# Use o StorageGRID

## StorageGRID software

NetApp
July 23, 2026

# Índice

# Use StorageGRID tenants e clientes

## Use uma conta de tenant

### Use uma conta de locatário do StorageGRID

Uma conta de locatário permite que você use a API REST do Simple Storage Service (S3) para armazenar e recuperar objetos em um sistema StorageGRID.

#### O que é uma conta de tenant?

Cada conta de locatário possui seus próprios grupos federados ou locais, usuários, buckets S3 e objetos.

As contas de locatário podem ser usadas para segregar objetos armazenados por diferentes entidades. Por exemplo, várias contas de locatário podem ser usadas para qualquer um destes casos de uso:

- **Caso de uso empresarial:** Se o sistema StorageGRID estiver sendo usado em uma empresa, o storage de objetos pode ser segregado pelos diferentes departamentos da organização. Por exemplo, pode haver contas de locatário para o departamento de Marketing, o departamento de Suporte ao Cliente, o departamento de Recursos Humanos e assim por diante.

  > Se você usa o protocolo de cliente S3, também pode usar buckets e políticas de bucket do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa criar contas de locatário separadas. Veja as instruções para implementar "Buckets S3 e políticas de bucket" para mais informações.

- **Caso de uso do provedor de serviços:** Se o sistema StorageGRID estiver sendo usado por um provedor de serviços, o storage de objetos do grid pode ser segregado pelas diferentes entidades que alugam o armazenamento. Por exemplo, pode haver contas de locatário para Company A, Company B, Company C e assim por diante.

#### Como criar uma conta de locatário

As contas de locatário são criadas por um "Administrador de grid StorageGRID usando o Gerenciador de Grid". Ao criar uma conta de locatário, o administrador da grade especifica o seguinte:

- Informações básicas, incluindo o nome do locatário, o tipo de cliente (S3) e a cota de armazenamento opcional.
- Permissões para a conta do locatário, como se a conta do locatário pode usar serviços de plataforma S3, configurar sua própria fonte de identidade, usar S3 Select ou usar uma conexão de federação de grid.
- O acesso inicial à raiz para o locatário, dependendo se o sistema StorageGRID usa grupos e usuários locais, federação de identidade ou logon único (SSO).

Além disso, os administradores do grid podem habilitar a configuração de S3 Object Lock para o sistema StorageGRID caso as contas de locatário do S3 precisem estar em conformidade com requisitos regulatórios. Quando o S3 Object Lock está habilitado, todas as contas de locatário do S3 podem criar e gerenciar buckets em conformidade.

##### Configurar locatários do S3

Após uma "A conta de locatário S3 é criada", você pode acessar o Tenant Manager para realizar tarefas como

as seguintes:

- Configure a federação de identidades (a menos que a fonte de identidade seja compartilhada com o grid)
- Gerenciar grupos e usuários
- Use a federação de grids para clonagem de contas e replicação entre grids
- Gerenciar chaves de acesso S3
- Criar e gerenciar buckets S3
- Use os serviços da plataforma S3
- Use o S3 Select
- Monitorar o uso de armazenamento

Embora seja possível criar e gerenciar buckets do S3 com o Tenant Manager, você deve usar um "Cliente S3" ou "Console S3" para ingerir e gerenciar objetos.

## Como iniciar sessão e terminar sessão

### Faça login no StorageGRID Tenant Manager

Você acessa o Gerenciador de Inquilinos inserindo a URL do inquilino na barra de endereços de um "navegador web compatível" navegador.

**Antes de começar**

- Você já possui suas credenciais de login.
- Você tem um URL para acessar o Tenant Manager, fornecido pelo administrador do seu grid. O URL será semelhante a um destes exemplos:

