correspondência "maior que ou igual".
NumericLessThan	Compara uma chave com um valor numérico baseado na correspondência "menos que".
NumericLessThanEquals	Compara uma chave com um valor numérico baseado na correspondência "menor que ou igual".
Bool	Compara uma chave com um valor booleano baseado na correspondência "true or false".
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.

### **Tecclas de condição suportadas**

Categoria	Chaves de condição aplicáveis	Descrição
Operadores IP	AWS:SourceIp	<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><b>Observação:</b> 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><b>Nota:</b> 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, uma vez que sua validade não pode ser determinada.</p>
Recurso/identidade	aws:nome de usuário	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.
S3: ListBucket e. S3:ListBucketVersions Permissions	s3:delimitador	Irá comparar com o parâmetro delimitador especificado em uma solicitação OBTER bucket ou OBTER versões de Objeto bucket.
S3: ListBucket e. S3:ListBucketVersions Permissions	s3: teclas de max	Irá comparar-se com o parâmetro Max-keys especificado em uma solicitação GET Bucket ou GET Bucket Object Versions.
S3: ListBucket e. S3:ListBucketVersions Permissions	s3:prefixo	Irá comparar com o parâmetro de prefixo especificado em uma solicitação GET Bucket ou GET Bucket Object Versions.

## Especificando 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 SourceIp 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.
<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.

## Criação de políticas que exigem manipulação 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.

<b>Descrição da política</b>	<b>Tipo de política</b>	<b>Comportamento da Amazon</b>	<b>Comportamento de StorageGRID</b>
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
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



Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento de StorageGRID
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 **Configuração Opções de Grade** e marque a caixa de seleção **impedir modificação de cliente**.
- 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 PUT Object ALLOW à política S3.



A configuração DeleteObject para NEGAR em uma política 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 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

["Gerenciar objetos com ILM"](#)

["Criação de políticas que exigem manipulação especial"](#)

["Como as regras do StorageGRID ILM gerenciam objetos"](#)

["S3 exemplos de políticas de grupo"](#)

## S3 exemplos de políticas

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

### S3 exemplos de política de bucket

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.

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  
<em>file://policy.json</em>
```

#### Exemplo: Permita que todos acessem somente leitura a um bucket

Neste exemplo, todos, incluindo anônimos, podem listar objetos no bucket e executar operações Get Object em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que essa política pode não ser particularmente útil, já que 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 GET Object 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/*"
    }
  ]
}

```

## Informações relacionadas

["Operações em baldes"](#)

## S3 exemplos de políticas de grupo

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, uma vez que está implícita. As políticas de grupo são configuradas usando o Gerenciador de inquilinos ou a API.



### Exemplo: Definindo a política de grupo usando o Gerenciador do locatário

Ao usar o Gerenciador do Locatário para adicionar ou editar um grupo, você pode selecionar como deseja criar a política de grupo que define quais permissões de acesso S3 membros deste grupo terão, da seguinte forma:

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

Neste exemplo, os membros do grupo só podem listar e acessar sua pasta específica (prefixo de chave) no intervalo especificado.



The screenshot shows the AWS IAM console interface for defining a group policy. On the left, four radio buttons are visible: "No S3 Access", "Read Only Access", "Full Access", and "Custom". The "Custom" option is selected, indicated by a blue dot. Below it, a note says "(Must be a valid JSON formatted string.)". To the right, a large text area contains the following JSON policy:

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

### 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}/*"
    }
  ]
}
```

#### Informações relacionadas

["Use uma conta de locatário"](#)

["Usando a permissão PutOverwriteObject"](#)

["Proteção WORM \(write-once-read-many\)"](#)

## Configurando a segurança para a API REST

Você deve analisar as medidas de segurança implementadas para a API REST e entender como proteger seu sistema.

### Como o StorageGRID fornece segurança para a API REST

Você deve entender como o sistema StorageGRID implementa segurança, autenticação e autorização para a API REST.

O StorageGRID usa as seguintes medidas de segurança.

- As comunicações do cliente com o serviço Load Balancer usam HTTPS se o HTTPS estiver configurado para o ponto de extremidade do balanceador de carga.

Quando você configura um ponto de extremidade do balanceador de carga, o HTTP pode ser habilitado opcionalmente. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

- Por padrão, o StorageGRID usa HTTPS para comunicações de clientes com nós de armazenamento e o serviço CLB em nós de gateway.

O HTTP pode, opcionalmente, ser habilitado para essas conexões. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.



O serviço CLB está obsoleto.

- As comunicações entre o StorageGRID e o cliente são criptografadas usando TLS.
- As comunicações entre o serviço Load Balancer e os nós de armazenamento dentro da grade são criptografadas se o ponto de extremidade do balanceador de carga está configurado para aceitar conexões HTTP ou HTTPS.
- Os clientes devem fornecer cabeçalhos de autenticação HTTP ao StorageGRID para executar operações de API REST.

### Certificados de segurança e aplicativos de cliente

Os clientes podem se conectar ao serviço Load Balancer em nós de gateway ou nós de administrador, diretamente aos nós de storage ou ao serviço CLB em nós de gateway.

Em todos os casos, os aplicativos clientes podem fazer conexões TLS usando um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado gerado pelo sistema StorageGRID:

- Quando os aplicativos cliente se conectam ao serviço do Load Balancer, eles fazem isso usando o certificado que foi configurado para o ponto de extremidade do balanceador de carga específico usado para fazer a conexão. Cada endpoint tem seu próprio certificado, que é um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado que o administrador da grade gerou no StorageGRID ao configurar o endpoint.
- Quando os aplicativos cliente se conectam diretamente a um nó de armazenamento ou ao serviço CLB nos nós de gateway, eles usam os certificados de servidor gerados pelo sistema que foram gerados para nós de armazenamento quando o sistema StorageGRID foi instalado (que são assinados pela autoridade de certificação do sistema) ou um único certificado de servidor personalizado fornecido para a grade por um administrador de grade.