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

  https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

  https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
  ```

  A URL sempre inclui um domínio totalmente qualificado (FQDN), o endereço IP de um nó Admin ou o endereço IP virtual de um grupo HA de nós Admin. Também pode incluir um número de porta, o ID da conta do tenant de 20 dígitos ou ambos.

- Se a URL não incluir o ID de conta de 20 dígitos do locatário, você já possui esse ID de conta.
- Você está usando um "navegador web compatível".
- Os cookies estão ativados no seu navegador.
- Você pertence a um grupo de usuários que possui "permissões de acesso específicas".

**Passos**

1. Inicie um "navegador web compatível".
2. Na barra de endereços do navegador, digite a URL para acessar o Tenant Manager.

3. Se você receber um alerta de segurança, instale o certificado usando o assistente de instalação do navegador.
4. Faça login no Tenant Manager.

   A tela de login que aparece depende da URL inserida e se o single sign-on (SSO) foi configurado para StorageGRID.

   **Não usar SSO**

   Se StorageGRID não estiver usando SSO, uma das seguintes telas aparece:

   - Página de login do Grid Manager. Selecione o link **Tenant sign-in**.
   - Página de login do Tenant Manager. O campo **Account** pode já estar preenchido.
     i. Se o ID da conta do locatário de 20 dígitos não for exibido, selecione o nome da conta do locatário se ele aparecer na lista de contas recentes ou insira o ID da conta.
     ii. Digite seu nome de usuário e senha.
     iii. Selecione **Sign in**.

     O painel de controle do Tenant Manager é exibido.

     iv. Se você recebeu uma senha inicial de outra pessoa, selecione ***username*** > **Alterar senha** para proteger sua conta.

   **Utilizando SSO**

   Se StorageGRID estiver usando SSO, uma das seguintes telas é exibida:

   - Página de SSO da sua organização.

     Insira suas credenciais padrão de SSO e selecione **Entrar**.

   - A página de login SSO do Tenant Manager.
     i. Se o ID da conta do locatário de 20 dígitos não for exibido, selecione o nome da conta do locatário se ele aparecer na lista de contas recentes ou insira o ID da conta.
     ii. Selecione **Sign in**.
     iii. Faça login com suas credenciais SSO padrão na página de login SSO da sua organização.

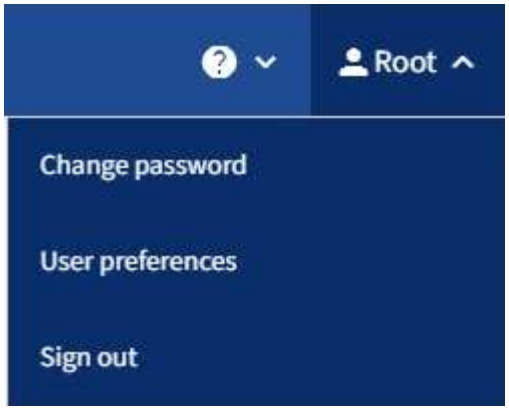
     O painel de controle do Tenant Manager é exibido.

### Saia do StorageGRID Tenant Manager

Ao terminar de usar o Tenant Manager, você deve sair para garantir que usuários não autorizados não possam acessar o StorageGRID. Fechar o navegador pode não encerrar sua sessão no sistema, dependendo das configurações de cookies do navegador.

**Passos**

1. Localize o menu suspenso de nome de usuário no canto superior direito da interface de usuário.




2. Selecione o nome de usuário e, em seguida, selecione **Sair**.

   - Se o SSO não estiver em uso:

     Você foi desconectado do nó de administração. A página de login do Tenant Manager é exibida.

     Se você tiver feito login em mais de um nó de administração, deverá sair de cada nó.

   - Se o SSO estiver ativado:

     Você foi desconectado de todos os nós de administração que estava acessando. A página de login do StorageGRID é exibida. O nome da conta do tenant que você acabou de acessar é listado como padrão na lista suspensa **Contas recentes**, e o **ID da conta** do tenant é exibido.

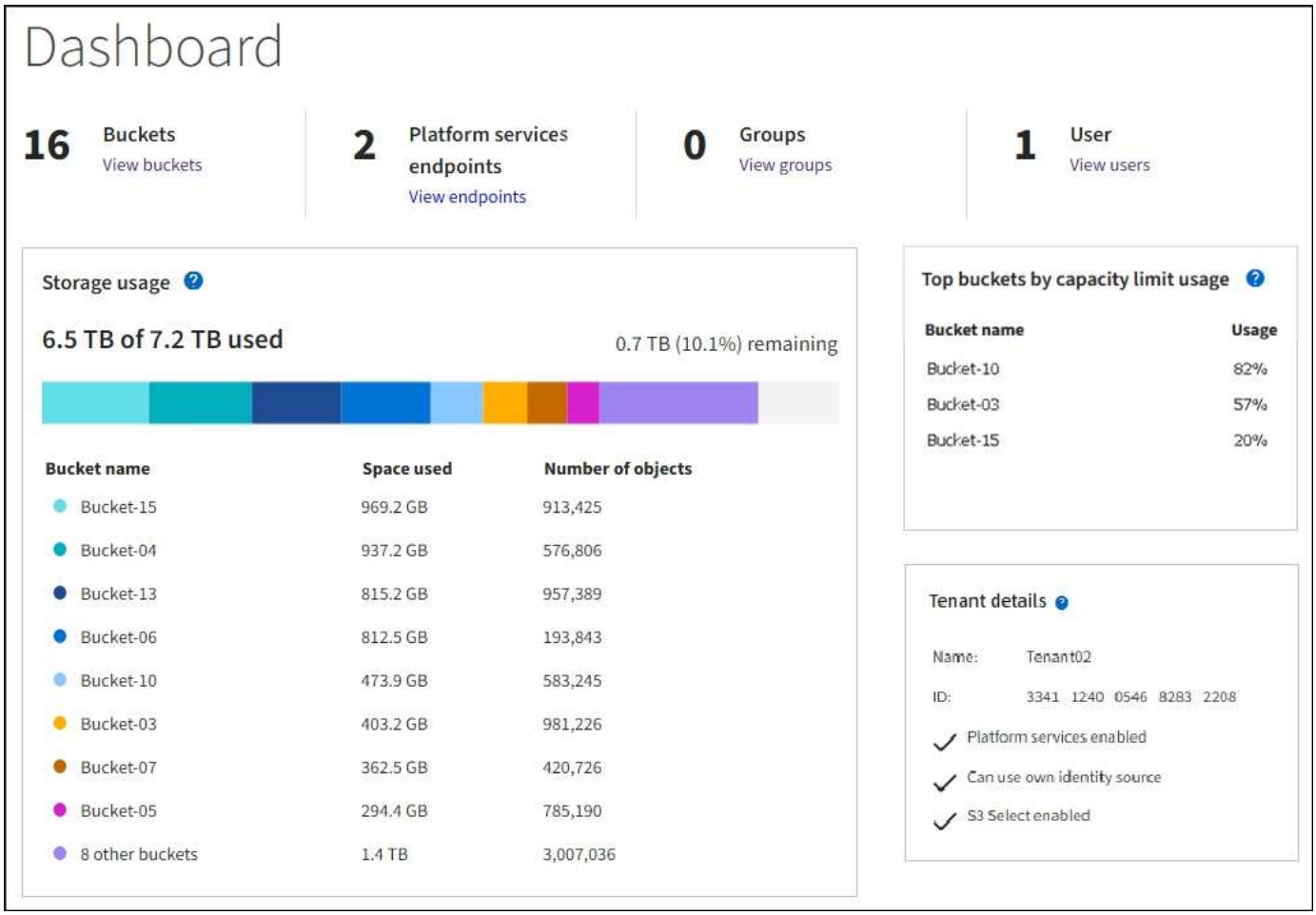
Se o SSO estiver ativado e você também estiver conectado ao Grid Manager, você deve sair do Grid Manager para sair do SSO.

## Painel de controle do Tenant Manager no StorageGRID

O painel do Tenant Manager fornece uma visão geral da configuração da conta do tenant e da quantidade de espaço usada pelos objetos nos buckets S3 do tenant. Se o tenant tiver uma cota, o painel mostra quanto da cota está sendo usada e quanto resta. Se houver algum erro relacionado à conta do tenant, os erros são exibidos no painel.

O tamanho lógico de todos os objetos pertencentes a este locatário inclui uploads multipartes incompletos e em andamento. O tamanho não inclui espaço físico adicional usado para políticas de ILM. Os valores de espaço usado são estimativas. Essas estimativas são afetadas pelo momento das ingestões, conectividade de rede e status do nó.

Quando os objetos tiverem sido carregados, o painel de controle ficará semelhante ao exemplo a seguir:




### Informações da conta do tenant

A parte superior do painel exibe o número de buckets ou contêineres, grupos e usuários configurados. Também exibe o número de endpoints de serviços da plataforma, caso algum tenha sido configurado. Selecione os links para visualizar os detalhes.

Dependendo do "permissões de gerenciamento de locatários" que você possui e das opções que configurou, o restante do painel exibe várias combinações de diretrizes, uso de armazenamento, informações de objetos e detalhes do locatário.

### Uso de armazenamento e cotas

O painel de utilização de armazenamento contém as seguintes informações:

- A quantidade de dados de objetos para o locatário.

  Este valor indica a quantidade total de dados de objetos carregados e não representa o espaço usado para armazenar cópias desses objetos e seus metadados.

- Se uma cota for definida, ela representa a quantidade total de espaço disponível para dados de objetos e a quantidade e porcentagem de espaço restante. A cota limita a quantidade de dados de objetos que podem ser ingeridos.

O uso da cota é baseado em estimativas internas e pode ser excedido em alguns casos. Por exemplo, StorageGRID verifica a cota quando um locatário inicia o upload de objetos e rejeita novas ingestões se o locatário tiver excedido a cota. No entanto, StorageGRID não leva em consideração o tamanho do upload atual ao determinar se a cota foi excedida. Se objetos forem excluídos, um locatário pode ser impedido temporariamente de fazer upload de novos objetos até que o uso da cota seja recalculado. Os cálculos de uso da cota podem levar 10 minutos ou mais.

- Um gráfico de barras que representa os tamanhos relativos dos maiores buckets ou containers.

  Você pode posicionar o cursor sobre qualquer um dos segmentos do gráfico para visualizar o espaço total ocupado por esse bucket ou contêiner.


- Para complementar o gráfico de barras, uma lista dos maiores buckets ou contêineres, incluindo a quantidade total de dados de objetos e o número de objetos em cada bucket ou contêiner.

| Bucket name | Space used | Number of objects |
|---|---|---|
| Bucket-02 | 944.7 GB | 7,575 |
| Bucket-09 | 899.6 GB | 589,677 |
| Bucket-15 | 889.6 GB | 623,542 |
| Bucket-06 | 846.4 GB | 648,619 |
| Bucket-07 | 730.8 GB | 808,655 |
| Bucket-04 | 700.8 GB | 420,493 |
| Bucket-11 | 663.5 GB | 993,729 |
| Bucket-03 | 656.9 GB | 379,329 |
| 9 other buckets | 2.3 TB | 5,171,588 |

  Se o inquilino tiver mais de nove buckets ou containers, todos os outros buckets ou containers serão combinados em uma única entrada na parte inferior da lista.

Para alterar as unidades dos valores de armazenamento exibidos no Gerenciador de Locatários, selecione o menu suspenso do usuário no canto superior direito do Gerenciador de Locatários e, em seguida, selecione **Preferências do usuário**.

### Alertas de uso de quota

Se os alertas de uso de cota estiverem ativados no Grid Manager, esses alertas aparecerão no Tenant Manager quando a cota estiver baixa ou excedida, da seguinte forma:

- Se 90% ou mais da quota de um inquilino tiver sido utilizada, o alerta **Uso elevado da quota do inquilino** será acionado.

  Considere solicitar ao administrador da sua grid um aumento de cota.

- Se você exceder sua cota, uma notificação informa que você não pode enviar novos objetos.

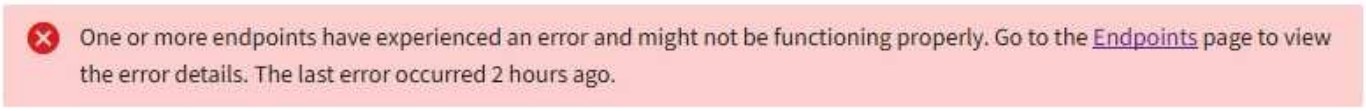
#### Uso do limite de capacidade

Se você definiu um limite de capacidade para seus buckets, o painel do Tenant Manager exibe uma lista dos principais buckets por uso do limite de capacidade.

Se nenhum limite for definido para um bucket, sua capacidade será ilimitada. No entanto, se sua conta de locatário tiver uma cota de armazenamento total e essa cota for atingida, você não poderá ingerir mais objetos independentemente do limite de capacidade restante no bucket.

#### Erros de endpoint

Se você utilizou o Grid Manager para configurar um ou mais endpoints para uso com serviços da plataforma, o painel do Tenant Manager exibe um alerta caso ocorram erros em qualquer endpoint nos últimos sete dias.




Para ver detalhes sobre "erros de endpoint de serviços de plataforma", selecione **Endpoints** para exibir a página Endpoints.

## API de gerenciamento de inquilinos

#### Saiba mais sobre a StorageGRID Tenant Management API

Você pode executar tarefas de gerenciamento do sistema usando a API REST de gerenciamento do locatário em vez da interface de usuário do Tenant Manager. Por exemplo, você pode querer usar a API para automatizar operações ou criar várias entidades, como usuários, mais rapidamente.

A Tenant Management API:

- Utiliza a plataforma de API de código aberto Swagger. O Swagger oferece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores interajam com a API. A interface de usuário do Swagger fornece detalhes completos e documentação para cada operação da API.
- Usa "versionamento para suportar atualizações não disruptivas".

Para acessar a documentação Swagger da Tenant Management API:

1. Faça login no Tenant Manager.
2. Na parte superior do Tenant Manager, selecione o ícone de ajuda e selecione **API documentation**.

##### Operações de API

A Tenant Management API organiza as operações de API disponíveis nas seguintes seções:

- **conta**: Operações na conta do locatário atual, incluindo obter informações sobre o uso do armazenamento.
- **auth**: Operações para realizar autenticação de sessão do usuário.

  A API de Gerenciamento de Inquilinos oferece suporte ao esquema de autenticação Bearer Token. Para um login de inquilino, você fornece um nome de usuário, senha e accountId no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com sucesso, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho das solicitações de API subsequentes ("Authorization: Bearer token").

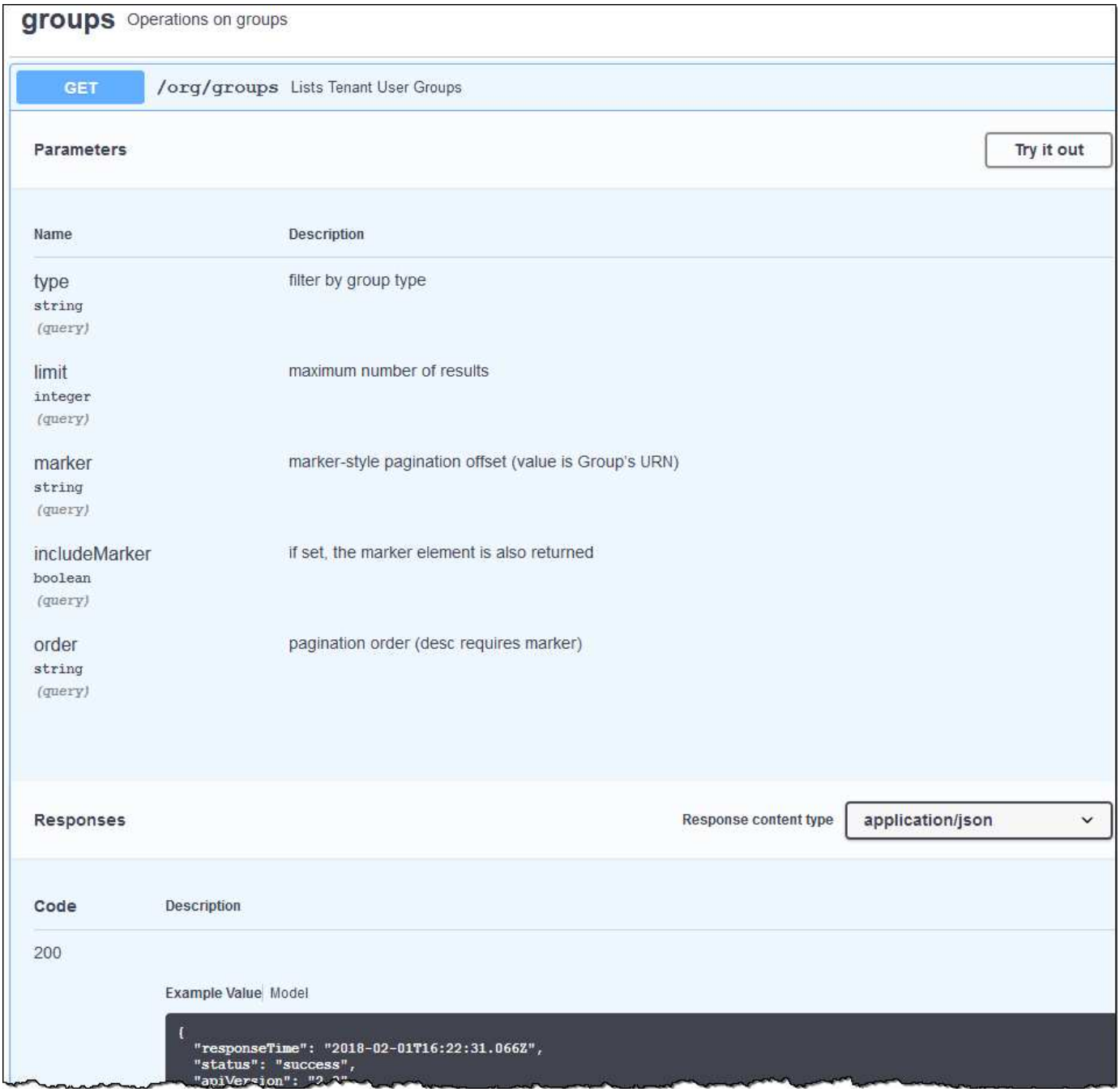
  Para obter informações sobre como melhorar a segurança de autenticação, consulte "Proteja contra falsificação de solicitação entre sites".

  > Se o login único (SSO) estiver habilitado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Consulte o "Instruções para usar a API de Gerenciamento de Grid".

- **config**: Operações relacionadas ao lançamento do produto e às versões da API de Tenant Management. Você pode listar a versão de lançamento do produto e as principais versões da API compatíveis com esse lançamento.
- **containers**: Operações em buckets S3.
- **recursos-desativados**: operações para visualizar recursos que podem ter sido desativados.
- **endpoints**: Operações para gerenciar um endpoint. Os endpoints permitem que um bucket do S3 utilize um serviço externo para StorageGRID CloudMirror replicação, notificações ou integração de pesquisa.
- **grid-federation-connections**: Operações em conexões de federação de grids e replicação entre grids.
- **grupos**: Operações para gerenciar grupos de locatários locais e recuperar grupos de locatários federados de uma fonte de identidade externa.
- **identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo e usuário federados.
- **ilm**: Operações nas configurações de gerenciamento do ciclo de vida das informações (ILM).
- **regiões**: Operações para determinar quais regiões foram configuradas para o sistema StorageGRID.
- **s3**: Operações para gerenciar chaves de acesso S3 para usuários locatários.
- **s3-object-lock**: Operações nas configurações globais de bloqueio de objetos do S3, usadas para dar suporte à conformidade regulamentar.
- **usuários**: Operações para visualizar e gerenciar usuários do locatário.

#### Detalhes da operação

Ao expandir cada operação da API, você pode ver sua ação HTTP, endpoint URL, uma lista de quaisquer parâmetros obrigatórios ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as possíveis respostas.




**Emitir solicitações de API**

> Qualquer operação de API realizada por meio da página de documentação da API é uma operação em tempo real. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

**Passos**

1. Selecione a ação HTTP para ver os detalhes da solicitação.
2. Determine se a solicitação requer parâmetros adicionais, como um ID de grupo ou de usuário. Em seguida, obtenha esses valores. Pode ser necessário fazer uma solicitação de API diferente primeiro para obter as informações de que você precisa.
3. Determine se você precisa modificar o corpo da solicitação de exemplo. Caso precise, selecione **Model** para conhecer os requisitos de cada campo.

4. Selecione **Experimentar**.
5. Forneça todos os parâmetros necessários ou modifique o corpo da solicitação conforme necessário.
6. Selecione **Executar**.
7. Analise o código de resposta para determinar se a solicitação foi bem-sucedida.

#### StorageGRID Versionamento da API de gerenciamento de locatários do StorageGRID

A API de Gerenciamento de Inquilinos utiliza controle de versão para oferecer suporte a atualizações não disruptivas.

Por exemplo, esta URL de solicitação especifica a versão 4 da API.

`https://hostname_or_ip_address/api/v4/authorize`

A versão principal da API é atualizada quando são feitas alterações que *não são compatíveis* com versões anteriores. A versão secundária da API é atualizada quando são feitas alterações que *são compatíveis* com versões anteriores. Alterações compatíveis incluem a adição de novos endpoints ou novas propriedades.

O exemplo a seguir ilustra como a versão da API é atualizada com base no tipo de alterações realizadas.

| Tipo de alteração na API | Versão antiga | Nova versão |
|---|---|---|
| Compatível com versões anteriores | 2,1 | 2,2 |
| Não é compatível com versões antigas | 2,1 | 3,0 |

Ao instalar o software StorageGRID pela primeira vez, apenas a versão mais recente da API é habilitada. No entanto, ao atualizar para uma nova versão de recursos do StorageGRID, você continua tendo acesso à versão anterior da API por pelo menos uma versão de recursos do StorageGRID.

> Você pode configurar as versões suportadas. Consulte a seção **config** da documentação da API Swagger para o "API de gerenciamento de grid" para mais informações. Você deve desativar o suporte para a versão antiga após atualizar todos os clientes da API para usar a versão mais recente.

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho da resposta é "Deprecated: true"
- O corpo da resposta JSON inclui "deprecated": true
- Um aviso de descontinuação é adicionado ao nms.log. Por exemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

##### Determine quais versões da API são compatíveis na versão atual

Use a solicitação `GET /versions` à API para retornar uma lista das versões principais da API suportadas. Essa solicitação está localizada na seção **config** da documentação da API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

#### Especifique uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v4`) ou um cabeçalho (`Api-Version: 4`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

### Proteja contra falsificação de solicitação entre sites (CSRF) no StorageGRID

Você pode ajudar a proteger contra ataques de Cross-Site Request Forgery (CSRF) ao StorageGRID usando tokens CSRF para aprimorar a autenticação que utiliza cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes da API podem escolher se desejam habilitá-lo ao fazer login.

Um atacante capaz de enviar uma solicitação para um site diferente (como por meio de um formulário HTTP POST) pode fazer com que determinadas solicitações sejam realizadas usando os cookies do usuário autenticado.

StorageGRID ajuda a proteger contra ataques CSRF usando tokens CSRF. Quando ativado, o conteúdo de um cookie específico deve corresponder ao conteúdo de um cabeçalho específico ou de um parâmetro específico no corpo de uma POST.

Para ativar o recurso, defina o `csrfToken`parâmetro como `true` durante a autenticação. O padrão é `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando verdadeiro, um cookie `GridCsrfToken` é definido com um valor aleatório para autenticações no Grid Manager, e o cookie `AccountCsrfToken` é definido com um valor aleatório para autenticações no Tenant Manager.

Se o cookie estiver presente, todas as solicitações que podem modificar o estado do sistema (POST, PUT, PATCH, DELETE) devem incluir um dos seguintes:

- O `X-Csrf-Token`cabeçalho, com o valor do cabeçalho definido como o valor do cookie do token CSRF.
- Para endpoints que aceitam um corpo codificado em formulário: um `csrfToken`parâmetro de corpo de requisição codificado em formulário.

Para configurar a proteção CSRF, use o "API de gerenciamento de grid" ou "API de gerenciamento de inquilinos".

> ⓘ As solicitações que possuem um cookie de token CSRF definido também imporão o cabeçalho "Content-Type: application/json" para qualquer solicitação que espere um corpo de solicitação JSON como proteção adicional contra ataques CSRF.

## Use conexões de federação de grid

### Clonar grupos de locatários e usuários em StorageGRID

Se um locatário foi criado ou editado para usar uma conexão de federação de grid, esse locatário é replicado de um sistema StorageGRID (o locatário de origem) para outro sistema StorageGRID (o locatário de réplica). Após o locatário ser replicado, todos os grupos e usuários adicionados ao locatário de origem são clonados para o locatário de réplica.

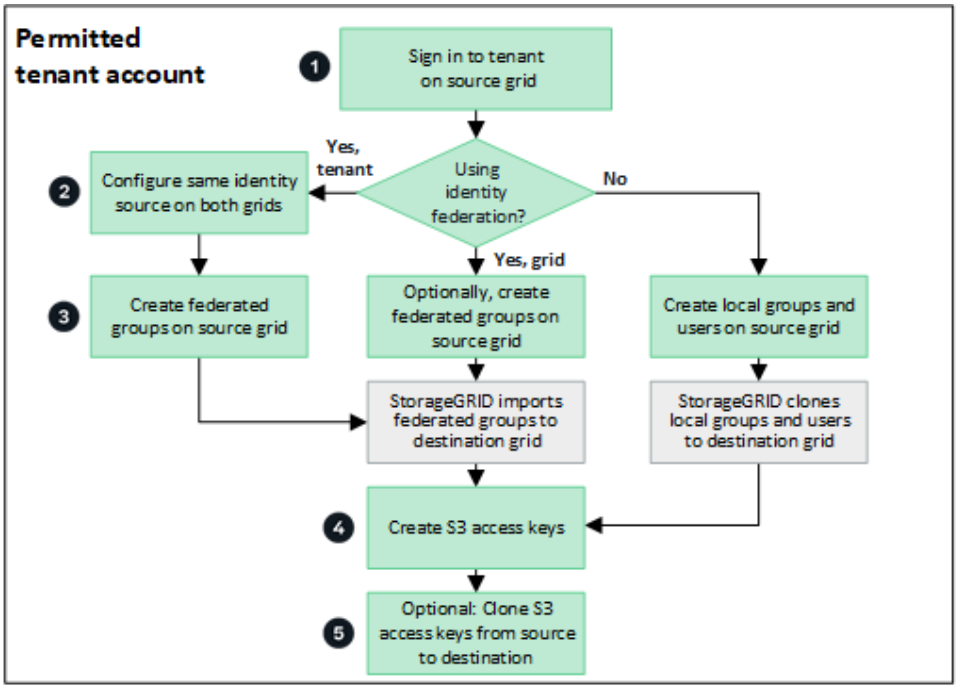
O sistema StorageGRID onde o tenant é originalmente criado é o *grid de origem* do tenant. O sistema StorageGRID onde o tenant é replicado é o *grid de destino* do tenant. Ambas as contas de tenant têm o mesmo ID de conta, nome, descrição, cota de armazenamento e permissões atribuídas, mas o tenant de destino não possui inicialmente uma senha de usuário raiz. Para obter detalhes, consulte "O que é clonagem de conta" e "Gerenciar locatários permitidos".

A clonagem das informações da conta do locatário é necessária para "replicação entre grids" dos objetos do bucket. Ter os mesmos grupos de locatários e usuários em ambas as grids garante que você possa acessar os buckets e objetos correspondentes em qualquer uma das grids.

#### Fluxo de trabalho do locatário para clonagem de conta

Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, revise o diagrama de

fluxo de trabalho para ver as etapas que você executará para clonar grupos, usuários e chaves de acesso S3.




Estas são as etapas principais do fluxo de trabalho:

### 1 Faça login no tenant

Faça login na conta do locatário na grade de origem (a grade onde o locatário foi criado inicialmente.)

### 2 Opcionalmente, configure a federação de identidades

Se a sua conta de locatário tiver a permissão **Usar a própria fonte de identidade** para usar grupos e usuários federados, configure a mesma fonte de identidade (com as mesmas configurações) para as contas de locatário de origem e destino. Grupos e usuários federados não podem ser clonados a menos que ambas as grids estejam usando a mesma fonte de identidade. Para obter instruções, consulte "Use federação de identidades".

### 3 Criar grupos e usuários

Ao criar grupos e usuários, sempre comece pela grade de origem do locatário. Ao adicionar um novo grupo, o StorageGRID o clona automaticamente para a grade de destino.

- Se a federação de identidades estiver configurada para todo o sistema StorageGRID ou para sua conta de locatário, "criar novos grupos de locatários" importe grupos federados da fonte de identidade.
- Se você não estiver usando federação de identidades, "criar novos grupos locais" e então "criar usuários locais".

### 4 Criar chaves de acesso S3

Você pode "Crie suas próprias chaves de acesso" ou "Criar chaves de acesso de outro usuário" na grade de

origem ou na grade de destino para acessar os buckets nessa grade.

### 5 Opcionalmente, clone as chaves de acesso S3

Se você precisar acessar buckets com as mesmas chaves de acesso em ambas as grades, crie as chaves de acesso na grade de origem e, em seguida, use a API do Tenant Manager para cloná-las manualmente para a grade de destino. Para obter instruções, consulte "Clonar chaves de acesso S3 usando a API".

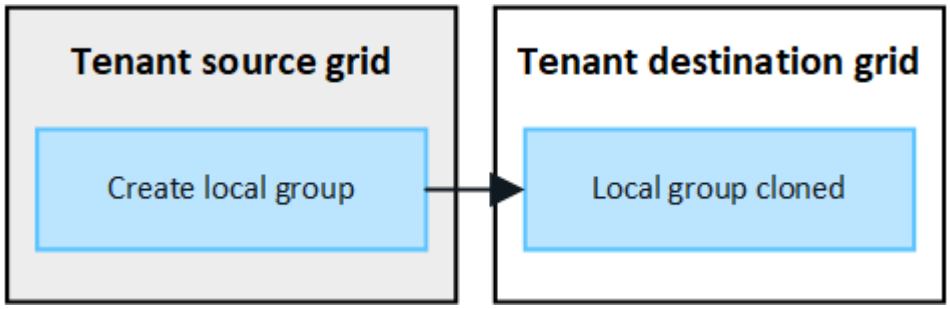
#### Como são clonados os grupos, usuários e chaves de acesso S3?

Analise esta seção para entender como grupos, usuários e chaves de acesso S3 são clonados entre a grade de origem do locatário e a grade de destino do locatário.

#### Os grupos locais criados na grade de origem são clonados

Após a criação de uma conta de locatário e sua replicação para a grade de destino, o StorageGRID clona automaticamente quaisquer grupos locais que você adicionar à grade de origem do locatário para a grade de destino do locatário.

Tanto o grupo original quanto seu clone possuem o mesmo modo de acesso, permissões de grupo e política de grupo S3. Para obter instruções, consulte "Criar grupos para o tenant S3".

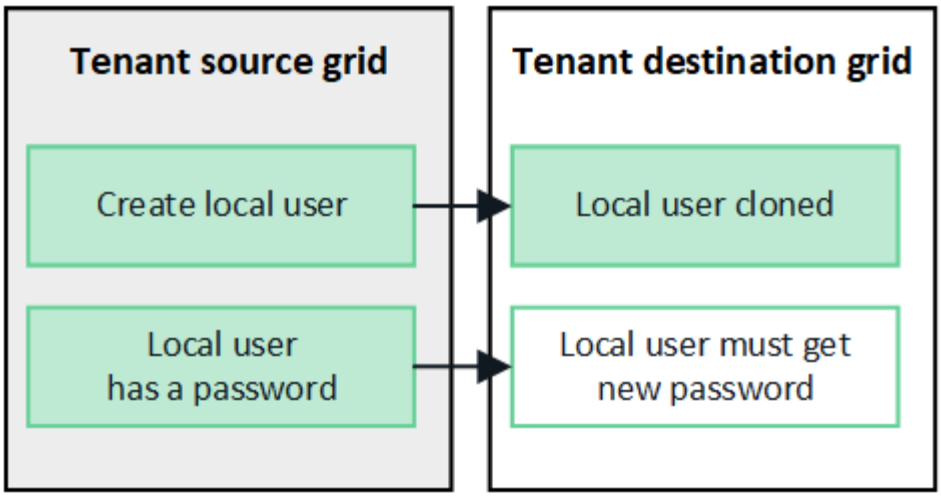



> Os usuários que você selecionar ao criar um grupo local na grid de origem não serão incluídos quando o grupo for clonado para a grid de destino. Por esse motivo, não selecione usuários ao criar o grupo. Em vez disso, selecione o grupo ao criar os usuários.

#### Usuários locais criados na grade de origem são clonados

Ao criar um novo usuário local na grade de origem, StorageGRID clona automaticamente esse usuário para a grade de destino. Tanto o usuário original quanto seu clone têm o mesmo nome completo, nome de usuário e configuração de **Negar acesso**. Ambos os usuários também pertencem aos mesmos grupos. Para obter instruções, consulte "Gerenciar usuários".

Por motivos de segurança, as senhas de usuários locais não são clonadas para o grid de destino. Se um usuário local precisar acessar o Tenant Manager no grid de destino, o usuário raiz da conta do tenant deve adicionar uma senha para esse usuário no grid de destino. Para obter instruções, consulte "Gerenciar usuários".

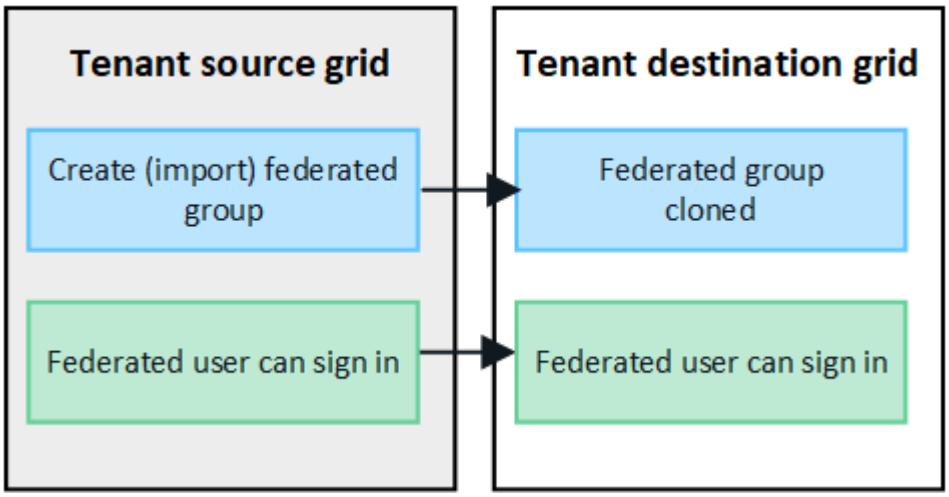



**Grupos federados criados na grade de origem são clonados**

Supondo que os requisitos para usar a clonagem de conta com "autenticação única" e "federação de identidade" tenham sido atendidos, os grupos federados que você criar (importar) para o locatário na grade de origem serão clonados automaticamente para o locatário na grade de destino.

Ambos os grupos têm o mesmo modo de acesso, permissões de grupo e política de grupo S3.

Após a criação de grupos federados para o locatário de origem e sua clonagem para o locatário de destino, os usuários federados podem fazer login no locatário em qualquer uma das grids.

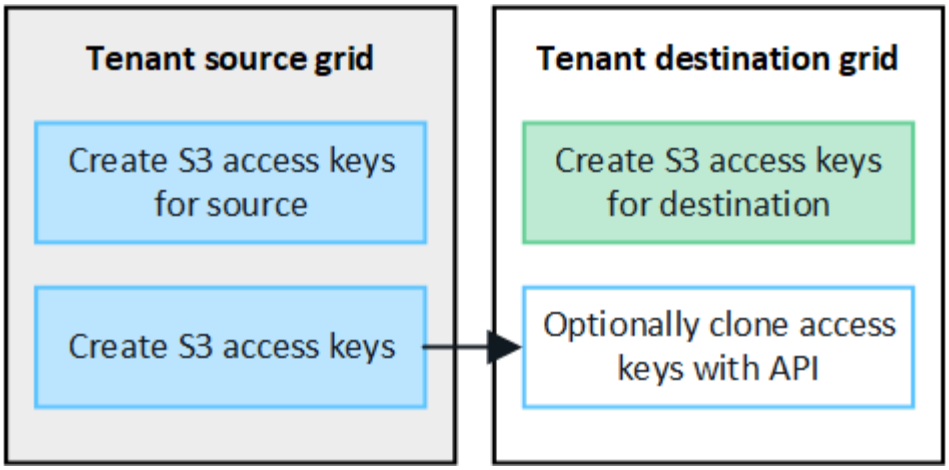



**As chaves de acesso S3 podem ser clonadas manualmente**

StorageGRID não clona automaticamente as chaves de acesso do S3 porque a segurança é aprimorada com chaves diferentes em cada grid.

Para gerenciar as chaves de acesso nas duas grades, você pode fazer o seguinte:

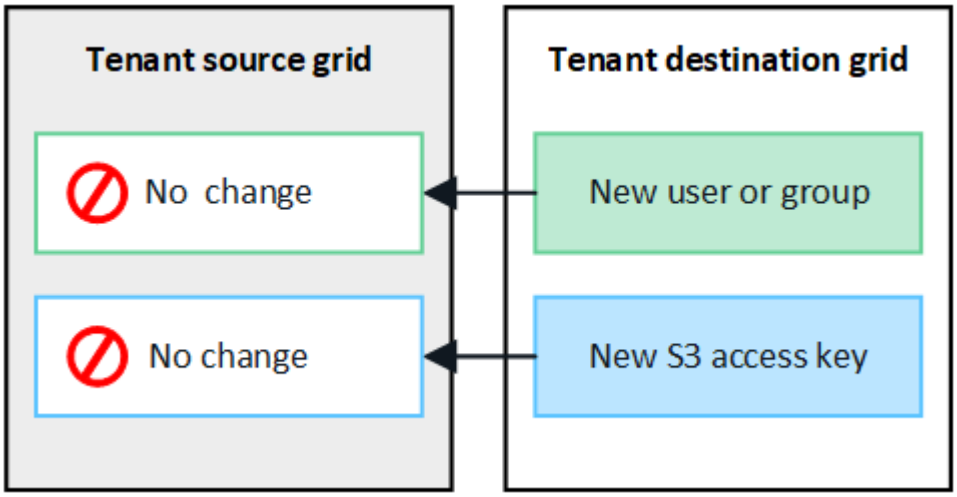
- Se você não precisar usar as mesmas chaves para cada grid, você pode "Crie suas próprias chaves de acesso" ou "Criar chaves de acesso de outro usuário" em cada grid.
- Se você precisar usar as mesmas chaves em ambas as grades, poderá criar chaves na grade de origem e, em seguida, usar a API do Gerenciador de Locatários para "clonar as chaves" manualmente na grade de destino.




Ao clonar as chaves de acesso do S3 para um usuário federado, tanto o usuário quanto as chaves de acesso do S3 são clonados para o locatário de destino.

**Grupos e usuários adicionados ao grid de destino não são clonados**

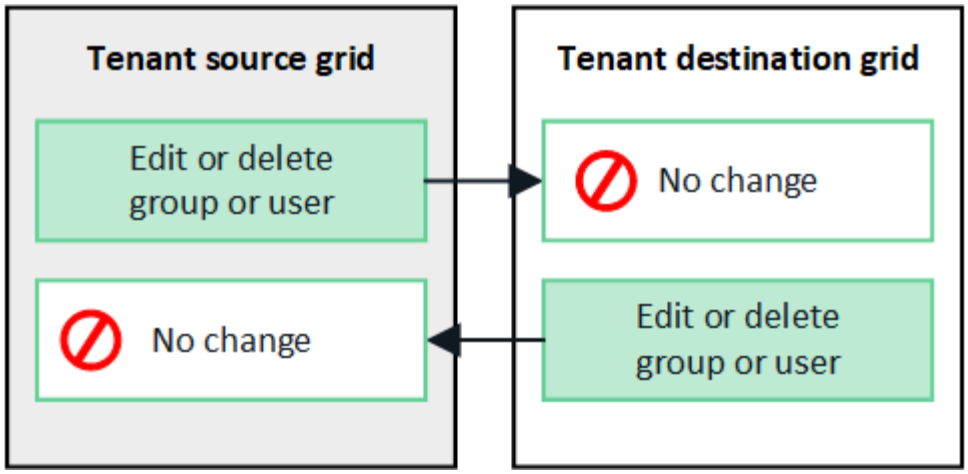
A clonagem ocorre somente da grade de origem do locatário para a grade de destino do locatário. Se você criar ou importar grupos e usuários na grade de destino do locatário, StorageGRID não clonará esses itens de volta para a grade de origem do locatário.




**Grupos, usuários e chaves de acesso editados ou excluídos não são clonados**

A clonagem ocorre somente quando você cria novos grupos e usuários.

Se você editar ou excluir grupos, usuários ou chaves de acesso em qualquer uma das grades, suas alterações não serão clonadas na outra grade.




**Clone chaves de acesso S3 entre StorageGRID grids usando a Tenant Management API**

Se a sua conta de locatário do StorageGRID tiver a permissão **Usar conexão de federação de grid**, você pode usar a API de Gerenciamento de Locatários para clonar manualmente as chaves de acesso S3 do locatário no grid de origem para o locatário no grid de destino.

**Antes de começar**

- A conta do locatário possui a permissão **Usar conexão de federação de grid**.
- A conexão da federação de grid tem um **Status de conexão** de **Conectado**.
- Você está conectado ao Gerenciador de Locatários na grade de origem do locatário usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Gerencie suas próprias credenciais do S3 ou permissão de acesso root".
- Se você estiver clonando chaves de acesso para um usuário local, o usuário já existe em ambas as grids.

> Ao clonar as chaves de acesso do S3 para um usuário federado, tanto o usuário quanto as chaves de acesso do S3 são adicionados ao locatário de destino.

**Clone suas próprias chaves de acesso**

Você pode clonar suas próprias chaves de acesso se precisar acessar os mesmos buckets em ambas as grids.

**Passos**

1. Utilize o Gerenciador de Inquilinos na grade de origem "Crie suas próprias chaves de acesso" e faça o download do `.csv`arquivo.
2. Na parte superior do Tenant Manager, selecione o ícone de ajuda e selecione **API documentation**.
3. Na seção **s3**, selecione o seguinte endpoint:

```
POST /org/users/current-user/replicate-s3-access-key
```

4. Selecione **Experimentar**.
5. Na caixa de texto **body**, substitua as entradas de exemplo para **accessKey** e **secretAccessKey** pelos valores do arquivo **.csv** que você baixou.

   Certifique-se de manter as aspas duplas em torno de cada string.


6. Se a chave expirar, substitua a entrada de exemplo para **expires** pela data e hora de expiração como uma string no formato de data e hora ISO 8601 (por exemplo, `2024-02-28T22:46:33-08:00`). Se a chave não expirar, insira **null** como o valor para a entrada **expires** (ou remova a linha **Expires** e a vírgula anterior).
7. Selecione **Executar**.
8. Confirme se o código de resposta do servidor é **204**, indicando que a chave foi clonada com sucesso para o grid de destino.

#### Clonar as chaves de acesso de outro usuário

Você pode clonar as chaves de acesso de outro usuário caso ele precise acessar os mesmos buckets em ambas as grids.

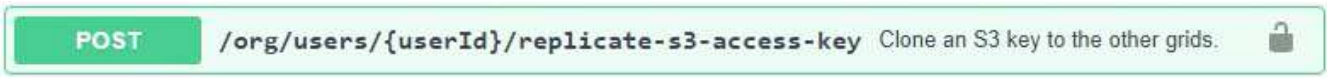
**Passos**

1. Utilize o Gerenciador de Inquilinos na grade de origem "crie as chaves de acesso S3 do outro usuário" e faça o download do `.csv`arquivo.
2. Na parte superior do Tenant Manager, selecione o ícone de ajuda e selecione **API documentation**.
3. Obtenha o ID do usuário. Você precisará desse valor para clonar as chaves de acesso do outro usuário.
   a. Na seção **usuários**, selecione o seguinte endpoint:

      `GET /org/users`

   b. Selecione **Experimentar**.
   c. Especifique quaisquer parâmetros que você deseja usar ao pesquisar usuários.
   d. Selecione **Executar**.
   e. Localize o usuário cujas chaves você deseja clonar e copie o número do campo **id**.
4. Na seção **s3**, selecione o seguinte endpoint:

   `POST /org/users/{userId}/replicate-s3-access-key`



5. Selecione **Experimentar**.
6. Na caixa de texto **userId**, cole o ID de usuário que você copiou.
7. Na caixa de texto **body**, substitua as entradas de exemplo para **example access key** e **secret access key** pelos valores do arquivo **.csv** para esse usuário.

   Certifique-se de manter as aspas duplas em torno da string.

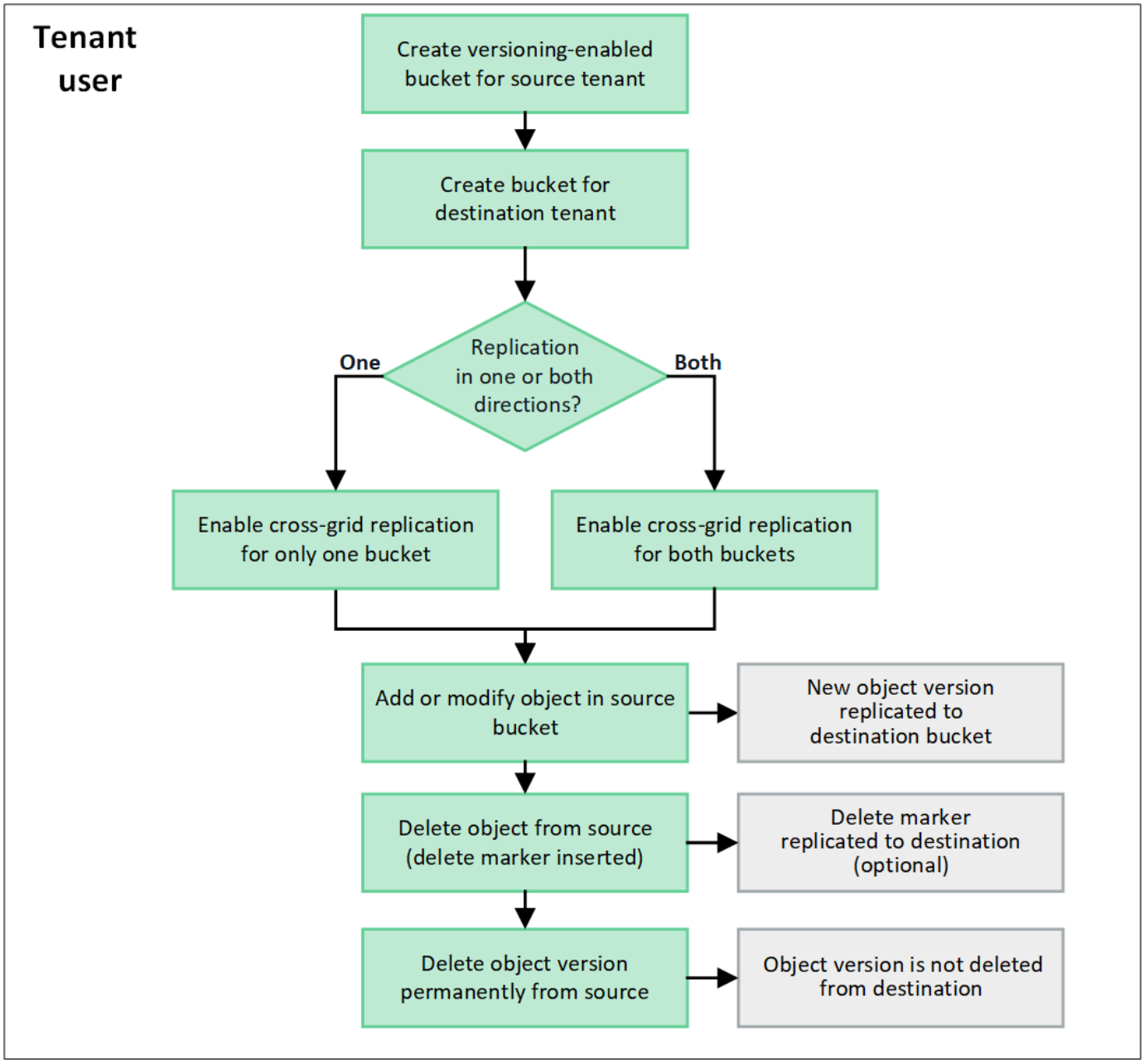
8. Se a chave expirar, substitua a entrada de exemplo para **expires** pela data e hora de expiração como uma string no formato de data e hora ISO 8601 (por exemplo, `2023-02-28T22:46:33-08:00`). Se a chave não expirar, insira **null** como o valor para a entrada **expires** (ou remova a linha **Expires** e a vírgula anterior).
9. Selecione **Executar**.
10. Confirme se o código de resposta do servidor é **204**, indicando que a chave foi clonada com sucesso para o grid de destino.

#### Gerencie a replicação entre grids no StorageGRID

Se a sua conta de locatário recebeu a permissão **Usar conexão de federação de grid** no momento da criação, você pode usar a replicação entre grids para replicar automaticamente objetos entre buckets na grid de origem do locatário e buckets na grid de destino do locatário. A replicação entre grids pode ocorrer em uma ou ambas as direções.

##### Fluxo de trabalho para replicação entre grids

O diagrama de fluxo de trabalho resume as etapas que você executa para configurar a replicação entre buckets em duas grades. Essas etapas são descritas com mais detalhes abaixo do diagrama.




#### Configurar replicação entre grids

Antes de usar a replicação entre grades, você precisa fazer login nas contas de locatário correspondentes em cada grid e criar dois buckets. Em seguida, você pode habilitar a replicação entre grades em um ou em ambos os buckets.

#### Antes de começar

- Você analisou os requisitos para replicação entre grades. Consulte "O que é replicação entre grids".
- Você está usando um "navegador web compatível".
- A conta do locatário possui a permissão **Usar conexão de federação de grid**, e contas de locatário idênticas existem em ambas as grids. Consulte "Gerencie os locatários permitidos para conexão de federação de grid".
- O usuário locatário com o qual você está fazendo login já existe em ambas as grades e pertence a um grupo de usuários que possui o "Permissão de acesso root".

- Se você estiver acessando a grade de destino do locatário como um usuário local, o usuário raiz da conta do locatário definiu uma senha para sua conta de usuário nessa grade.

### Crie dois buckets

Como primeiro passo, faça login nas contas de tenant correspondentes em cada grid e crie um bucket em cada grid.

**Passos**

1. A partir de qualquer uma das grids na conexão de federação de grids, crie um novo bucket:
   a. Faça login na conta do locatário usando as credenciais de um usuário locatário que exista em ambas as grids.

      Se você não conseguir acessar a grid de destino do locatário como usuário local, confirme se o usuário raiz da conta do locatário definiu uma senha para sua conta de usuário.

   b. Siga as instruções para "criar um bucket S3".

      Os nomes dos buckets e as regiões podem ser diferentes em cada grid.

   c. Na guia **Gerenciar configurações de objeto**, selecione **Ativar versionamento de objeto**.
   d. Se o S3 Object Lock estiver ativado para o seu sistema StorageGRID, consulte "Replicação entre grades com S3 Object Lock".
   e. Selecione **Create bucket**.
   f. Selecione **Concluir**.
2. Repita estes passos para criar um bucket para a mesma conta de locatário na outra grid na conexão de federação de grids.

   Conforme necessário, cada bucket pode usar uma região diferente.

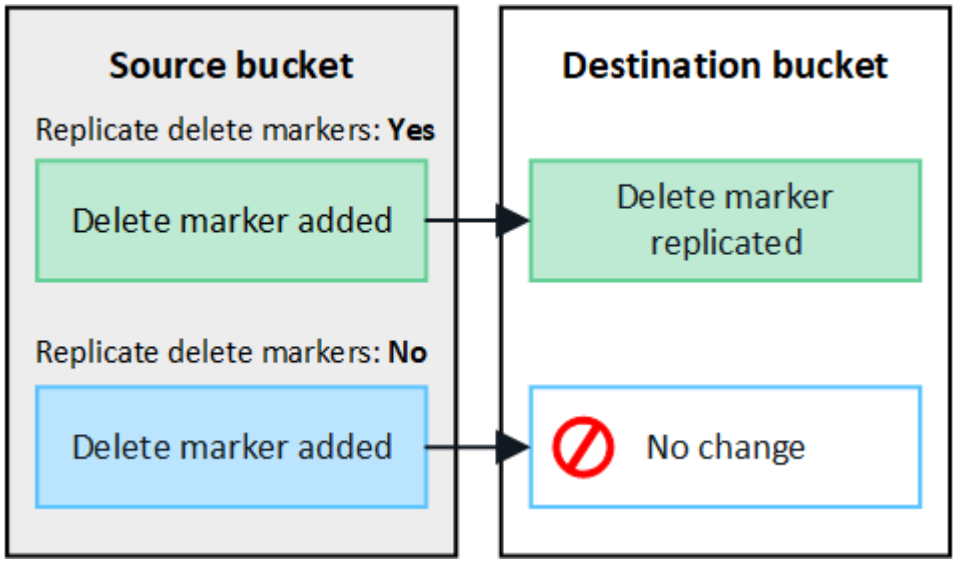
### Habilitar replicação entre grids

Você deve executar essas etapas antes de adicionar quaisquer objetos a qualquer um dos buckets.

**Passos**

1. Partindo de uma grid cujos objetos você deseja replicar, habilite "replicação entre grids em uma direção":
   a. Faça login na conta do locatário do bucket.
   b. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
   c. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
   d. Selecione a guia **Replicação entre grades**.
   e. Selecione **Ativar** e revise a lista de requisitos.
   f. Se todos os requisitos forem atendidos, selecione a conexão de federação de grid que você deseja usar.
   g. Opcionalmente, altere a configuração de **Replicar marcadores de exclusão** para determinar o que acontece no grid de destino se um cliente S3 enviar uma solicitação de exclusão para o grid de origem que não inclua um ID de versão:

- **Sim** (padrão): Um marcador de exclusão é adicionado ao bucket de origem e replicado para o bucket de destino.
- **Não**: Um marcador de exclusão é adicionado ao bucket de origem, mas não é replicado para o bucket de destino.




> Se a solicitação de exclusão incluir um ID de versão, essa versão do objeto será removida permanentemente do bucket de origem. StorageGRID não replica solicitações de exclusão que incluem um ID de versão, então a mesma versão do objeto não é excluída do destino.

Consulte "O que é replicação entre grids" para obter detalhes.

a. Opcionalmente, altere a configuração da categoria de auditoria **Replicação entre grades** para gerenciar o volume de mensagens de auditoria:
   - **Erro** (padrão): Somente as solicitações de replicação entre grids com falha são incluídas na saída de auditoria.
   - **Normal**: Todas as solicitações de replicação entre grades são incluídas, o que aumenta significativamente o volume da saída de auditoria.
b. Revise suas seleções. Você não poderá alterar essas configurações a menos que ambos os buckets estejam vazios.
c. Selecione **Ativar e testar**.

   Após alguns instantes, uma mensagem de sucesso é exibida. Os objetos adicionados a este bucket agora são replicados automaticamente para a outra grid. A **replicação entre grids** é exibida como um recurso ativado na página de detalhes do bucket.

2. Opcionalmente, vá para o bucket correspondente na outra grid e "Habilitar replicação entre grids em ambas as direções".

#### Testar a replicação entre grids

Se a replicação entre grades estiver habilitada para um bucket, talvez seja necessário verificar se a conexão e a replicação entre grades estão funcionando corretamente e se os buckets de origem e destino ainda atendem a todos os requisitos (por exemplo, o versionamento ainda está habilitado).

**Antes de começar**

- Você está usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Permissão de acesso root".

**Passos**

1. Faça login na conta do locatário do bucket.
2. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
4. Selecione a guia **Replicação entre grades**.
5. Selecione **Test connection**.

   Se a conexão estiver saudável, um banner de sucesso será exibido. Caso contrário, uma mensagem de erro será exibida, que você e o administrador da grid podem usar para resolver o problema. Para obter detalhes, consulte "Solucionar problemas de erros de federação de grid".

6. Se a replicação entre grades estiver configurada para ocorrer em ambas as direções, acesse o bucket correspondente na outra grade e selecione **Test connection** para verificar se a replicação entre grades está funcionando na outra direção.

#### Desativar replicação entre grades

Você pode interromper permanentemente a replicação entre grades se não quiser mais copiar objetos para a outra grade.

Antes de desativar a replicação entre grades, observe o seguinte:

- Desativar a replicação entre grades não remove nenhum objeto que já tenha sido copiado entre grades. Por exemplo, objetos em `my-bucket` na Grade 1 que foram copiados para `my-bucket` na Grade 2 não são removidos se você desativar a replicação entre grades para esse bucket. Se você quiser excluir esses objetos, você deve removê-los manualmente.
- Se a replicação entre grades estiver habilitada para cada um dos buckets (ou seja, se a replicação ocorrer em ambas as direções), você pode desabilitar a replicação entre grades para um ou ambos os buckets. Por exemplo, você pode querer desabilitar a replicação de objetos de `my-bucket` na Grade 1 para `my-bucket` na Grade 2, enquanto continua replicando objetos de `my-bucket` na Grade 2 para `my-bucket` na Grade 1.
- Você deve desativar a replicação entre grades antes de poder remover a permissão de um locatário para usar a conexão de federação de grade. Consulte "Gerenciar locatários permitidos".
- Se você desativar a replicação entre grades para um bucket que contém objetos, não poderá reativar a replicação entre grades, a menos que exclua todos os objetos tanto do bucket de origem quanto do bucket de destino.

  Você não pode reativar a replicação a menos que ambos os buckets estejam vazios.

**Antes de começar**

- Você está usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Permissão de acesso root".

**Passos**

1. A partir do grid cujos objetos você não deseja mais replicar, interrompa a replicação entre grids para o

bucket:

a. Faça login na conta do locatário do bucket.
b. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
c. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
d. Selecione a guia **Replicação entre grades**.
e. Selecione **Desativar replicação**.
f. Se você tem certeza de que deseja desativar a replicação entre grids para este bucket, digite **Yes** na caixa de texto e selecione **Disable**.

   Após alguns instantes, uma mensagem de sucesso é exibida. Novos objetos adicionados a este bucket não podem mais ser replicados automaticamente para a outra grid. **Replicação entre grids** não é mais exibida como um recurso ativado na página Buckets.

2. Se a replicação entre grades foi configurada para ocorrer em ambas as direções, acesse o bucket correspondente na outra grade e interrompa a replicação entre grades na outra direção.

### Visualizar conexões de federação de grid no StorageGRID

Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, você pode visualizar as conexões permitidas.

#### Antes de começar

- A conta do locatário possui a permissão **Usar conexão de federação de grid**.
- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Permissão de acesso root".

#### Passos

1. Selecione **STORAGE (S3)** > **Conexões de federação de grid**.

   A página de conexão da federação Grid é exibida e inclui uma tabela que resume as seguintes informações:

| Coluna | Descrição |
|---|---|
| Nome da conexão | As conexões de federação de grid que este locatário tem permissão para usar. |
| Buckets com replicação entre grids | Para cada conexão de federação de grid, os buckets de tenant que têm a replicação entre grids habilitada. Os objetos adicionados a esses buckets serão replicados para o outro grid na conexão. |
| Último erro | Para cada conexão de federação de grades, o erro mais recente ocorrido, se houver, durante a replicação de dados para a outra grade. Consulte Limpar o último erro. |

2. Opcionalmente, selecione um nome de bucket para "ver detalhes do bucket".

#### Limpar o último erro

Um erro pode aparecer na coluna **Último erro** por um dos seguintes motivos:

- A versão do objeto de origem não foi encontrada.
- O bucket de origem não foi encontrado.
- O bucket de destino foi excluído.
- O bucket de destino foi recriado por uma conta diferente.
- O bucket de destino está com o controle de versão suspenso.
- O bucket de destino foi recriado pela mesma conta, mas agora está sem versionamento.

> Esta coluna mostra apenas o último erro de replicação entre grades ocorrido; erros anteriores que possam ter ocorrido não serão exibidos.

**Passos**

1. Se uma mensagem aparecer na coluna **Último erro**, visualize o texto da mensagem.

   Por exemplo, esse erro indica que o bucket de destino para replicação entre grids estava em um estado inválido, possivelmente porque o versionamento estava suspenso ou o S3 Object Lock estava ativado.


2. Execute as ações recomendadas. Por exemplo, se o versionamento foi suspenso no bucket de destino para replicação entre grids, reative o versionamento para esse bucket.
3. Selecione a conexão na tabela.
4. Selecione **Limpar erro**.
5. Selecione **Sim** para limpar a mensagem e atualizar o status do sistema.
6. Aguarde de 5 a 6 minutos e, em seguida, insira um novo objeto no bucket. Confirme que a mensagem de erro não reaparece.

   > Para garantir que a mensagem de erro seja eliminada, aguarde pelo menos 5 minutos após o horário indicado na mensagem antes de inserir um novo objeto.

7. Para determinar se algum objeto não foi replicado devido a um erro no bucket, consulte "Identifique e repita operações de replicação com falha".

# Gerenciar grupos e usuários

## Use a federação de identidades no StorageGRID

Utilizar a federação de identidades agiliza a configuração de grupos de locatários e usuários, e permite que os usuários do locatário façam login na conta do locatário usando credenciais familiares.

### Configurar a federação de identidades para o Tenant Manager

Você pode configurar a federação de identidades para o Tenant Manager se desejar que os grupos e usuários do locatário sejam gerenciados em outro sistema, como Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server.

#### Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Permissão de acesso root".
- Você está usando Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server como provedor de identidade.

  > Se você deseja usar um serviço LDAP v3 que não esteja listado, entre em contato com o suporte técnico.

- Se você planeja usar o OpenLDAP, você deve configurar o servidor OpenLDAP. Veja Diretrizes para configurar o servidor OpenLDAP.
- Se você planeja usar o Transport Layer Security (TLS) para comunicações com o servidor LDAP, o provedor de identidade deve estar usando TLS 1.2 ou 1.3. Consulte "Cifras suportadas para conexões TLS de saída".

#### Sobre esta tarefa

A possibilidade de configurar um serviço de federação de identidades para seu locatário depende de como sua conta de locatário foi configurada. Seu locatário pode compartilhar o serviço de federação de identidades configurado para o Grid Manager. Se você vir esta mensagem ao acessar a página de federação de identidades, não é possível configurar uma fonte de identidade federada separada para este locatário.

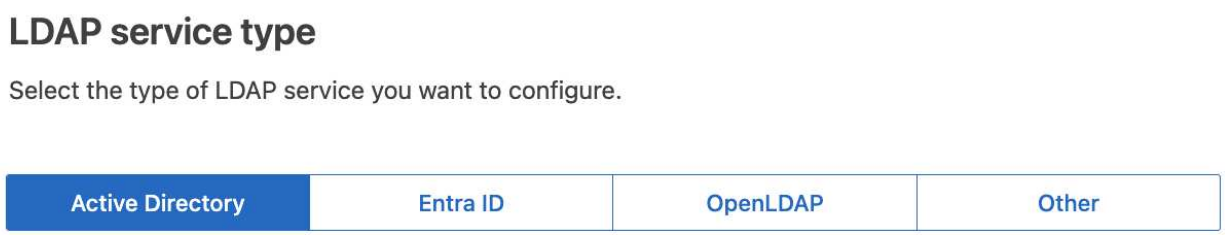
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

#### Insira a configuração

Ao configurar a federação de identidade, você fornece os valores que o StorageGRID precisa para se conectar a um serviço LDAP.

#### Passos

1. Selecione **Gerenciamento de acesso** > **Federação de identidades**.
2. Selecione **Ativar federação de identidades**.
3. Na seção tipo de serviço LDAP, selecione o tipo de serviço LDAP que você deseja configurar.




Selecione **Outro** para configurar valores de um servidor LDAP que utiliza o Oracle Directory Server.

4. Se você selecionou **Outro**, preencha os campos na seção Atributos LDAP. Caso contrário, vá para a próxima etapa.
   - **Nome Único do Usuário**: O nome do atributo que contém o identificador único de um usuário LDAP. Este atributo é equivalente a `sAMAccountName` para Active Directory e `uid` para OpenLDAP. Se você estiver configurando o Oracle Directory Server, insira `uid`.
   - **UUID do usuário**: O nome do atributo que contém o identificador único permanente de um usuário LDAP. Este atributo é equivalente a `objectGUID` para Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando Oracle Directory Server, insira `nsuniqueid`. O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos, em formato de 16 bytes ou string, onde os hífens são ignorados.
   - **Nome Único do Grupo**: O nome do atributo que contém o identificador único de um grupo LDAP. Este atributo é equivalente a `sAMAccountName` para Active Directory e `cn` para OpenLDAP. Se você estiver configurando Oracle Directory Server, insira `cn`.
   - **UUID do Grupo**: O nome do atributo que contém o identificador único permanente de um grupo LDAP. Este atributo é equivalente a `objectGUID` para Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando Oracle Directory Server, insira `nsuniqueid`. O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos, em formato de 16 bytes ou string, onde os hífens são ignorados.
5. Para todos os tipos de serviço LDAP, insira as informações necessárias do servidor LDAP e da conexão de rede na seção Configurar servidor LDAP.
   - **Nome do host**: O domínio totalmente qualificado (FQDN) ou endereço IP do servidor LDAP.
   - **Porta**: A porta usada para conectar ao servidor LDAP.

     A porta padrão para STARTTLS é 389 e a porta padrão para LDAPS é 636. No entanto, você pode usar qualquer porta, desde que seu firewall esteja configurado corretamente.

   - **Nome de usuário**: O caminho completo do nome diferenciado (DN) do usuário que vai se conectar ao servidor LDAP.

     Para o Active Directory, você também pode especificar o Down-Level Logon Name ou o User Principal Name.

     O usuário especificado deve ter permissão para listar grupos e usuários e para acessar os seguintes atributos:

     - `sAMAccountName` ou `uid`
     - `objectGUID`, `entryUUID`, ou `nsuniqueid`

- `cn`
- `memberOf` ou `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, e `userPrincipalName`
- **Entra ID**: `accountEnabled` e `userPrincipalName`

◦ **Senha**: a senha associada ao nome de usuário.

> Se você alterar a senha no futuro, você deve atualizá-la nesta página.

◦ **DN Base do Grupo**: O caminho completo do nome diferenciado (DN) de uma subárvore LDAP na qual você deseja pesquisar grupos. No exemplo do Active Directory (abaixo), todos os grupos cujo nome diferenciado é relativo ao DN base (DC=storagegrid,DC=example,DC=com) podem ser usados como grupos federados.

> Os valores do **Nome único do grupo** devem ser únicos dentro do **DN base do grupo** ao qual pertencem.

◦ **DN Base do Usuário**: O caminho completo do nome diferenciado (DN) de uma subárvore LDAP na qual você deseja pesquisar usuários.

> Os valores do **Nome único do usuário** devem ser únicos dentro do **DN base do usuário** ao qual pertencem.

◦ **Formato de nome de usuário de vinculação** (opcional): o padrão de nome de usuário que StorageGRID deve usar se o padrão não puder ser determinado automaticamente.

É recomendável fornecer o **formato de nome de usuário de vinculação**, pois isso pode permitir que os usuários façam login caso o StorageGRID não consiga se vincular à conta de serviço.

Insira um destes padrões:

- **UserPrincipalName padrão (AD e Entra ID)**: `[USERNAME]@example.com`
- **Padrão de nome de logon de nível inferior (AD e Entra ID)**: `example\[USERNAME]`
- **Padrão de nome diferenciado**: `CN=[USERNAME],CN=Users,DC=example,DC=com`

  Inclua **[USERNAME]** exatamente como está escrito.

6. Na seção Transport Layer Security (TLS), selecione uma configuração de segurança.
   ◦ **Usar STARTTLS**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada para Active Directory, OpenLDAP ou outros, mas esta opção não é compatível com Microsoft Entra ID.
   ◦ **Usar LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar esta opção para Microsoft Entra ID.
   ◦ **Não utilize TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será seguro. Esta opção não é compatível com Microsoft Entra ID.

A opção **Não usar TLS** não é compatível se o seu servidor Active Directory exigir assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

7. Se você selecionou STARTTLS ou LDAPS, escolha o certificado usado para proteger a conexão.
   - **Usar certificado CA do sistema operacional**: Use o certificado CA padrão do Grid instalado no sistema operacional para proteger as conexões.
   - **Usar certificado CA personalizado**: use um certificado de segurança personalizado.

     Se você selecionar esta opção, copie e cole o certificado de segurança personalizado na caixa de texto do certificado da CA.

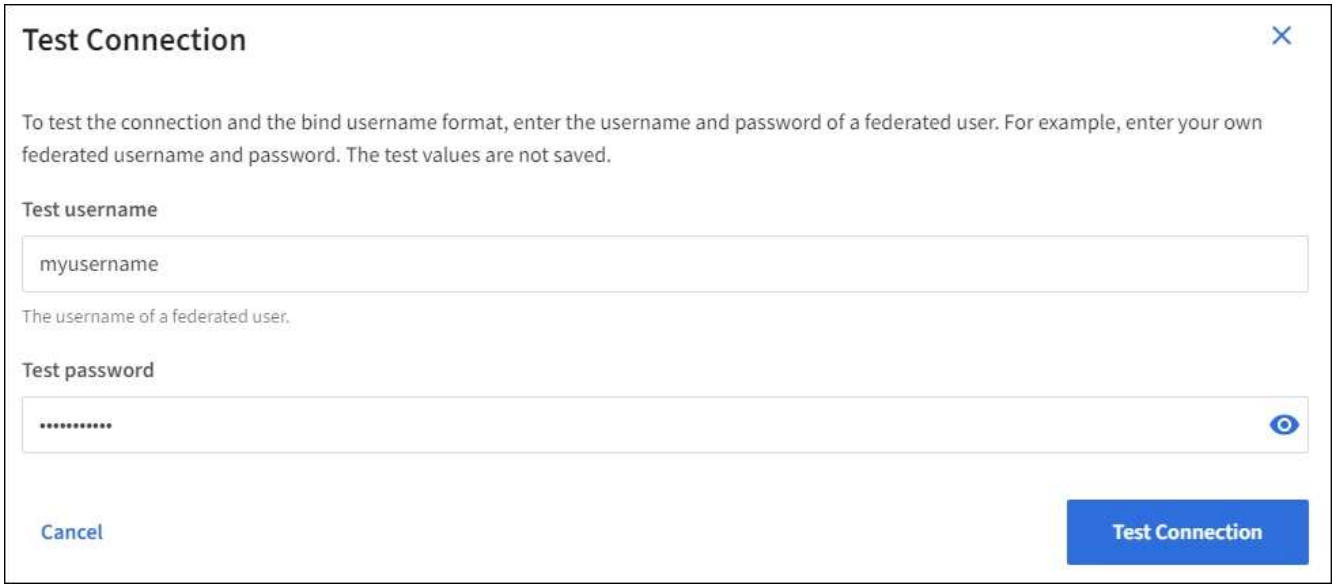
### Teste a conexão e salve a configuração

Após inserir todos os valores, você deve testar a conexão antes de salvar a configuração. StorageGRID verifica as configurações de conexão para o servidor LDAP e o formato do nome de usuário de bind, caso você tenha fornecido um.

**Passos**

1. Selecione **Test connection**.
2. Se você não forneceu um formato de nome de usuário de vinculação:
   - Uma mensagem "Conexão testada com sucesso" é exibida se as configurações de conexão forem válidas. Selecione **Salvar** para salvar a configuração.
   - A mensagem "Não foi possível estabelecer a conexão de teste" será exibida se as configurações de conexão forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.
3. Se você forneceu um formato de nome de usuário de vinculação, insira o nome de usuário e a senha de um usuário federado válido.

   Por exemplo, insira seu próprio nome de usuário e senha. Não inclua caracteres especiais no nome de usuário, como @ ou /.