Os clientes devem ser configurados para confiar na autoridade de certificação que assinou qualquer certificado que usam para estabelecer conexões TLS.

Consulte as instruções de administração do StorageGRID para obter informações sobre a configuração de pontos de extremidade do balanceador de carga e para obter instruções sobre como adicionar um único certificado de servidor personalizado para conexões TLS diretamente aos nós de armazenamento ou ao serviço CLB nos nós de gateway.

### Resumo

A tabela a seguir mostra como os problemas de segurança são implementados nas APIs REST S3 e Swift:

Problema de segurança	Implementação da API REST
Segurança da ligação	TLS

Problema de segurança	Implementação da API REST
Autenticação do servidor	Certificado de servidor X,509 assinado pela CA do sistema ou certificado de servidor personalizado fornecido pelo administrador
Autenticação de cliente	<ul style="list-style-type: none"> <li>• S3: Conta S3 (ID da chave de acesso e chave de acesso secreta)</li> <li>• Swift: Conta Swift (nome de usuário e senha)</li> </ul>
Autorização do cliente	<ul style="list-style-type: none"> <li>• S3: Propriedade do bucket e todas as políticas de controle de acesso aplicáveis</li> <li>• Swift: Acesso à função de administrador</li> </ul>

### Informações relacionadas

["Administrar o StorageGRID"](#)

## Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID suporta um conjunto limitado de conjuntos de codificação que os aplicativos clientes podem usar ao estabelecer uma sessão de Segurança da camada de Transporte (TLS).

### Versões suportadas do TLS

O StorageGRID é compatível com TLS 1,2 e TLS 1,3.



SSLv3 e TLS 1,1 (ou versões anteriores) não são mais compatíveis.

### Suítes de cifra suportadas

Versão TLS	IANA nome do conjunto de cifra
1,2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1,2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
1,2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1,3	TLS_AES_256_GCM_SHA384
1,3	TLS_CHACHA20_POLY1305_SHA256
1,3	TLS_AES_128_GCM_SHA256

## Conjuntos de codificação obsoletos

Os seguintes conjuntos de codificação são obsoletos. O suporte para essas cifras será removido em uma versão futura.

Nome IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

### Informações relacionadas

["Como as conexões do cliente podem ser configuradas"](#)

## Operações de monitoramento e auditoria

Você pode monitorar workloads e eficiências das operações do cliente visualizando tendências de transações para toda a grade ou para nós específicos. Você pode usar mensagens de auditoria para monitorar operações e transações do cliente.

- ["Monitoramento de taxas de ingestão e recuperação de objetos"](#)
- ["Acesso e revisão de logs de auditoria"](#)

## Monitoramento de taxas de ingestão e recuperação de objetos

Você pode monitorar taxas de ingestão e recuperação de objetos, bem como métricas para contagens de objetos, consultas e verificação. Você pode exibir o número de tentativas bem-sucedidas e com falha por aplicativos clientes para ler, gravar e modificar objetos no sistema StorageGRID.