   - Uma mensagem "Conexão testada com sucesso" é exibida se as configurações de conexão forem válidas. Selecione **Salvar** para salvar a configuração.

- Uma mensagem de erro será exibida se as configurações de conexão, o formato do nome de usuário de vinculação ou o nome de usuário e senha de teste forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

#### Forçar sincronização com a fonte de identidade

O sistema StorageGRID sincroniza periodicamente grupos e usuários federados da fonte de identidade. Você pode forçar o início da sincronização se quiser habilitar ou restringir permissões de usuário o mais rápido possível.

**Passos**

1. Acesse a página de federação de identidades.
2. Selecione **Sync server** na parte superior da página.

   O processo de sincronização pode demorar algum tempo dependendo do seu ambiente.

   O alerta **Falha na sincronização da federação de identidades** é acionado se houver um problema na sincronização de grupos e usuários federados da fonte de identidade.

#### Desativar federação de identidade

Você pode desativar temporariamente ou permanentemente a federação de identidades para grupos e usuários. Quando a federação de identidades está desativada, não há comunicação entre StorageGRID e a fonte de identidade. No entanto, todas as configurações que você configurou são mantidas, permitindo que você reative facilmente a federação de identidades no futuro.

**Sobre esta tarefa**

Antes de desativar a federação de identidades, você deve estar ciente do seguinte:

- Usuários federados não poderão fazer login.
- Os usuários federados que estiverem conectados no momento manterão o acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login após a expiração da sessão.
- A sincronização entre o sistema StorageGRID e a fonte de identidade não ocorrerá e alertas não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Habilitar federação de identidades** fica desabilitada se o status de logon único (SSO) for **Habilitado** ou **Modo Sandbox**. O status do SSO na página de logon único deve ser **Desabilitado** antes que você possa desabilitar a federação de identidades. Consulte "Desativar single sign-on".

**Passos**

1. Acesse a página de federação de identidades.
2. Desmarque a caixa de seleção **Ativar federação de identidades**.

#### Diretrizes para configurar o servidor OpenLDAP

Se você deseja usar um servidor OpenLDAP para federação de identidades, você deve configurar definições específicas no servidor OpenLDAP.

Para fontes de identidade que não sejam o Active Directory ou o Microsoft Entra ID, StorageGRID não bloqueará automaticamente o acesso S3 para usuários que estejam desabilitados externamente. Para bloquear o acesso S3, exclua quaisquer chaves S3 do usuário ou remova o usuário de todos os grupos.

#### Memberof e sobreposições refint

As sobreposições memberof e refint devem estar habilitadas. Para obter mais informações, consulte as instruções para manutenção reversa de associação de grupo no "Documentação do OpenLDAP: Guia do administrador da versão 2.4".

#### Indexação

Você deve configurar os seguintes atributos do OpenLDAP com as palavras-chave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Além disso, certifique-se de que os campos mencionados na ajuda para Username estejam indexados para um desempenho ideal.

Consulte as informações sobre a manutenção reversa da associação a grupos no "Documentação do OpenLDAP: Guia do administrador da versão 2.4".

### Gerenciar grupos de locatários

#### Crie grupos para um locatário S3 no StorageGRID

Você pode gerenciar permissões para grupos de usuários do S3 importando grupos federados ou criando grupos locais.

#### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Permissão de acesso root".
- Se você planeja importar um grupo federado, você tem "federação de identidade configurada" e o grupo federado já existe na fonte de identidade configurada.
- Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, você tiver revisado o fluxo de trabalho e as considerações para "clonagem de grupos de inquilinos e usuários" e estiver conectado à grid de origem do locatário.

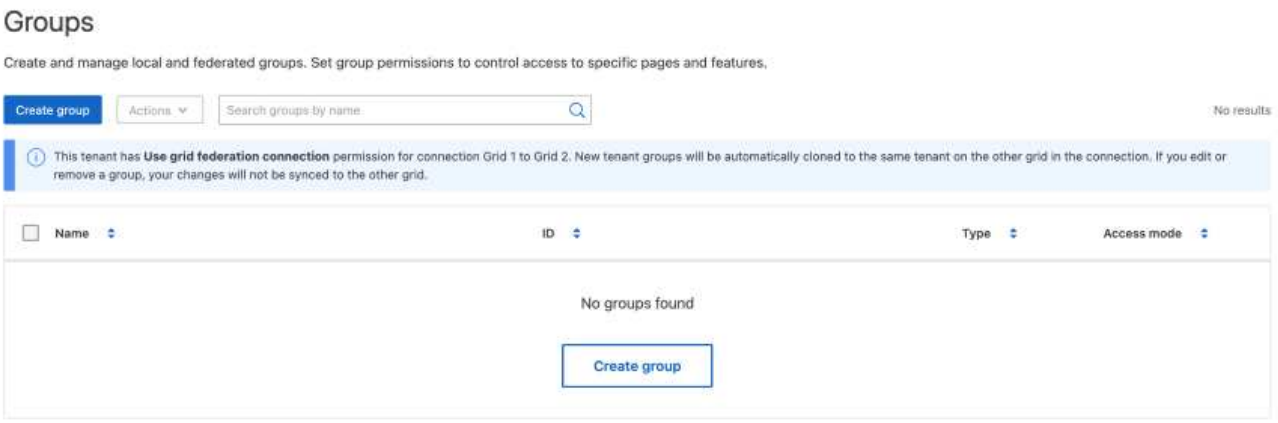
#### Acesse o assistente de criação de grupo

Como primeiro passo, acesse o assistente Create group.

#### Passos

1. Selecione **Gerenciamento de Acesso** > **Grupos**.
2. Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, confirme se uma faixa

azul aparece, indicando que novos grupos criados neste grid serão clonados para o mesmo locatário no outro grid da conexão. Se essa faixa não aparecer, você pode estar conectado ao grid de destino do locatário.




3. Selecione **Criar grupo**.

### Escolha um tipo de grupo

Você pode criar um grupo local ou importar um grupo federado.

**Passos**

1. Selecione a guia **Grupo local** para criar um grupo local ou selecione a guia **Grupo federado** para importar um grupo da fonte de identidade previamente configurada.

   Se o single sign-on (SSO) estiver habilitado para seu sistema StorageGRID, os usuários pertencentes a grupos locais não poderão acessar o Tenant Manager, embora possam usar aplicativos cliente para gerenciar os recursos do tenant, com base nas permissões de grupo.

2. Digite o nome do grupo.
   - **Grupo local**: Insira um nome de exibição e um nome exclusivo. Você pode editar o nome de exibição depois.

     Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, ocorrerá um erro de clonagem se o mesmo **Nome exclusivo** já existir para o locatário na grid de destino.

   - **Grupo federado**: Insira o nome exclusivo. Para Active Directory, o nome exclusivo é o nome associado ao `sAMAccountName` atributo. Para OpenLDAP, o nome exclusivo é o nome associado ao `uid` atributo.
3. Selecione **Continue**.

### Gerenciar permissões de grupo

As permissões de grupo controlam quais tarefas os usuários podem executar no Gerenciador de Inquilinos e na API de Gerenciamento de Inquilinos.

**Passos**

1. Para **Modo de acesso**, selecione uma das seguintes opções:

- **Leitura e gravação** (padrão): os usuários podem fazer login no Gerenciador de Locatários e gerenciar a configuração do locatário.
- **Somente leitura**: Os usuários podem apenas visualizar as configurações e os recursos. Eles não podem fazer alterações nem executar operações no Tenant Manager ou Tenant Management API. Usuários locais com permissão somente leitura podem alterar suas próprias senhas.

> Se um usuário pertencer a vários grupos e qualquer um deles estiver definido como somente leitura, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

2. Selecione uma ou mais permissões para este grupo.

   Consulte "Permissões de gerenciamento de tenant".

3. Selecione **Continue**.

### Definir política de grupo S3

A política de grupo determina quais permissões de acesso ao S3 os usuários terão.

**Passos**

1. Selecione a política que você deseja usar para este grupo.

| Política de grupo | Descrição |
|---|---|
| Sem acesso ao S3 | Padrão. Os usuários deste grupo não têm acesso aos recursos do S3, a menos que o acesso seja concedido por meio de uma política de bucket. Se você selecionar esta opção, somente o usuário raiz 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 deste grupo podem listar objetos e ler dados de objetos, metadados e tags. Ao selecionar esta opção, a string JSON para uma política de grupo somente leitura aparece na caixa de texto. Você não pode editar essa string. |
| Acesso total | Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Ao selecionar esta opção, a string JSON para uma política de grupo de acesso total aparece na caixa de texto. Você não pode editar esta string. |
| Mitigação de Ransomware | Esta política de exemplo aplica-se a todos os buckets deste locatário. Os usuários deste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que tenham o versionamento de objetos ativado.<br><br>Os usuários do Tenant Manager que possuem a permissão **Gerenciar todos os buckets** podem substituir esta política de grupo. Limite a permissão **Gerenciar todos os buckets** a usuários confiáveis e utilize a autenticação multifator (MFA) quando disponível. |

| Política de grupo | Descrição |
| --- | --- |
| Personalizado | Os usuários do grupo recebem as permissões que você especificar na caixa de texto. |

2. Se você selecionou **Personalizado**, insira a política de grupo. Cada política de grupo tem um limite de tamanho de 5.120 bytes. Você deve inserir uma string formatada em JSON válida.

   Para obter informações detalhadas sobre políticas de grupo, incluindo sintaxe de linguagem e exemplos, consulte "Exemplos de políticas de grupo".

3. Se estiver criando um grupo local, selecione **Continuar**. Se estiver criando um grupo federado, selecione **Criar grupo** e **Concluir**.

### Adicionar usuários (somente grupos locais)

Você pode salvar o grupo sem adicionar usuários ou, opcionalmente, adicionar quaisquer usuários locais que já existam.

> Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, quaisquer usuários que você selecionar ao criar um grupo local no grid de origem não serão incluídos quando o grupo for clonado para o grid de destino. Por esse motivo, não selecione usuários ao criar o grupo. Em vez disso, selecione o grupo ao criar os usuários.

**Passos**

1. Opcionalmente, selecione um ou mais usuários locais para este grupo.
2. Selecione **Criar grupo** e **Concluir**.

   O grupo que você criou aparece na lista de grupos.

   Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid** e você estiver no grid de origem do locatário, o novo grupo será clonado para o grid de destino do locatário. **Sucesso** aparece como o **Status da clonagem** na seção Visão geral da página de detalhes do grupo.

#### Permissões de gerenciamento de locatários do StorageGRID

Antes de criar um grupo de locatários, considere quais permissões você deseja atribuir a esse grupo. As permissões de gerenciamento de locatários determinam quais tarefas os usuários podem executar usando o Tenant Manager ou a Tenant Management API. Um usuário pode pertencer a um ou mais grupos. As permissões são cumulativas se um usuário pertencer a vários grupos.

Para iniciar sessão no Gerenciador de Inquilinos ou usar a API de Gerenciamento de Inquilinos, os usuários devem pertencer a um grupo que tenha pelo menos uma permissão. Todos os usuários que podem iniciar sessão podem executar as seguintes tarefas:

- Veja o dashboard
- Alterar a própria senha (para usuários locais)

Para todas as permissões, a configuração do Modo de acesso do grupo determina se os usuários podem alterar as configurações e executar operações ou se podem apenas visualizar as configurações e recursos

relacionados.

> Se um usuário pertencer a vários grupos e qualquer um deles estiver definido como somente leitura, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

Você pode atribuir as seguintes permissões a um grupo.

| Permissão | Descrição | Detalhes |
|---|---|---|
| Acesso à raiz | Fornece acesso completo ao Tenant Manager e à Tenant Management API. | |
| Gerencie suas próprias credenciais do S3 | Permite aos usuários criar e remover suas próprias chaves de acesso ao S3. | Usuários que não possuem essa permissão não veem a opção de menu **ARMAZENAMENTO (S3)** > **Minhas chaves de acesso ao S3**. |
| Ver todos os buckets | Permite aos usuários visualizar todos os buckets e configurações de bucket. | Usuários que não possuem a permissão "Visualizar todos os buckets" ou "Gerenciar todos os buckets" não veem a opção de menu "Buckets".<br><br>Essa permissão foi substituída pela permissão Gerenciar todos os buckets. Ela não afeta as políticas de bucket ou grupo do S3 usadas pelos clientes do S3 ou pelo Console do S3. |
| Gerenciar todos os buckets | Permite que os usuários utilizem o Tenant Manager e a API de Tenant Management para criar e excluir buckets do S3 e gerenciar as configurações de todos os buckets do S3 na conta do tenant, independentemente das políticas de bucket ou de grupo do S3. | Usuários que não possuem a permissão "Visualizar todos os buckets" ou "Gerenciar todos os buckets" não veem a opção de menu "Buckets".<br><br>Essa permissão substitui a permissão Visualizar todos os buckets. Ela não afeta as políticas de bucket ou grupo do S3 usadas pelos clientes do S3 ou pelo Console do S3. |
| Gerenciar endpoints | Permite que os usuários utilizem o Tenant Manager ou a API de gerenciamento de locatários para criar ou editar endpoints de serviço da plataforma, que são usados como destino para os serviços da plataforma StorageGRID. | Usuários que não possuem essa permissão não veem a opção de menu **Pontos de extremidade dos serviços da plataforma**. |

| Permissão | Descrição | Detalhes |
| --- | --- | --- |
| Use a aba Console do S3 | Quando combinada com a permissão "Visualizar todos os buckets" ou "Gerenciar todos os buckets", permite que os usuários visualizem e gerenciem objetos na guia "Console do S3" da página de detalhes de um bucket. | |

#### Gerenciar grupos de locatários do StorageGRID

## Gerencie seus grupos de inquilinos conforme necessário para visualizar, editar ou duplicar um grupo e muito mais.

### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Permissão de acesso root".

### Ver ou editar grupo

Você pode visualizar e editar as informações básicas e os detalhes de cada grupo.

### Passos

1. Selecione **Gerenciamento de Acesso** > **Grupos**.
2. Analise as informações fornecidas na página Grupos, que lista informações básicas para todos os grupos locais e federados desta conta de tenant.

   Se a conta do locatário tiver a permissão **Usar conexão de federação de grade** e você estiver visualizando grupos na grade de origem do locatário:

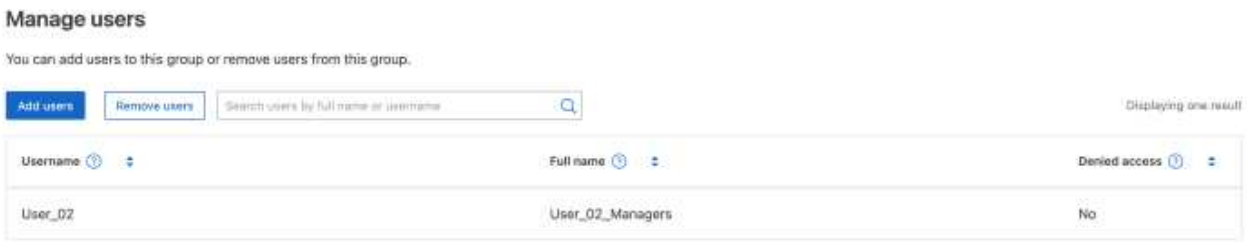
   - Uma mensagem no banner indica que, se você editar ou remover um grupo, suas alterações não serão sincronizadas com a outra grid.
   - Conforme necessário, uma mensagem em destaque indica se os grupos não foram clonados para o locatário na grade de destino. Você pode tentar novamente um clone de grupo que falharam.
3. Se você deseja alterar o nome do grupo:
   a. Selecione a caixa de seleção do grupo.
   b. Selecione **Ações** > **Editar nome do grupo**.
   c. Digite o novo nome.
   d. Selecione **Salvar alterações**.
4. Se você deseja visualizar mais detalhes ou fazer edições adicionais, faça um dos seguintes procedimentos:
   - Selecione o nome do grupo.
   - Selecione a caixa de seleção do grupo e selecione **Ações** > **Exibir detalhes do grupo**.
5. Consulte a seção Visão geral, que apresenta as seguintes informações para cada grupo:
   - Nome de exibição
   - Nome único

- Tipo
- Modo de acesso
- Permissões
- Política S3
- Número de usuários neste grupo
- Campos adicionais se a conta do locatário tiver a permissão **Usar conexão de federação de grid** e você estiver visualizando o grupo no grid de origem do locatário:
  - Status da clonagem, **Sucesso** ou **Falha**
  - Uma faixa azul indica que, se você editar ou excluir este grupo, suas alterações não serão sincronizadas com a outra grid.

6. Edite as configurações do grupo conforme necessário. Consulte "Crie grupos para um locatário do S3" para obter detalhes sobre o que inserir.
   a. Na seção Visão geral, altere o nome de exibição selecionando o nome ou o ícone de edição .
   b. Na guia **Permissões de grupo**, atualize as permissões e selecione **Salvar alterações**.
   c. Na guia **Política de grupo**, faça as alterações desejadas e selecione **Salvar alterações**.

      Opcionalmente, selecione uma política de grupo S3 diferente ou insira a string JSON para uma política personalizada, conforme necessário.

7. Para adicionar um ou mais usuários locais existentes ao grupo:
   a. Selecione a guia Usuários.




   b. Selecione **Adicionar usuários**.
   c. Selecione os usuários existentes que você deseja adicionar e selecione **Adicionar usuários**.

      Uma mensagem de sucesso aparece no canto superior direito.

8. Para remover usuários locais do grupo:
   a. Selecione a guia Usuários.
   b. Selecione **Remover usuários**.
   c. Selecione os usuários que você deseja remover e selecione **Remover usuários**.

      Uma mensagem de sucesso aparece no canto superior direito.

9. Confirme se você selecionou **Salvar alterações** para cada seção que você modificou.

### Grupo duplicado

Você pode duplicar um grupo existente para criar novos grupos mais rapidamente.

> Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid** e você duplicar um grupo do grid de origem do locatário, o grupo duplicado será clonado para o grid de destino do locatário.

**Passos**

1. Selecione **Gerenciamento de Acesso** > **Grupos**.
2. Selecione a caixa de seleção do grupo que você deseja duplicar.
3. Selecione **Ações** > **Duplicar grupo**.
4. Veja "Crie grupos para um locatário do S3" os detalhes sobre o que inserir.
5. Selecione **Criar grupo**.

### Tentar novamente clonagem de grupo

Para tentar novamente uma clonagem que falhou:

1. Selecione cada grupo que indicar *(Falha na clonagem)* abaixo do nome do grupo.
2. Selecione **Ações** > **Clonar grupos**.
3. Veja o status da operação de clonagem na página de detalhes de cada grupo que você está clonando.

Para obter informações adicionais, consulte "Clonar grupos de tenants e usuários".

### Excluir um ou mais grupos

Você pode excluir um ou mais grupos. Qualquer usuário que pertença apenas a um grupo que for excluído não poderá mais acessar o Tenant Manager nem usar a conta do tenant.

> Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grade** e você excluir um grupo, StorageGRID não excluirá o grupo correspondente na outra grade. Se você precisar manter essas informações sincronizadas, deverá excluir o mesmo grupo de ambas as grades.

**Passos**

1. Selecione **Gerenciamento de Acesso** > **Grupos**.
2. Selecione a caixa de seleção para cada grupo que você deseja excluir.
3. Selecione **Ações** > **Excluir grupo** ou **Ações** > **Excluir grupos**.

   Uma caixa de diálogo de confirmação é exibida.

4. Selecione **Excluir grupo** ou **Excluir grupos**.

### Configurar AssumeRole

**Antes de começar**

Você precisa ser um administrador para configurar AssumeRole.

**Sobre esta tarefa**

Para configurar AssumeRole, crie o grupo de destino a ser assumido, caso ele ainda não exista. Edite a política S3 do grupo para especificar as ações permitidas ao assumir esse grupo. Edite a política de confiança S3 do grupo para especificar os usuários confiáveis autorizados a assumir o grupo com a API AssumeRole.

As credenciais de segurança temporárias criadas ao assumir este grupo são válidas por um período limitado. A sessão dura entre 15 minutos e 12 horas, e a sessão padrão é de 1 hora. Quando você remove o usuário da política de confiança do S3 do grupo, o usuário não pode mais assumir este grupo.

**Passos**

1. Selecione **Gerenciamento de Acesso** > **Grupos**.
2. Clique no nome do grupo.
3. Selecione a guia **Política de confiança do S3**.
4. Adicione sua política de confiança do S3, incluindo uma lista de usuários que podem executar AssumeRole.
5. Selecione **Save changes**.
6. Selecione a guia **Política de grupo S3**.
7. Edite a política do S3 para especificar apenas as ações do S3 necessárias para os usuários confiáveis adicionados na política de confiança do S3 deste grupo.
8. Selecione **Save changes**.

**Exemplo de uma AssumeRole política de confiança S3**

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

Após a conclusão da configuração, os usuários listados na política de confiança do S3 podem executar AssumeRole e receber credenciais. As permissões finais são determinadas pela política de grupo, política de bucket e política de sessão. Para mais informações, consulte "Use políticas de acesso".

**Gerenciar usuários de locatários do StorageGRID**

Você pode criar usuários locais e atribuí-los a grupos locais para determinar a quais recursos esses usuários podem acessar. Você também pode importar usuários federados. O Tenant Manager inclui um usuário local predefinido, chamado "root".

Embora seja possível adicionar e remover usuários locais, você não pode remover o usuário raiz.

> Se o login único (SSO) estiver habilitado para seu sistema StorageGRID, os usuários locais não poderão fazer login no Tenant Manager ou na Tenant Management API, embora possam usar aplicativos cliente para acessar os recursos do tenant, com base nas permissões de grupo.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Permissão de acesso root".
- Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, você tiver revisado o fluxo de trabalho e as considerações para "clonagem de grupos de inquilinos e usuários" e estiver conectado à grid de origem do locatário.

#### Criar um usuário local

Você pode criar um usuário local e atribuí-lo a um ou mais grupos locais para controlar suas permissões de acesso.

Usuários do S3 que não pertencem a nenhum grupo não têm permissões de gerenciamento nem políticas de grupo do S3 aplicadas a eles. Esses usuários podem ter acesso ao bucket do S3 concedido por meio de uma política de bucket.

### Acesse o assistente de criação de usuário

**Passos**

1. Selecione **Gerenciamento de Acesso** > **Usuários**.

   Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, uma faixa azul indica que esta é a grid de origem do locatário. Quaisquer usuários locais que você criar nesta grid serão clonados para a outra grid na conexão.


2. Selecione **Criar usuário**.

### Insira as credenciais

**Passos**

1. Na etapa **Inserir credenciais do usuário**, preencha os seguintes campos.

| Campo | Descrição |
| --- | --- |
| Nome completo | O nome completo deste usuário, por exemplo, o nome e sobrenome de uma pessoa ou o nome de um aplicativo. |
| Nome de usuário | O nome que este usuário usará para fazer login. Os nomes de usuário devem ser únicos e não podem ser alterados.<br><br>**Observação**: Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, ocorrerá um erro de clonagem se o mesmo **Nome de usuário** já existir para o locatário na grid de destino. |
| Senha e confirmar senha | A senha que o usuário usará inicialmente ao fazer login. |
| Negar acesso | Selecione **Sim** para impedir que este usuário faça login na conta do tenant, mesmo que ele ainda pertença a um ou mais grupos.<br><br>Por exemplo, selecione **Sim** para suspender temporariamente a capacidade de um usuário de fazer login. |

2. Selecione **Continue**.

### Atribuir a grupos

**Passos**

1. Atribua o usuário a um ou mais grupos locais para determinar quais tarefas ele pode executar.

   Atribuir um usuário a grupos é opcional. Se preferir, você pode selecionar usuários ao criar ou editar grupos.

   Usuários que não pertencem a nenhum grupo não terão permissões de gerenciamento. As permissões são cumulativas. Usuários terão todas as permissões para todos os grupos aos quais pertencem. Veja "Permissões de gerenciamento de tenant".

2. Selecione **Criar usuário**.

   Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid** e você estiver na grid de origem do locatário, o novo usuário local será clonado para a grid de destino do locatário. **Sucesso** aparece como o **Status da clonagem** na seção Visão geral da página de detalhes do usuário.

3. Selecione **Concluir** para retornar à página de Usuários.

#### Visualizar ou editar usuário local

**Passos**

1. Selecione **Gerenciamento de Acesso** > **Usuários**.
2. Analise as informações fornecidas na página Usuários, que lista informações básicas para todos os usuários locais e federados desta conta de tenant.

   Se a conta do locatário tiver a permissão **Usar conexão de federação de grid** e você estiver visualizando o usuário na grid de origem do locatário:

- Uma mensagem no banner indica que, se você editar ou remover um usuário, suas alterações não serão sincronizadas com a outra grid.
- Conforme necessário, uma mensagem em banner indica se os usuários não foram clonados para o locatário na grade de destino. Você pode Tentar novamente uma clonagem de usuário que falhou.

3. Se você deseja alterar o nome completo do usuário:
   a. Selecione a caixa de seleção para o usuário.
   b. Selecione **Ações** > **Editar nome completo**.
   c. Digite o novo nome.
   d. Selecione **Salvar alterações**.
4. Se você deseja visualizar mais detalhes ou fazer edições adicionais, faça um dos seguintes procedimentos:
   - Selecione o nome de usuário.
   - Selecione a caixa de seleção do usuário e selecione **Ações** > **Exibir detalhes do usuário**.
5. Consulte a seção Visão geral, que exibe as seguintes informações para cada usuário:
   - Nome completo
   - Nome de usuário
   - Tipo de usuário
   - Acesso negado
   - Modo de acesso
   - Membros do grupo
   - Campos adicionais se a conta do locatário tiver a permissão **Usar conexão de federação de grid** e você estiver visualizando o usuário na grid de origem do locatário:
     - Status da clonagem, **Sucesso** ou **Falha**
     - Uma faixa azul indicando que, se você editar este usuário, suas alterações não serão sincronizadas com a outra grid.
6. Edite as configurações do usuário conforme necessário. Consulte Criar usuário local para detalhes sobre o que inserir.
   a. Na seção Visão geral, altere o nome completo selecionando o nome ou o ícone de edição .

      Você não pode alterar o nome de usuário.

   b. Na aba **Senha**, altere a senha do usuário e selecione **Salvar alterações**.
   c. Na guia **Acesso**, selecione **Não** para permitir que o usuário faça login ou selecione **Sim** para impedir que o usuário faça login. Em seguida, selecione **Salvar alterações**.
   d. Na guia **Chaves de acesso**, selecione **Criar chave** e siga as instruções para "criando chaves de acesso S3 para outro usuário".
   e. Na guia **Grupos**, selecione **Editar grupos** para adicionar o usuário a grupos ou remover o usuário de grupos. Em seguida, selecione **Salvar alterações**.
7. Confirme se você selecionou **Salvar alterações** para cada seção que você modificou.

#### Importar usuários federados

Você pode importar um ou mais usuários federados, até um máximo de 100 usuários, diretamente na página

Usuários.

**Passos**

1. Selecione **Gerenciamento de Acesso** > **Usuários**.
2. Selecione **Import federated users**.
3. Insira o UUID ou nome de usuário de um ou mais usuários federados.

   Para múltiplas entradas, adicione cada UUID ou nome de usuário em uma nova linha.

4. Selecione **Import**.

   Se a importação para o campo Usuários falhar para um ou mais usuários, execute as seguintes etapas:

   a. Expanda **Usuários não importados** e selecione **Copiar usuários**.
   b. Tente importar novamente selecionando **Anterior** e colando os usuários copiados na caixa de diálogo **Importar usuários federados**.

   Após fechar a caixa de diálogo **Importar usuários federados**, as informações dos usuários federados são exibidas na página Usuários para os usuários importados com sucesso.

#### Usuário local duplicado

Você pode duplicar um usuário local para criar um novo usuário mais rapidamente.

> Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid** e você duplicar um usuário da grid de origem do locatário, o usuário duplicado será clonado para a grid de destino do locatário.

**Passos**

1. Selecione **Gerenciamento de Acesso** > **Usuários**.
2. Selecione a caixa de seleção do usuário que você deseja duplicar.
3. Selecione **Ações** > **Duplicar usuário**.
4. Veja Criar usuário local para obter detalhes sobre o que inserir.
5. Selecione **Criar usuário**.

#### Tentar novamente clonar usuário

Para tentar novamente uma clonagem que falhou:

1. Selecione cada usuário que apresentar *(Falha na clonagem)* abaixo do nome de usuário.
2. Selecione **Ações** > **Clonar usuários**.
3. Veja o status da operação de clonagem na página de detalhes de cada usuário que você está clonando.

Para obter informações adicionais, consulte "Clonar grupos de tenants e usuários".

#### Excluir um ou mais usuários locais

Você pode excluir permanentemente um ou mais usuários locais que não precisam mais acessar a conta de locatário do StorageGRID.

Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid** e você excluir um usuário local, StorageGRID não excluirá o usuário correspondente no outro grid. Se você precisar manter essas informações sincronizadas, você deve excluir o mesmo usuário de ambos os grids.

Você deve usar a fonte de identidade federada para excluir usuários federados.

**Passos**

1. Selecione **Gerenciamento de Acesso** > **Usuários**.
2. Selecione a caixa de seleção para cada usuário que você deseja excluir.
3. Selecione **Ações** > **Excluir usuário** ou **Ações** > **Excluir usuários**.

   Uma caixa de diálogo de confirmação é exibida.

4. Selecione **Excluir usuário** ou **Excluir usuários**.

## Gerenciar chaves de acesso S3

### Gerencie as chaves de acesso S3 no StorageGRID

Cada usuário de uma conta de locatário S3 deve possuir uma chave de acesso para armazenar e recuperar objetos no sistema StorageGRID. Uma chave de acesso consiste em um ID de chave de acesso e uma chave de acesso secreta.

As chaves de acesso S3 podem ser gerenciadas da seguinte forma:

- Usuários que possuem a permissão **Gerenciar suas próprias credenciais do S3** podem criar ou remover suas próprias chaves de acesso ao S3.
- Usuários com permissão de **Root access** podem gerenciar as chaves de acesso da conta root do S3 e de todos os outros usuários. As chaves de acesso root fornecem acesso total a todos os buckets e objetos do tenant, a menos que sejam explicitamente desativadas por uma política de bucket.

StorageGRID suporta autenticação Signature Version 2 e Signature Version 4. O acesso entre contas não é permitido, a menos que seja explicitamente habilitado por uma política de bucket.

### Crie suas próprias chaves de acesso S3 no StorageGRID

Se você estiver usando um tenant do S3 e tiver as permissões necessárias, poderá criar suas próprias chaves de acesso ao S3. Você precisa de uma chave de acesso para acessar seus buckets e objetos.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Gerencie suas próprias credenciais do S3 ou permissão de acesso root".

**Sobre esta tarefa**

Você pode criar uma ou mais chaves de acesso S3 que permitem criar e gerenciar buckets para sua conta de tenant. Após criar uma nova chave de acesso, atualize o aplicativo com seu novo ID da chave de acesso e

chave de acesso secreta. Por segurança, não crie mais chaves do que você precisa e exclua as chaves que não estiver usando. Se você tiver apenas uma chave e ela estiver prestes a expirar, crie uma nova antes que a antiga expire e depois exclua a antiga.

Cada chave pode ter um tempo de expiração específico ou não ter tempo de expiração. Siga estas diretrizes para o tempo de expiração:

- Defina um prazo de validade para suas chaves para limitar seu acesso a um determinado período. Definir um prazo de validade curto pode ajudar a reduzir seu risco caso seu ID de acesso e chave de acesso secreta sejam expostos acidentalmente. Chaves expiradas são removidas automaticamente.
- Se o risco de segurança em seu ambiente for baixo e você não precisar criar novas chaves periodicamente, você não precisa definir um prazo de validade para suas chaves. Se você decidir criar novas chaves depois, exclua as chaves antigas manualmente.

> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para sua conta no Tenant Manager. Por esse motivo, proteja as chaves de acesso como você protegeria uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

**Passos**

1. Selecione **STORAGE (S3)** > **My access keys**.

   A página "Minhas chaves de acesso" é exibida e lista todas as chaves de acesso existentes.

2. Selecione **Criar chave**.
3. Faça um dos seguintes procedimentos:
   - Selecione **Não definir um tempo de expiração** para criar uma chave que não expirará. (Padrão)
   - Selecione **Definir um tempo de expiração** e defina a data e a hora de expiração.

     > A data de validade pode ser de no máximo cinco anos a partir da data atual. O tempo de validade pode ser de no mínimo um minuto a partir do tempo atual.

4. Selecione **Criar chave de acesso**.

   A caixa de diálogo "Baixar chave de acesso" é exibida, listando o ID da sua chave de acesso e a chave de acesso secreta.

5. Copie o ID da chave de acesso e a chave de acesso secreta para um local seguro ou selecione **Baixar .csv** para salvar um arquivo de planilha contendo o ID da chave de acesso e a chave de acesso secreta.

   > Não feche esta caixa de diálogo até que você tenha copiado ou baixado estas informações. Você não pode copiar ou baixar chaves depois que a caixa de diálogo for fechada.

6. Selecione **Concluir**.

   A nova chave está listada na página My access keys.

7. Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, você pode, opcionalmente, usar a API de gerenciamento de locatários para clonar manualmente as chaves de acesso S3 do locatário na grid de origem para o locatário na grid de destino. Consulte "Clonar chaves de acesso S3 usando a API".

### Visualize suas chaves de acesso S3 no StorageGRID

Se você estiver usando um tenant do S3 e tiver o "permissão apropriada", poderá visualizar uma lista das suas chaves de acesso do S3. Você pode classificar a lista por tempo de expiração, assim pode identificar quais chaves expirarão em breve. Se necessário, você pode "criar novas chaves" ou "excluir chaves" que não estiver mais usando.

> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para sua conta no Tenant Manager. Por esse motivo, proteja as chaves de acesso como você protegeria uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui a permissão "Gerenciar suas próprias credenciais do S3" "permissão".

**Passos**

1. Selecione **STORAGE (S3)** > **My access keys**.
2. Na página Minhas chaves de acesso, classifique as chaves de acesso existentes por **Data de expiração** ou **ID da chave de acesso**.
3. Conforme necessário, crie novas chaves ou exclua quaisquer chaves que você não esteja mais usando.

   Se você criar novas chaves antes que as chaves existentes expirem, poderá começar a usar as novas chaves sem perder temporariamente o acesso aos objetos da conta.

   As chaves expiradas são removidas automaticamente.

### Exclua suas próprias chaves de acesso S3 no StorageGRID

Se você estiver usando um tenant do S3 e tiver as permissões adequadas, poderá excluir suas próprias chaves de acesso do S3. Depois que uma chave de acesso é excluída, ela não pode mais ser usada para acessar os objetos e buckets na conta do tenant.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você tem o "Gerencie suas próprias permissões de credenciais do S3".

> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para sua conta no Tenant Manager. Por esse motivo, proteja as chaves de acesso como você protegeria uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

**Passos**

1. Selecione **STORAGE (S3)** > **My access keys**.
2. Na página My access keys, selecione a caixa de seleção de cada chave de acesso que você deseja remover.
3. Selecione a tecla **Delete**.
4. Na caixa de diálogo de confirmação, selecione **Delete key**.

   Uma mensagem de confirmação aparece no canto superior direito da página.

### Crie chaves de acesso S3 de outro usuário no StorageGRID

Se você estiver usando um tenant do S3 e tiver as permissões adequadas, você pode criar chaves de acesso do S3 para outros usuários, como aplicativos que precisam acessar buckets e objetos.

#### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Permissão de acesso root".

#### Sobre esta tarefa

Você pode criar uma ou mais chaves de acesso S3 para outros usuários para que eles possam criar e gerenciar buckets para a conta de locatário deles. Após criar uma nova chave de acesso, atualize o aplicativo com o novo ID da chave de acesso e a chave secreta de acesso. Por segurança, não crie mais chaves do que o usuário precisa e exclua as chaves que não estão sendo usadas. Se você tiver apenas uma chave e ela estiver prestes a expirar, crie uma nova antes que a antiga expire e depois exclua a antiga.

Cada chave pode ter um tempo de expiração específico ou não ter tempo de expiração. Siga estas diretrizes para o tempo de expiração:

- Defina um tempo de expiração para as chaves para limitar o acesso do usuário a um determinado período. Definir um tempo de expiração curto pode ajudar a reduzir o risco caso o ID da chave de acesso e a chave de acesso secreta sejam expostos acidentalmente. As chaves expiradas são removidas automaticamente.
- Se o risco de segurança em seu ambiente for baixo e você não precisar criar novas chaves periodicamente, você não precisa definir um prazo de validade para as chaves. Se você decidir criar novas chaves depois, exclua as chaves antigas manualmente.

> Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para esse usuário no Tenant Manager. Por esse motivo, proteja as chaves de acesso como você protegeria uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da conta e nunca as compartilhe com outros usuários.

#### Passos

1. Selecione **Gerenciamento de Acesso** > **Usuários**.
2. Selecione o usuário cujas chaves de acesso ao S3 você deseja gerenciar.

   A página de detalhes do usuário aparece.

3. Selecione **Chaves de acesso** e, em seguida, selecione **Criar chave**.

4. Faça um dos seguintes procedimentos:
   - Selecione **Não definir um tempo de expiração** para criar uma chave que não expira. (Padrão)
   - Selecione **Definir um tempo de expiração** e defina a data e a hora de expiração.

   > A data de validade pode ser de no máximo cinco anos a partir da data atual. O tempo de validade pode ser de no mínimo um minuto a partir do tempo atual.

5. Selecione **Criar chave de acesso**.

   A caixa de diálogo "Baixar chave de acesso" é exibida, listando o ID da chave de acesso e a chave de acesso secreta.

6. Copie o ID da chave de acesso e a chave de acesso secreta para um local seguro ou selecione **Baixar .csv** para salvar um arquivo de planilha contendo o ID da chave de acesso e a chave de acesso secreta.

   > Não feche esta caixa de diálogo até que você tenha copiado ou baixado estas informações. Você não pode copiar ou baixar chaves depois que a caixa de diálogo for fechada.

7. Selecione **Concluir**.

   A nova chave está listada na aba "Chaves de acesso" da página de detalhes do usuário.

8. Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, você pode, opcionalmente, usar a API de gerenciamento de locatários para clonar manualmente as chaves de acesso S3 do locatário na grid de origem para o locatário na grid de destino. Consulte "Clonar chaves de acesso S3 usando a API".

### Visualizar as chaves de acesso S3 de outro usuário no StorageGRID

Se você estiver usando um tenant do S3 e tiver as permissões apropriadas, pode visualizar as chaves de acesso do S3 de outro usuário. Você pode classificar a lista por tempo de expiração para determinar quais chaves expirarão em breve. Se necessário, você pode criar novas chaves e excluir as chaves que não estão mais em uso.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

> Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para esse usuário no Tenant Manager. Por esse motivo, proteja as chaves de acesso como você protegeria uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da conta e nunca as compartilhe com outros usuários.

**Passos**

1. Selecione **Gerenciamento de Acesso** > **Usuários**.
2. Na página Usuários, selecione o usuário cujas chaves de acesso ao S3 você deseja visualizar.
3. Na página Detalhes do usuário, selecione **Chaves de acesso**.
4. Classifique as chaves por **Tempo de expiração** ou **ID da chave de acesso**.

5. Conforme necessário, crie novas chaves e exclua manualmente as chaves que não estiverem mais em uso.

   Se você criar novas chaves antes que as chaves existentes expirem, o usuário poderá começar a usar as novas chaves sem perder temporariamente o acesso aos objetos na conta.

   As chaves expiradas são removidas automaticamente.

**Informações relacionadas**

- "Criar chaves de acesso S3 de outro usuário"
- "Excluir as chaves de acesso S3 de outro usuário"

### Excluir as chaves de acesso S3 de outro usuário no StorageGRID

Se você estiver usando um tenant do S3 e tiver as permissões apropriadas, poderá excluir as chaves de acesso do S3 de outro usuário. Depois que uma chave de acesso é excluída, ela não pode mais ser usada para acessar os objetos e buckets na conta do tenant.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

> Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para esse usuário no Tenant Manager. Por esse motivo, proteja as chaves de acesso como você protegeria uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da conta e nunca as compartilhe com outros usuários.

**Passos**

1. Selecione **Gerenciamento de Acesso** > **Usuários**.
2. Na página Usuários, selecione o usuário cujas chaves de acesso ao S3 você deseja gerenciar.
3. Na página Detalhes do usuário, selecione **Chaves de acesso** e, em seguida, marque a caixa de seleção para cada chave de acesso que você deseja excluir.
4. Selecione **Ações** > **Excluir chave selecionada**.
5. Na caixa de diálogo de confirmação, selecione **Delete key**.

   Uma mensagem de confirmação aparece no canto superior direito da página.

## Gerenciar buckets do S3

### Crie um bucket S3 do StorageGRID

Você pode usar o Gerenciador de Locatários para criar buckets S3 para dados de objetos.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".

- Você pertence a um grupo de usuários que possui acesso de root ou permissão para gerenciar todos os buckets "permissão". Essas permissões substituem as configurações de permissões nas políticas de grupo ou de bucket.

> As permissões para definir ou modificar as propriedades de bloqueio de objetos S3 de buckets ou objetos podem ser concedidas por "política de bucket ou política de grupo".

- Se você planeja habilitar o S3 Object Lock para um bucket, um administrador do grid habilitou a configuração global de S3 Object Lock para o sistema StorageGRID e você revisou os requisitos para buckets e objetos de S3 Object Lock.
- Se cada locatário tiver 5.000 buckets, cada Storage Node na grade terá um mínimo de 64 GB de RAM.

> Cada grid pode ter um máximo de 100.000 buckets, incluindo "buckets de branch".

#### Acesse o assistente

**Passos**

1. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione **Create bucket**.

#### Insira os detalhes

**Passos**

1. Insira os detalhes do bucket.

| Campo | Descrição |
| --- | --- |
| Nome do bucket | Um nome para o bucket que esteja em conformidade com estas regras:<br>• Deve ser único em cada sistema StorageGRID (e não apenas único dentro da conta do locatário).<br>• Deve ser compatível com DNS.<br>• Deve conter no mínimo 3 e no máximo 63 caracteres.<br>• Cada etiqueta deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens.<br>• Não devem constar pontos em solicitações no estilo de hospedagem virtual. Pontos podem causar problemas na verificação do certificado curinga do servidor.<br>Para obter mais informações, consulte o "Documentação da Amazon Web Services (AWS) sobre regras de nomenclatura de buckets".<br>**Observação**: Não é possível alterar o nome do bucket depois de criar o bucket. |

| Campo | Descrição |
| --- | --- |
| Região | A região do bucket.<br><br>O administrador do StorageGRID gerencia as regiões disponíveis. A região de um bucket pode afetar a política de proteção de dados aplicada aos objetos. Por padrão, todos os buckets são criados na região `us-east-1`. Se a região padrão estiver configurada para uma região diferente de `us-east-1`, essa outra região será selecionada inicialmente na lista suspensa.<br><br>**Observação**: Não é possível alterar a região depois de criar o bucket. |

2. Selecione **Continue**.

#### Gerenciar configurações

**Passos**

1. Opcionalmente, habilite o versionamento de objetos para o bucket.

   Habilite o versionamento de objetos se desejar armazenar todas as versões de cada objeto neste bucket. Você pode então recuperar versões anteriores de um objeto conforme necessário.

   Você deve habilitar o versionamento de objetos se:

   - O bucket será usado para replicação entre grids.
   - Você deseja criar um "bucket de branch" a partir deste bucket.

2. Se a configuração global de Bloqueio de Objetos S3 estiver ativada, opcionalmente ative o Bloqueio de Objetos S3 para o bucket armazenar objetos usando um modelo de gravação única e leitura múltipla (WORM).

   Habilite o S3 Object Lock para um bucket somente se você precisar manter os objetos por um período determinado, por exemplo, para atender a certos requisitos regulatórios. S3 Object Lock é uma configuração permanente que ajuda você a evitar que os objetos sejam excluídos ou sobrescritos por um período fixo ou indefinidamente.

   > Depois que a configuração de Bloqueio de Objetos do S3 é ativada para um bucket, ela não pode ser desativada. Qualquer pessoa com as permissões corretas pode adicionar objetos a esse bucket que não podem ser alterados. Você pode não conseguir excluir esses objetos nem o próprio bucket.

   Se você habilitar o S3 Object Lock para um bucket, o versionamento do bucket será ativado automaticamente.

3. Se você selecionou **Ativar S3 Object Lock**, opcionalmente ative a **retenção padrão** para este bucket.

   > O administrador do seu grid deve lhe dar permissão para "Use recursos específicos do S3 Object Lock".