### Passos

1. Faça login no Gerenciador de Grade usando um navegador compatível.
2. No painel de instrumentos, localize a seção Protocol Operations (operações de protocolo).

Esta seção resume o número de operações do cliente realizadas pelo seu sistema StorageGRID. As taxas de protocolo são médias nos últimos dois minutos.

3. Selecione **nós**.
4. Na página inicial dos nós (nível de implantação), clique na guia **Load Balancer**.

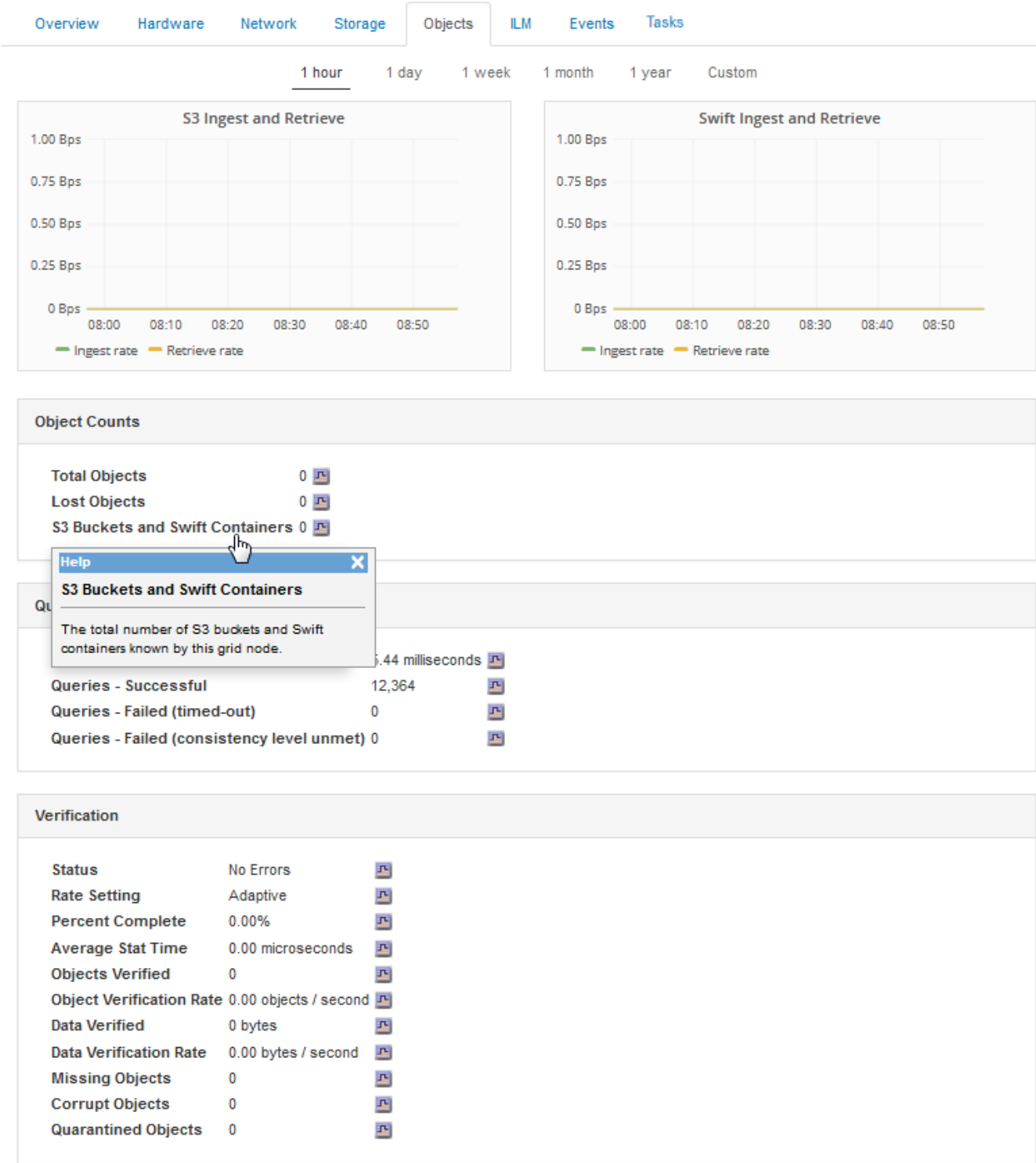
Os gráficos mostram tendências para todo o tráfego do cliente direcionado para pontos de extremidade do balanceador de carga dentro da grade. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

5. Na home page dos nós (nível de implantação), clique na guia **objetos**.

O gráfico mostra as taxas de ingestão e recuperação de todo o seu sistema StorageGRID em bytes por segundo e total de bytes. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

6. Para ver as informações de um nó de armazenamento específico, selecione o nó na lista à esquerda e clique na guia **Objects**.
- O gráfico mostra as taxas de ingestão e recuperação de objetos para este nó de armazenamento. A guia também inclui métricas para contagens de objetos, consultas e verificação. Você pode clicar nos rótulos para ver as definições dessas métricas.

DC1-S2 (Storage Node)



7. Se você quiser ainda mais detalhes:

- a. Selecione **Support > Tools > Grid Topology**.
- b. Selecione **site Visão geral Principal**.

A seção operações da API exibe informações resumidas para toda a grade.

- c. Selecione **Storage Node LDR client Application Overview Main**

A seção operações exibe informações resumidas para o nó de armazenamento selecionado.

## Acesso e revisão de logs de auditoria

As mensagens de auditoria são geradas pelos serviços do StorageGRID e armazenadas em arquivos de log de texto. As mensagens de auditoria específicas da API nos logs de auditoria fornecem dados críticos de monitoramento de segurança, operação e desempenho que podem ajudá-lo a avaliar a integridade do sistema.

### O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

### Sobre esta tarefa

O arquivo de log de auditoria ativo é `audit.log` chamado , e é armazenado em nós de administração.

Uma vez por dia, o arquivo `audit.log` ativo é salvo e um novo `audit.log` arquivo é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato `yyyy-mm-dd.txt`.

Após um dia, o arquivo salvo é compactado e renomeado, no formato `yyyy-mm-dd.txt.gz`, que preserva a data original.

Este exemplo mostra o `audit.log` ficheiro ativo, o ficheiro do dia anterior (`2018-04-15.txt`) e o ficheiro comprimido para o dia anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

### Passos

1. Faça login em um nó Admin:
  - a. Digite o seguinte comando `ssh admin@primary_Admin_Node_IP`
  - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Vá para o diretório que contém os arquivos de log de auditoria:

```
cd /var/local/audit/export
```
3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.



### **S3 operações rastreadas nos logs de auditoria**

Várias operações de bucket e operações de objetos são rastreadas nos logs de auditoria do StorageGRID.

#### **Operações de bucket rastreadas nos logs de auditoria**

- ELIMINAR balde
- ELIMINAR marcação de intervalo
- Excluir vários objetos
- OBTER balde (Listar objetos)
- OBTER versões Objeto balde
- OBTER marcação Bucket
- Balde DA cabeça
- COLOQUE o balde
- COLOQUE a conformidade do balde
- COLOQUE a marcação de balde
- COLOQUE o controle de versão do Bucket

#### **Operações de objeto rastreadas nos logs de auditoria**

- Concluir carregamento Multipart
- Carregar artigo (quando a regra ILM usa os comportamentos de ingestão rigorosos ou equilibrados)
- Carregar artigo - Copiar (quando a regra ILM usa os comportamentos de ingestão estritos ou equilibrados)
- Objeto DELETE
- Objeto GET
- Objeto HEAD
- Restauração PÓS-objeto
- Objeto PUT
- COLOCAR Objeto - Copiar

#### **Informações relacionadas**

["Operações em baldes"](#)

["Operações em objetos"](#)

## **Benefícios de conexões HTTP ativas, ociosas e simultâneas**

Como configurar conexões HTTP pode afetar o desempenho do sistema StorageGRID. As configurações diferem dependendo se a conexão HTTP está ativa ou inativa ou se você tem várias conexões simultâneas.

Você pode identificar os benefícios de desempenho para os seguintes tipos de conexões HTTP:

- Conexões HTTP ociosas
- Conexões HTTP ativas
- Conexões HTTP simultâneas

#### Informações relacionadas

- ["Benefícios de manter conexões HTTP ociosas abertas"](#)
- ["Benefícios de conexões HTTP ativas"](#)
- ["Benefícios de conexões HTTP simultâneas"](#)
- ["Separação de pools de conexão HTTP para operações de leitura e gravação"](#)

## Benefícios de manter conexões HTTP ociosas abertas

Você deve manter as conexões HTTP abertas mesmo quando os aplicativos cliente estiverem ociosos para permitir que os aplicativos cliente executem transações subsequentes pela conexão aberta. Com base nas medições do sistema e na experiência de integração, você deve manter uma conexão HTTP inativa aberta por um máximo de 10 minutos. O StorageGRID pode fechar automaticamente uma conexão HTTP que é mantida aberta e inativa por mais de 10 minutos.

Conexões HTTP abertas e ociosas fornecem os seguintes benefícios:

- Latência reduzida desde o tempo em que o sistema StorageGRID determina que ele tem que executar uma transação HTTP para o tempo em que o sistema StorageGRID pode executar a transação

A latência reduzida é a principal vantagem, especialmente pelo tempo necessário para estabelecer conexões TCP/IP e TLS.

- Aumento da taxa de transferência de dados por priming do algoritmo de início lento TCP/IP com transferências realizadas anteriormente
- Notificação instantânea de várias classes de condições de falha que interrompem a conectividade entre o aplicativo cliente e o sistema StorageGRID

Determinar por quanto tempo manter uma conexão inativa aberta é uma troca entre os benefícios do início lento que está associado à conexão existente e à alocação ideal da conexão com os recursos internos do sistema.

## Benefícios de conexões HTTP ativas

Para conexões diretamente aos nós de armazenamento ou ao serviço CLB (obsoleto) em nós de Gateway, você deve limitar a duração de uma conexão HTTP ativa a um máximo de 10 minutos, mesmo que a conexão HTTP realize transações continuamente.

Determinar a duração máxima em que uma conexão deve ser mantida aberta é um trade-off entre os benefícios da persistência da conexão e a alocação ideal da conexão aos recursos internos do sistema.

Para conexões de cliente a nós de armazenamento ou ao serviço CLB, limitar conexões HTTP ativas fornece os seguintes benefícios:

- Permite o balanceamento de carga ideal em todo o sistema StorageGRID.

Ao usar o serviço CLB, você deve evitar conexões TCP/IP de longa duração para otimizar o balanceamento de carga em todo o sistema StorageGRID. Você deve configurar aplicativos cliente para controlar a duração de cada conexão HTTP e fechar a conexão HTTP após um tempo definido para que a conexão HTTP possa ser restabelecida e reequilibrada.