   Quando a **Retenção padrão** está ativada, novos objetos adicionados ao bucket serão automaticamente protegidos contra exclusão ou sobrescrita. A configuração **Retenção padrão** não se aplica a objetos que possuem seus próprios períodos de retenção.

a. Se a **retenção padrão** estiver ativada, especifique um **modo de retenção padrão** para o bucket.

| Modo de retenção padrão | Descrição |
|---|---|
| Governança | • Usuários com a `s3:BypassGovernanceRetention` permissão podem usar o `x-amz-bypass-governance-retention: true` cabeçalho da solicitação para ignorar as configurações de retenção.<br>• Esses usuários podem excluir uma versão de objeto antes que a data de retenção seja atingida.<br>• Esses usuários podem aumentar, diminuir ou remover a retain-until-date de um objeto. |
| Conformidade | • O objeto não pode ser excluído até que sua retain-until-date seja atingida.<br>• A data de retenção do objeto pode ser aumentada, mas não pode ser diminuída.<br>• A data de retenção do objeto não pode ser removida até que essa data seja atingida.<br><br>**Nota**: O administrador da sua grid deve permitir que você use o modo de conformidade. |

b. Se a **retenção padrão** estiver ativada, especifique o **período de retenção padrão** para o bucket.

O **período de retenção padrão** indica por quanto tempo os novos objetos adicionados a este bucket devem ser retidos, a partir do momento em que são ingeridos. Especifique um valor menor ou igual ao período máximo de retenção para o tenant, conforme definido pelo administrador do grid.

Um período de retenção *máximo*, que pode ser um valor de 1 dia a 100 anos, é definido quando o administrador do grid cria o tenant. Quando você define um período de retenção *padrão*, ele não pode exceder o valor definido para o período de retenção máximo. Se necessário, solicite ao seu administrador do grid para aumentar ou diminuir o período de retenção máximo.

4. Opcionalmente, selecione **Ativar limite de capacidade**, insira um valor e selecione a unidade de capacidade.

O limite de capacidade é a capacidade máxima disponível para os objetos deste bucket. Este valor representa uma quantidade lógica (tamanho do objeto), não uma quantidade física (tamanho em disco).

Se nenhum limite for definido, a capacidade deste bucket é ilimitada. Consulte "Utilização do limite de capacidade" para mais informações.

5. Opcionalmente, selecione **Ativar limite de contagem de objetos**.

O limite de contagem de objetos é o número máximo de objetos que este bucket pode conter. Este valor representa uma quantidade lógica (contagem de objetos). Se nenhum limite for definido, a contagem de objetos é ilimitada.

6. Selecione **Create bucket**.

O bucket é criado e adicionado à tabela na página Buckets.

7. Opcionalmente, selecione **Acessar a página de detalhes do bucket** para "ver detalhes do bucket" e realizar configurações adicionais.

Você também pode "criar buckets de ramificação" conforme necessário.

### Veja os detalhes do bucket S3 no StorageGRID

Você pode visualizar os buckets na sua conta de locatário.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui as "Permissão de acesso root, gerenciar todos os buckets ou visualizar todos os buckets". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket.

**Passos**

1. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.

   A página Buckets é exibida.

2. Analise a tabela de resumo para cada bucket.

   Conforme necessário, você pode classificar as informações por qualquer coluna ou navegar para frente e para trás na lista.

   > Os valores de Contagem de Objetos, Espaço Utilizado e Uso exibidos são estimativas. Essas estimativas são afetadas pelo momento das ingestões, pela conectividade de rede e pelo status do nó. Se os buckets tiverem o versionamento ativado, as versões de objetos excluídos são incluídas na contagem de objetos.

   **Nome**
   O nome exclusivo do bucket, que não pode ser alterado.

   **Recursos ativados**
   Lista de funcionalidades habilitadas para o bucket.

   **Bloqueio de objeto S3**
   Indica se o S3 Object Lock está ativado para o bucket.

   Esta coluna só aparece se o S3 Object Lock estiver ativado para o grid. Esta coluna também exibe informações para quaisquer buckets legados Compliant.

   **Região**
   A região do bucket, que não pode ser alterada. Esta coluna está oculta por padrão.

   **Contagem de objetos**
   O número de objetos neste bucket. Se o versionamento estiver ativado nos buckets, as versões de objetos não atuais são incluídas neste valor.

   Quando objetos são adicionados ou excluídos, esse valor pode não ser atualizado imediatamente.

**Espaço utilizado**

O tamanho lógico de todos os objetos no bucket. O tamanho lógico não inclui o espaço real necessário para cópias replicadas ou com código de apagamento, nem para metadados de objetos.

Esse valor pode levar até 10 minutos para ser atualizado.

**Uso**

A porcentagem utilizada em relação ao limite de capacidade do bucket, caso tenha sido definido um.

O valor de utilização é baseado em estimativas internas e pode ser excedido em alguns casos. Por exemplo, StorageGRID verifica o limite de capacidade (se definido) quando um locatário inicia o upload de objetos e rejeita novas ingestões para este bucket se o locatário tiver excedido o limite de capacidade. No entanto, StorageGRID não leva em consideração o tamanho do upload atual ao determinar se o limite de capacidade foi excedido. Se objetos forem excluídos, um locatário pode ser impedido temporariamente de fazer upload de novos objetos para este bucket até que o uso do limite de capacidade seja recalculado. Os cálculos podem levar 10 minutos ou mais.

Este valor indica o tamanho lógico, não o tamanho físico necessário para armazenar os objetos e seus metadados.

**Capacidade**

Se definido, o limite de capacidade do bucket.

**Data de criação**

A data e a hora em que o bucket foi criado. Esta coluna está oculta por padrão.

3. Para visualizar os detalhes de um bucket específico, selecione o nome do bucket na tabela.
   a. Veja o resumo das informações na parte superior da página da web para confirmar os detalhes do bucket, como Region e Object count.
   b. Visualize as barras de utilização do limite de capacidade e do limite de contagem de objetos. Se a utilização estiver em 100% ou próxima de 100%, considere aumentar o limite ou excluir alguns objetos.
   c. Se necessário, selecione **Excluir objetos no bucket** e **Excluir bucket**.

Preste muita atenção aos avisos que aparecem ao selecionar cada uma dessas opções. Para obter mais informações, consulte:

- "Excluir todos os objetos em um bucket"
- "Excluir um bucket" (o bucket deve estar vazio)

   d. Visualize ou altere as configurações do bucket em cada uma das abas, conforme necessário.
      - **Console S3**: Visualize os objetos do bucket. Para obter mais informações, consulte "Use o console S3".
      - **Opções do bucket**: visualize ou altere as configurações de opções. Algumas configurações, como S3 Object Lock, não podem ser alteradas após a criação do bucket.
        - "Gerencie a consistência do bucket"
        - "Atualizações do último tempo de acesso"
        - "Limite de capacidade"
        - "Limite de contagem de objetos"

        - "Versionamento de objetos"
        - "Bloqueio de objeto S3"
        - "Retenção padrão do bucket"
        - "Gerencie a replicação entre grades" (se permitido ao inquilino)
    - **Serviços de plataforma**: "Gerenciar serviços de plataforma" (se permitido para o locatário)
    - **Acesso ao bucket**: visualize ou altere as configurações de opções. Você precisa ter permissões de acesso específicas.
        - Configure "CORS para buckets e objetos" para que o bucket e os objetos nele contidos fiquem acessíveis a aplicativos web em outros domínios.
        - "Controlar o acesso do usuário" para um bucket S3 e os objetos contidos nesse bucket.
    - **Ramos**: Veja a lista de buckets de ramos para o bucket. "Criar um novo bucket de branch ou gerenciar buckets de branch".

#### Saiba mais sobre os buckets de ramificação do StorageGRID

## Um bucket de ramificação fornece acesso a objetos em um bucket conforme eles existiam em um determinado momento.

Você cria um bucket de ramificação a partir de um bucket existente. Depois de criar um bucket de ramificação, o bucket original a partir do qual ele foi criado passa a ser chamado de *bucket base*. Além disso, você pode criar um bucket de ramificação a partir de outro bucket de ramificação.

Um bucket de ramificação fornece acesso a dados protegidos, mas não serve como backup. Para continuar protegendo os dados, use estes recursos nos buckets base:

- "Bloqueio de objeto S3"
- "Replicação entre grades" para buckets base
- "Políticas de bucket" para buckets versionados limpar versões antigas de objetos

Observe as seguintes características dos buckets de branch:

- Você pode acessar os objetos nos buckets de ramificação usando "Console S3 para baixar objetos".
- Quando os clientes acessam objetos em um bucket de ramificação, as "políticas de acesso" do bucket de ramificação, e não as políticas do bucket base, determinam se o acesso é concedido ou negado.
- Os objetos criados em um bucket base são avaliados com base em como "Regras do ILM" se aplicam ao bucket base. Os objetos criados em um bucket de ramificação são avaliados com base em como as regras do ILM se aplicam ao bucket de ramificação.
- A replicação entre grades não é suportada para buckets de ramificação.
- Os serviços de plataforma não são compatíveis com buckets de ramificação.

##### Exemplos de utilização de buckets de ramificação

- Você pode usar um bucket de ramificação para remover objetos corrompidos criando um bucket de ramificação a partir de um ponto no tempo anterior à ocorrência da corrupção e, em seguida, direcionando os aplicativos para o bucket de ramificação em vez do bucket base que contém objetos corrompidos.
- Você está salvando dados em um bucket versionado. Ocorreu uma vulnerabilidade acidental que causou a ingestão de muitos objetos indesejados após o tempo *T*. Você pode criar um bucket de ramificação para o

valor de tempo Antes, *T*, e redirecionar as operações do cliente para esse bucket de ramificação. Assim, somente os objetos ingeridos antes do tempo Antes, *T*, são expostos aos clientes.

#### Operações em objetos em buckets de branch

- Uma operação PUT de objeto em um bucket de branch cria um objeto no branch.
- Uma operação GET em um bucket de branch recupera um objeto da branch. Se o objeto não existir no bucket da branch, o objeto será recuperado do bucket base.
- A exclusão de objetos dos buckets de ramificação ocorre da seguinte forma:

| Operação | Alvo | Resultado | Visibilidade do objeto no bucket base | Visibilidade do objeto no bucket de branch |
|---|---|---|---|---|
| Excluir sem ID de versão | Bucket base | O marcador de exclusão é criado apenas para o bucket base | HEAD/GET retorna "Objeto não existe", mas versões específicas ainda podem ser acessadas | HEAD/GET retorna Objeto existe, e versões específicas ainda podem ser acessadas<br><br>O marcador de exclusão teria sido criado após o bucket do branch `beforeTime`. |
| Excluir com ID de versão | Bucket base | A versão específica do objeto é excluída tanto para o bucket base quanto para o bucket de branch. | HEAD/GET retorna "Versão do objeto não existe" | HEAD/GET retorna "Versão do objeto não existe" |
| Excluir sem ID de versão | Bucket de branch | O marcador de exclusão é criado apenas para o bucket de branch | HEAD/GET retorna o objeto (o objeto do bucket base não é afetado) | HEAD/GET retorna "Objeto não existe" |
| Excluir com ID de versão | Bucket de branch | A versão específica do objeto é excluída apenas para bucket de ramificação | HEAD/GET retorna uma versão específica do objeto (o objeto do bucket base não é afetado) | HEAD/GET retorna "Versão do objeto não existe" |

Consulte também "Como os objetos versionados do S3 são excluídos".

### Gerenciar buckets de ramificação do StorageGRID

Utilize o Tenant Manager para criar e visualizar detalhes dos buckets de filiais.

#### Antes de começar

- Você fez login no Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui acesso Root ou "Gerenciar todas as permissões de buckets". Essas permissões substituem as configurações de permissões nas políticas de grupo ou bucket.

- O bucket base a partir do qual você deseja criar uma ramificação tem "versionamento ativado".
- Você é o proprietário do bucket base.

**Sobre esta tarefa**

Observe as seguintes informações para os buckets de ramificação:

- As permissões para definir as propriedades de bloqueio de objetos S3 de buckets ou objetos podem ser concedidas por "política de bucket ou política de grupo".
- Se você suspender o versionamento no bucket base, o conteúdo do bucket base não ficará mais visível nos buckets de ramificação.

Depois de configurar e criar um bucket de branch, você não pode alterar a configuração.

#### Criar bucket de ramificação

**Passos**

1. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o bucket do qual você deseja criar uma ramificação (o "bucket base").
3. Na página de detalhes do bucket, selecione **Branches** > **Create branch bucket**.

   O botão **Criar bucket de branch** fica desativado se o bucket base não tiver versionamento ativado.

#### Insira os detalhes

**Passos**

1. Insira os detalhes do bucket da filial.

| Campo | Descrição |
| --- | --- |
| Nome do bucket da filial | Um nome para o bucket da branch que esteja em conformidade com estas regras:<br>• Deve ser único em cada sistema StorageGRID (e não apenas único dentro da conta do locatário).<br>• Deve ser compatível com DNS.<br>• Deve conter no mínimo 3 e no máximo 63 caracteres.<br>• Cada etiqueta deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens.<br>• Não devem constar pontos em solicitações no estilo de hospedagem virtual. Pontos podem causar problemas na verificação do certificado curinga do servidor.<br>Para obter mais informações, consulte o "Documentação da Amazon Web Services (AWS) sobre regras de nomenclatura de buckets".<br>**Observação**: Você não pode alterar o nome depois de criar o bucket da branch. |

| Campo | Descrição |
| --- | --- |
| Região (não pode ser modificada para buckets de ramificação) | A região do bucket do branch.<br><br>A região do bucket de ramificação deve corresponder à região do bucket base, portanto, esse campo está desativado para buckets de ramificação. |
| Antes do tempo | O horário limite para que as versões de objetos criadas no bucket base sejam acessíveis a partir do bucket de ramificação. O bucket de ramificação fornece acesso às versões de objetos criadas antes do horário Before.<br><br>O termo "antes" deve se referir a uma data e hora que já passaram. Não pode ser uma data futura. |
| Tipo de bucket de branch | • **Leitura e gravação**: Você pode adicionar ou excluir objetos ou versões de objetos no bucket de ramificação.<br>• **Somente leitura**: Você não pode modificar objetos no bucket de ramificação.<br><br>**Nota**: Você pode definir o tipo de bucket de branch como somente leitura apenas se o bucket de branch estiver vazio. Se o tipo de um bucket de branch existente estiver definido como leitura e gravação e você não tiver gravado nele, você pode alterar o tipo para somente leitura. |

2. Selecione **Continue**.

#### Gerenciar configurações de objetos (opcional)

As configurações de objeto para um bucket de ramificação não afetam as versões de objeto no bucket base.

**Passos**

1. Se a configuração global de Bloqueio de Objetos S3 estiver ativada, opcionalmente ative o Bloqueio de Objetos S3 para o bucket da ramificação. Para ativar o Bloqueio de Objetos S3, o bucket da ramificação deve ser um bucket de leitura e gravação.

   Habilite o S3 Object Lock para um bucket de ramificação somente se você precisar manter os objetos por um período fixo, por exemplo, para atender a determinados requisitos regulatórios. O S3 Object Lock é uma configuração permanente que ajuda você a impedir que os objetos sejam excluídos ou sobrescritos por um período fixo ou indefinidamente.

   > Depois que a configuração de Bloqueio de Objetos do S3 é ativada para um bucket, ela não pode ser desativada. Qualquer pessoa com as permissões corretas pode adicionar objetos ao bucket da ramificação que não podem ser alterados. Você pode não conseguir excluir esses objetos ou o próprio bucket da ramificação.

2. Se você selecionou **Ativar bloqueio de objeto S3**, opcionalmente ative a **retenção padrão** para o bucket da ramificação.

   > O administrador do seu grid deve lhe dar permissão para "Use recursos específicos do S3 Object Lock".

Quando a **Retenção padrão** está ativada, novos objetos adicionados ao bucket da ramificação serão automaticamente protegidos contra exclusão ou sobrescrita. A configuração **Retenção padrão** não se aplica a objetos que possuem seus próprios períodos de retenção.

a. Se a **retenção padrão** estiver ativada, especifique um **modo de retenção padrão** para o bucket de ramificação.

| Modo de retenção padrão | Descrição |
|---|---|
| Governança | • Usuários com a `s3:BypassGovernanceRetention` permissão podem usar o `x-amz-bypass-governance-retention: true` cabeçalho da solicitação para ignorar as configurações de retenção.<br>• Esses usuários podem excluir uma versão de objeto antes que a data de retenção seja atingida.<br>• Esses usuários podem aumentar, diminuir ou remover a retain-until-date de um objeto. |
| Conformidade | • O objeto não pode ser excluído até que sua retain-until-date seja atingida.<br>• A data de retenção do objeto pode ser aumentada, mas não pode ser diminuída.<br>• A data de retenção do objeto não pode ser removida até que essa data seja atingida.<br><br>**Nota**: O administrador da sua grid deve permitir que você use o modo de conformidade. |

b. Se a **retenção padrão** estiver ativada, especifique o **período de retenção padrão** para o bucket da ramificação.

   O **período de retenção padrão** indica por quanto tempo os novos objetos adicionados ao bucket da ramificação devem ser retidos, a partir do momento em que são ingeridos. Especifique um valor menor ou igual ao período máximo de retenção para o tenant, conforme definido pelo administrador do grid.

Um período de retenção *máximo*, que pode ser um valor de 1 dia a 100 anos, é definido quando o administrador do grid cria o tenant. Quando você define um período de retenção *padrão*, ele não pode exceder o valor definido para o período de retenção máximo. Se necessário, solicite ao seu administrador do grid para aumentar ou diminuir o período de retenção máximo.

3. Opcionalmente, selecione **Ativar limite de capacidade**.

   O limite de capacidade é a capacidade máxima disponível para o bucket da filial. Esse valor representa uma quantidade lógica (tamanho do objeto), não uma quantidade física (tamanho em disco).

   Se nenhum limite for definido, a capacidade do bucket de ramificação é ilimitada. Consulte "Utilização do limite de capacidade" para mais informações.

   > Essa configuração se aplica somente a objetos ingeridos diretamente no bucket de ramificação, e não a objetos que são visíveis do bucket base através do bucket de ramificação.

4. Opcionalmente, selecione **Ativar limite de contagem de objetos**.

   O limite de contagem de objetos é o número máximo de objetos que o bucket da ramificação pode conter. Esse valor representa uma quantidade lógica (contagem de objetos). Se nenhum limite for definido, a contagem de objetos é ilimitada.

   > Essa configuração se aplica somente a objetos ingeridos diretamente no bucket de ramificação, e não a objetos que são visíveis do bucket base através do bucket de ramificação.

5. Selecione **Create bucket**.

   O bucket da ramificação é criado e adicionado à tabela na página Buckets.

6. Opcionalmente, selecione **Acessar a página de detalhes do bucket** para "ver detalhes do bucket do branch" e realizar configurações adicionais.

   Na página de detalhes do bucket, algumas opções de configuração relacionadas à modificação de objetos estão desativadas para buckets somente leitura.

### Aplicar uma tag de política ILM a um bucket do StorageGRID

Escolha uma tag de política ILM para aplicar a um bucket com base nos seus requisitos de storage de objetos.

A política ILM controla onde os dados do objeto são armazenados e se eles são excluídos após um determinado período. O administrador do grid cria políticas ILM e as atribui a tags de política ILM quando várias políticas ativas estão em uso.

> Evite reatribuir a tag de política de um bucket com frequência. Caso contrário, podem ocorrer problemas de desempenho.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui as "Permissão de acesso root, gerenciar todos os buckets ou visualizar todos os buckets". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket.

**Passos**

1. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.

   A página "Buckets" é exibida. Conforme necessário, você pode classificar as informações por qualquer coluna ou navegar para frente e para trás na lista.

2. Selecione o nome do bucket ao qual você deseja atribuir uma tag de política ILM.

   Você também pode alterar a atribuição da tag de política ILM para um bucket que já possui uma tag atribuída.

Os valores de Contagem de Objetos e Espaço Utilizado exibidos são estimativas. Essas estimativas são afetadas pelo momento das ingestões, pela conectividade de rede e pelo status do nó. Se os buckets tiverem o versionamento ativado, as versões de objetos excluídos são incluídas na contagem de objetos.

3. Na guia Opções do Bucket, expanda o painel de opções de tag de política ILM. Este painel só aparece se o administrador do seu grid tiver habilitado o uso de tags de política personalizadas.
4. Leia a descrição de cada tag de política para determinar qual tag deve ser aplicada ao bucket.

Alterar a tag de política ILM para um bucket acionará a reavaliação do ILM de todos os objetos no bucket. Se a nova política retiver objetos por um período limitado, os objetos mais antigos serão excluídos.

5. Selecione o botão de opção correspondente à tag que você deseja atribuir ao bucket.
6. Selecione **Salvar alterações**. Uma nova tag de bucket S3 será definida no bucket com a chave `NTAP-SG-ILM-BUCKET-TAG` e o valor do nome da tag da política ILM.

Certifique-se de que seus aplicativos S3 não sobrescrevam ou excluam acidentalmente a nova tag do bucket. Se essa tag for omitida ao aplicar uma nova TagSet ao bucket, os objetos no bucket voltarão a ser avaliados de acordo com a política ILM padrão.