O serviço CLB equilibra a carga em todo o sistema StorageGRID no momento em que um aplicativo cliente estabelece uma conexão HTTP. Ao longo do tempo, uma conexão HTTP pode não ser mais ótima, pois os requisitos de balanceamento de carga mudam. O sistema executa seu melhor balanceamento de carga quando os aplicativos clientes estabelecem uma conexão HTTP separada para cada transação, mas isso nega os ganhos muito mais valiosos associados às conexões persistentes.



O serviço CLB está obsoleto.

- Permite que aplicativos cliente direcionem transações HTTP para serviços LDR que têm espaço disponível.
- Permite iniciar os procedimentos de manutenção.

Alguns procedimentos de manutenção começam somente depois que todas as conexões HTTP em andamento estiverem concluídas.

Para conexões de clientes ao serviço Load Balancer, limitar a duração das conexões abertas pode ser útil para permitir que alguns procedimentos de manutenção sejam iniciados prontamente. Se a duração das conexões do cliente não for limitada, pode levar vários minutos para que as conexões ativas sejam automaticamente encerradas.

## Benefícios de conexões HTTP simultâneas

Você deve manter várias conexões TCP/IP ao sistema StorageGRID abertas para permitir paralelismo, o que aumenta o desempenho. O número ideal de conexões paralelas depende de uma variedade de fatores.

As conexões HTTP simultâneas oferecem os seguintes benefícios:

- Latência reduzida

As transações podem começar imediatamente em vez de esperar que outras transações sejam concluídas.

- Maior taxa de transferência

O sistema StorageGRID pode executar transações paralelas e aumentar a taxa de transferência de transações agregadas.

Os aplicativos clientes devem estabelecer várias conexões HTTP. Quando um aplicativo cliente tem que executar uma transação, ele pode selecionar e usar imediatamente qualquer conexão estabelecida que não esteja processando uma transação no momento.

A topologia de cada sistema StorageGRID tem um throughput de pico diferente para transações e conexões simultâneas antes que o desempenho comece a degradar. A taxa de transferência de pico depende de fatores como recursos de computação, recursos de rede, recursos de armazenamento e links WAN. O número de servidores e serviços e o número de aplicativos suportados pelo sistema StorageGRID também são fatores.

Os sistemas StorageGRID geralmente suportam vários aplicativos clientes. Você deve ter isso em mente quando determinar o número máximo de conexões simultâneas usadas por um aplicativo cliente. Se o aplicativo cliente consistir em várias entidades de software que estabelecem conexões com o sistema StorageGRID, você deve adicionar todas as conexões entre as entidades. Talvez seja necessário ajustar o número máximo de conexões simultâneas nas seguintes situações:

- A topologia do sistema StorageGRID afeta o número máximo de transações simultâneas e conexões que o sistema pode suportar.
- Os aplicativos clientes que interagem com o sistema StorageGRID em uma rede com largura de banda limitada podem ter que reduzir o grau de simultaneidade para garantir que as transações individuais sejam concluídas em um tempo razoável.
- Quando muitos aplicativos clientes compartilham o sistema StorageGRID, você pode ter que reduzir o grau de simultaneidade para evitar exceder os limites do sistema.

## **Separação de pools de conexão HTTP para operações de leitura e gravação**

Você pode usar pools separados de conexões HTTP para operações de leitura e gravação e controlar quanto de um pool usar para cada um. Pools separados de conexões HTTP permitem que você controle melhor as transações e equilibre as cargas.

Os aplicativos clientes podem criar cargas que são retrieve-dominant (read) ou store-dominant (write). Com pools separados de conexões HTTP para transações de leitura e gravação, você pode ajustar quanto de cada pool a dedicar para transações de leitura ou gravação.

## **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 SOBRESSAIENTES; 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.