Defina e modifique as tags de política ILM usando apenas o Tenant Manager ou a API do Tenant Manager, onde a tag de política ILM é validada. Não modifique a `NTAP-SG-ILM-BUCKET-TAG` tag de política ILM usando a API S3 PutBucketTagging ou a API S3 DeleteBucketTagging.

Alterar a etiqueta de política atribuída a um bucket causa um impacto temporário no desempenho enquanto os objetos estão sendo reavaliados usando a nova política ILM.

### Gerenciar política de bucket do StorageGRID

Você pode controlar o acesso de usuários a um bucket do S3 e aos objetos contidos nesse bucket.

#### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui as "Permissão de acesso root". As permissões "Visualizar todos os buckets" e "Gerenciar todos os buckets" permitem apenas a visualização.
- Você verificou que o número necessário de Storage Nodes e sites está disponível. Se dois ou mais Storage Nodes não estiverem disponíveis em qualquer site, ou se um site não estiver disponível, as alterações nessas configurações podem não estar disponíveis.

#### Passos

1. Selecione **Buckets** e, em seguida, selecione o bucket que você deseja gerenciar.
2. Na página de detalhes do bucket, selecione **Acesso ao bucket** > **Política do bucket**.
3. Faça um dos seguintes procedimentos:
   - Defina uma política de bucket selecionando a caixa de seleção **Ativar política**. Em seguida, insira

uma string válida no formato JSON.

Cada política de bucket tem um limite de tamanho de 20.480 bytes.

- Modifique uma política existente editando a string.
- Desative uma política desmarcando a opção **Ativar política**.

Para obter informações detalhadas sobre políticas de buckets, incluindo sintaxe da linguagem e exemplos, consulte "Exemplos de políticas de bucket".

### Gerenciar a consistência dos buckets do StorageGRID

Os valores de consistência podem ser usados para especificar a disponibilidade das alterações nas configurações do bucket, assim como para equilibrar a disponibilidade dos objetos em um bucket e a consistência desses objetos entre diferentes Storage Nodes e sites. Você pode alterar os valores de consistência para que sejam diferentes dos valores padrão, permitindo que os aplicativos cliente atendam às suas necessidades operacionais.

#### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissões nas políticas de grupo ou bucket.

##### Diretrizes de consistência de bucket

A consistência do bucket é usada para determinar a consistência para aplicativos cliente que afetam objetos dentro desse bucket do S3. Em geral, você deve usar a consistência **Leitura após nova gravação** para seus buckets.

###### Alterar a consistência do bucket

Se a consistência **Read-after-new-write** não atender aos requisitos do aplicativo cliente, você pode alterá-la definindo a consistência do bucket ou usando o `Consistency-Control` cabeçalho. O `Consistency-Control` cabeçalho substitui a consistência do bucket.

> Ao alterar a consistência de um bucket, apenas os objetos ingeridos após a alteração terão a garantia de atender à nova configuração.

#### Passos

1. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do bucket na tabela.

   A página de detalhes do bucket é exibida.

3. Na aba **Opções do bucket**, selecione o ** acordeão.
4. Selecione uma consistência para as operações realizadas nos objetos deste bucket.
   - **Todos**: Oferece o mais alto nível de consistência. Todos os nós recebem os dados imediatamente ou a solicitação falhará.

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

5. Selecione **Save changes**.

#### O que acontece quando você altera as configurações do bucket

Os buckets possuem diversas configurações que afetam o comportamento dos buckets e dos objetos dentro desses buckets.

As configurações de bucket a seguir usam consistência **forte** por padrão. Se dois ou mais nós de armazenamento não estiverem disponíveis em qualquer site, ou se um site não estiver disponível, quaisquer alterações nessas configurações podem não estar disponíveis.

- "Exclusão de bucket vazio em segundo plano"
- "Último acesso"
- "Ciclo de vida do bucket"
- "Política de bucket"
- "Tagueamento de bucket"
- "Versionamento de bucket"
- "Bloqueio de objeto S3"
- "Criptografia do bucket"

> O valor de consistência para versionamento de buckets, S3 Object Lock e criptografia de buckets não pode ser definido para um valor que não seja fortemente consistente.

As seguintes configurações de bucket não utilizam consistência forte e possuem maior disponibilidade para alterações. Alterações nessas configurações podem levar algum tempo para surtirem efeito.

- "Configuração dos serviços da plataforma: notificação, replicação ou integração de pesquisa"
- "Configurar o CORS do StorageGRID para buckets e objetos"
- Alterar a consistência do bucket

> Se a consistência padrão usada ao alterar as configurações do bucket não atender aos requisitos do aplicativo cliente, você pode alterar a consistência usando o `Consistency-Control` cabeçalho para o "S3 API REST" ou usando as opções `reducedConsistency` ou `force` no "API de gerenciamento de inquilinos".

### Ativar ou desativar atualizações de tempo de acesso no StorageGRID

Quando os administradores de grid criam as regras de gerenciamento do ciclo de vida das informações (ILM) para um sistema StorageGRID, eles podem, opcionalmente, especificar que o tempo de acesso do objeto seja usado para determinar se ele deve ser movido para um local de armazenamento diferente. Se você estiver usando um tenant S3, pode aproveitar essas regras habilitando as atualizações do tempo de acesso para os objetos em um bucket S3.

Estas instruções se aplicam apenas a sistemas StorageGRID que incluam pelo menos uma regra de gerenciamento do ciclo de vida das informações (ILM) que use a opção **tempo de acesso** como filtro avançado ou como tempo de referência. Você pode ignorar estas instruções se seu sistema StorageGRID não incluir tal regra. Veja "Usar tempo de acesso nas regras do ILM" para obter detalhes.

#### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissões nas políticas de grupo ou bucket.

#### Sobre esta tarefa

**Último tempo de acesso** é uma das opções disponíveis para a instrução de posicionamento **tempo de referência** de uma regra de gerenciamento do ciclo de vida das informações. Definir o tempo de referência de uma regra como último tempo de acesso permite que os administradores da grid especifiquem que os objetos sejam colocados em determinados locais de armazenamento com base em quando esses objetos foram recuperados (lidos ou visualizados) pela última vez.

Por exemplo, para garantir que os objetos visualizados recentemente permaneçam em um armazenamento mais rápido, um administrador de grid pode criar uma regra ILM especificando o seguinte:

- Os objetos recuperados no último mês devem permanecer nos Storage Nodes locais.
- Os objetos que não foram recuperados no último mês devem ser movidos para um local externo.

Por padrão, as atualizações do tempo de acesso estão desativadas. Se o seu StorageGRID incluir uma regra de gerenciamento do ciclo de vida das informações (ILM) que use a opção **Último tempo de acesso** e você quiser que essa opção se aplique aos objetos neste bucket, será necessário ativar as atualizações do tempo de acesso para os buckets S3 especificados nessa regra.

> Atualizar o tempo de acesso quando um objeto é recuperado pode reduzir o desempenho do StorageGRID, especialmente para objetos pequenos.

Ocorre um impacto no desempenho com as atualizações do tempo de acesso mais recente porque o StorageGRID precisa executar essas etapas adicionais sempre que os objetos são recuperados:

- Atualize os objetos com novos carimbos de data e hora
- Adicione os objetos à fila ILM para que possam ser reavaliados em relação às regras e à política ILM atuais

A tabela resume o comportamento aplicado a todos os objetos no bucket quando o tempo de acesso está desativado ou ativado.

| Tipo de solicitação | Comportamento se tempo de acesso estiver desativado (padrão) | | Comportamento se o tempo de acesso estiver ativado | |
|---|---|---|---|---|
| | Último tempo de acesso atualizado? | Objeto adicionado à fila de avaliação do ILM? | Último tempo de acesso atualizado? | Objeto adicionado à fila de avaliação do ILM? |
| Solicitação para recuperar os metadados de um objeto quando uma operação HEAD é emitida | Não | Não | Não | Não |
| Solicitação para recuperar um objeto, sua lista de controle de acesso ou seus metadados | Não | Não | Sim | Sim |
| Solicitação para atualizar os metadados de um objeto | Sim | Sim | Sim | Sim |
| Solicitação para listar objetos ou versões de objetos | Não | Não | Não | Não |
| Solicitação para copiar um objeto de um bucket para outro | • Não, para a cópia original<br>• Sim, para a cópia de destino | • Não, para a cópia original<br>• Sim, para a cópia de destino | • Sim, para a cópia de origem<br>• Sim, para a cópia de destino | • Sim, para a cópia de origem<br>• Sim, para a cópia de destino |
| Solicitação para concluir um upload multipart | Sim, para o objeto montado | Sim, para o objeto montado | Sim, para o objeto montado | Sim, para o objeto montado |

**Passos**

1. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do bucket na tabela.

   A página de detalhes do bucket é exibida.

3. Na guia **Opções do bucket**, selecione o acordeão **Atualizações do tempo de último acesso**.
4. Ativar ou desativar as atualizações do tempo de acesso do último acesso.
5. Selecione **Save changes**.

### Alterar o versionamento de objeto para um bucket S3 no StorageGRID

Se você estiver usando um tenant do S3, você pode alterar o estado de versionamento dos buckets do S3.

#### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissões nas políticas de grupo ou bucket.
- Você verificou que o número necessário de Storage Nodes e sites está disponível. Se dois ou mais Storage Nodes não estiverem disponíveis em qualquer site, ou se um site não estiver disponível, as alterações nessas configurações podem não estar disponíveis.

#### Sobre esta tarefa

Você pode habilitar ou suspender o versionamento de objetos para um bucket. Depois de habilitar o versionamento para um bucket, ele não pode retornar a um estado não versionado. No entanto, você pode suspender o versionamento para o bucket.

- Desativado: o controle de versão nunca foi ativado
- Ativado: o versionamento está ativado
- Suspenso: o versionamento estava ativado anteriormente e está suspenso

Para obter mais informações, consulte o seguinte:

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

#### Passos

1. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do bucket na tabela.

   A página de detalhes do bucket é exibida.

3. Na aba **Opções do bucket**, selecione o acordeão **Controle de versão de objetos**.
4. Selecione um estado de versionamento para os objetos neste bucket.

   O versionamento de objetos deve permanecer ativado para um bucket usado para replicação entre grids. Se o S3 Object Lock ou a conformidade legada estiverem ativados, as opções de **Versionamento de objetos** ficam desativadas.

| Opção | Descrição |
| --- | --- |
| Ativar versionamento | Habilite o versionamento de objetos se desejar armazenar todas as versões de cada objeto neste bucket. Você pode então recuperar versões anteriores de um objeto conforme necessário.<br><br>Os objetos que já estavam no bucket serão versionados quando forem modificados por um usuário. |
| Suspender o versionamento | Suspenda o versionamento de objetos se você não quiser mais que novas versões de objetos sejam criadas. Você ainda pode recuperar quaisquer versões de objetos existentes. |

5. Selecione **Save changes**.

### Use S3 Object Lock para reter objetos no StorageGRID

Você pode usar o S3 Object Lock se os buckets e objetos precisarem atender aos requisitos regulamentares de retenção.

> O administrador da sua grid deve conceder permissão para você usar recursos específicos do S3 Object Lock.

#### O que é o bloqueio de objeto S3?

O recurso StorageGRID S3 Object Lock é uma solução de proteção de objetos equivalente ao S3 Object Lock do Amazon Simple Storage Service (Amazon S3).

Quando a configuração global de S3 Object Lock está habilitada para um sistema StorageGRID, uma conta de locatário S3 pode criar buckets com ou sem S3 Object Lock habilitado. Se um bucket tiver S3 Object Lock habilitado, o versionamento do bucket é obrigatório e é habilitado automaticamente.

Um bucket sem S3 Object Lock só pode conter objetos sem configurações de retenção especificadas. Nenhum objeto ingerido terá configurações de retenção.

Um bucket com S3 Object Lock pode conter objetos com e sem configurações de retenção especificadas por aplicativos cliente S3. Alguns objetos ingeridos terão configurações de retenção.

Um bucket com S3 Object Lock e retenção padrão configurada pode ter objetos carregados com configurações de retenção especificadas e novos objetos sem configurações de retenção. Os novos objetos usam a configuração padrão, pois a configuração de retenção não foi definida no nível do objeto.

Na prática, todos os objetos recém-ingeridos têm configurações de retenção quando a retenção padrão está configurada. Os objetos existentes sem configurações de retenção permanecem inalterados.

#### Modos de retenção

O recurso StorageGRID S3 Object Lock oferece suporte a dois modos de retenção para aplicar diferentes níveis de proteção aos objetos. Esses modos são equivalentes aos modos de retenção do Amazon S3.

- No modo de conformidade:
  - O objeto não pode ser excluído até que sua retain-until-date seja atingida.

    - A data de retenção do objeto pode ser aumentada, mas não pode ser diminuída.
    - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- Em modo de governança:
    - Usuários com permissão especial podem usar um cabeçalho de bypass em solicitações para modificar determinadas configurações de retenção.
    - Esses usuários podem excluir uma versão de objeto antes que a data de retenção seja atingida.
    - Esses usuários podem aumentar, diminuir ou remover a retain-until-date de um objeto.

#### Configurações de retenção para versões de objetos

Se um bucket for criado com o S3 Object Lock ativado, os usuários podem usar o aplicativo cliente S3 para, opcionalmente, especificar as seguintes configurações de retenção para cada objeto adicionado ao bucket:

- **Modo de retenção**: conformidade ou governança.
- **Data de retenção**: Se a data de retenção de uma versão de objeto for futura, o objeto pode ser recuperado, mas não pode ser excluído.
- **Guarda legal**: Aplicar uma guarda legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar aplicar uma guarda legal a um objeto relacionado a uma investigação ou disputa legal. Uma guarda legal não tem data de expiração, mas permanece em vigor até ser explicitamente removida. As guardas legais são independentes da data de retenção.

  > ⓘ Se um objeto estiver sob guarda legal, ninguém pode excluir o objeto, independentemente do seu modo de retenção.

  Para obter detalhes sobre as configurações do objeto, consulte "Use a API REST S3 para configurar o S3 Object Lock".

#### Configuração padrão de retenção para buckets

Se um bucket for criado com o S3 Object Lock ativado, você pode, opcionalmente, especificar as seguintes configurações padrão para o bucket:

- **Modo de retenção padrão**: conformidade ou governança.
- **Período de retenção padrão**: Por quanto tempo as novas versões de objetos adicionadas a este bucket devem ser retidas, a partir do dia em que forem adicionadas.

As configurações padrão do bucket se aplicam somente a novos objetos que não possuem suas próprias configurações de retenção. Objetos de bucket existentes não são afetados quando você adiciona ou altera essas configurações padrão.

Veja "Crie um bucket S3" e "Atualizar retenção padrão do S3 Object Lock".

##### Tarefas de bloqueio de objetos S3

As listas a seguir para administradores de grid e usuários locatários contêm as tarefas de alto nível para usar o recurso S3 Object Lock.

**Administrador de grid**

- Ative a configuração global de bloqueio de objetos S3 para todo o sistema StorageGRID.

- Garanta que as políticas de gerenciamento do ciclo de vida das informações (ILM) estejam em conformidade; ou seja, que atendam aos "Requisitos de buckets com S3 Object Lock ativado".
- Se necessário, permita que um locatário use o modo de Compliance como modo de retenção. Caso contrário, somente o modo de Governance é permitido.
- Se necessário, defina um período máximo de retenção para um tenant.

**Usuário locatário**

- Analise as considerações para buckets e objetos com S3 Object Lock.
- Se necessário, entre em contato com o administrador da grid para ativar a configuração global de S3 Object Lock e definir as permissões.
- Crie buckets com o S3 Object Lock ativado.
- Opcionalmente, configure as definições de retenção padrão para um bucket:
  - Modo de retenção padrão: Governança ou Conformidade, se permitido pelo administrador da grid.
  - Período de retenção padrão: deve ser menor ou igual ao período de retenção máximo definido pelo administrador da grade.
- Use o aplicativo cliente S3 para adicionar objetos e, opcionalmente, definir a retenção específica do objeto:
  - Modo de retenção. Governança ou Conformidade, se permitido pelo administrador da grid.
  - Data de retenção: deve ser menor ou igual ao permitido pelo período máximo de retenção definido pelo administrador do grid.

#### Requisitos para buckets com S3 Object Lock ativado

- Se a configuração global de S3 Object Lock estiver habilitada para o sistema StorageGRID, você pode usar o Tenant Manager, a Tenant Management API ou a S3 REST API para criar buckets com S3 Object Lock habilitado.
- Se você planeja usar o S3 Object Lock, precisa habilitar o S3 Object Lock ao criar o bucket. Você não pode habilitar o S3 Object Lock para um bucket existente.
- Quando o S3 Object Lock está habilitado para um bucket, o StorageGRID habilita automaticamente o versionamento para esse bucket. Você não pode desabilitar o S3 Object Lock nem suspender o versionamento para o bucket.
- Opcionalmente, você pode especificar um modo de retenção padrão e um período de retenção para cada bucket usando o Tenant Manager, a Tenant Management API ou a S3 REST API. As configurações de retenção padrão do bucket se aplicam somente a novos objetos adicionados ao bucket que não têm suas próprias configurações de retenção. Você pode substituir essas configurações padrão especificando um modo de retenção e uma data de retenção para cada versão do objeto no momento do upload.
- A configuração do ciclo de vida do bucket é compatível com buckets que possuem o S3 Object Lock ativado.
- CloudMirror A replicação não é suportada para buckets com S3 Object Lock ativado.

#### Requisitos para objetos em buckets com S3 Object Lock ativado

- Para proteger uma versão de objeto, você pode especificar configurações de retenção padrão para o bucket ou pode especificar configurações de retenção para cada versão de objeto. As configurações de retenção em nível de objeto podem ser especificadas usando o aplicativo cliente S3 ou a API REST.
- As configurações de retenção se aplicam a versões individuais de objetos. Uma versão de objeto pode ter tanto uma configuração de data de retenção quanto de guarda legal, uma delas, mas não a outra, ou

nenhuma das duas. Especificar uma data de retenção ou uma configuração de guarda legal para um objeto protege apenas a versão especificada na solicitação. Você pode criar novas versões do objeto, enquanto a versão anterior do objeto permanece bloqueada.

#### Ciclo de vida de objetos em buckets com S3 Object Lock ativado

Cada objeto salvo em um bucket com o S3 Object Lock ativado passa por estas etapas:

1. **Ingestão de objeto**

   Quando uma versão de objeto é adicionada a um bucket com o S3 Object Lock ativado, as configurações de retenção são aplicadas da seguinte forma:

   - Se as configurações de retenção forem especificadas para o objeto, as configurações em nível de objeto serão aplicadas. Quaisquer configurações padrão de bucket serão ignoradas.
   - Se nenhuma configuração de retenção for especificada para o objeto, as configurações padrão do bucket serão aplicadas, se existirem.
   - Se nenhuma configuração de retenção for especificada para o objeto ou o bucket, o objeto não estará protegido pelo S3 Object Lock.

   Se as configurações de retenção forem aplicadas, tanto o objeto quanto quaisquer metadados definidos pelo usuário S3 estarão protegidos.

2. **Retenção e exclusão de objetos**

   Várias cópias de cada objeto protegido são armazenadas pelo StorageGRID pelo período de retenção especificado. O número exato e o tipo de cópias de objeto, assim como os locais de armazenamento, são determinados pelas regras de conformidade nas políticas ILM ativas. Se um objeto protegido pode ser excluído antes de atingir sua data de retenção depende do seu modo de retenção.

   - Se um objeto estiver sob guarda legal, ninguém pode excluir o objeto, independentemente do seu modo de retenção.

#### Ainda posso gerenciar buckets legados compatíveis?

O recurso S3 Object Lock substitui o recurso Compliance que estava disponível em versões anteriores do StorageGRID. Se você criou buckets compatíveis usando uma versão anterior do StorageGRID, pode continuar gerenciando as configurações desses buckets; no entanto, não é mais possível criar novos buckets compatíveis. Para obter instruções, consulte "NetApp Knowledge Base: como gerenciar buckets legados compatíveis no StorageGRID 11.5".

### Atualizar retenção padrão do S3 Object Lock no StorageGRID

Se você habilitou o S3 Object Lock ao criar o bucket, pode editar o bucket para alterar as configurações de retenção padrão. Você pode habilitar (ou desabilitar) a retenção padrão e definir um modo de retenção padrão e um período de retenção.

#### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissões nas políticas de grupo ou bucket.
- O bloqueio de objetos S3 está habilitado globalmente para o seu sistema StorageGRID e você o habilitou

ao criar o bucket. Consulte "Use o S3 Object Lock para reter objetos".

**Passos**

1. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do bucket na tabela.

   A página de detalhes do bucket é exibida.

3. Na aba **Opções do bucket**, selecione o acordeão **S3 Object Lock**.
4. Opcionalmente, habilite ou desabilite a **retenção padrão** para este bucket.

   As alterações a esta configuração não se aplicam a objetos que já estejam no bucket nem a quaisquer objetos que possam ter seus próprios períodos de retenção.

5. Se a **retenção padrão** estiver ativada, especifique um **modo de retenção padrão** para o bucket.

| Modo de retenção padrão | Descrição |
|---|---|
| Governança | • Usuários com a `s3:BypassGovernanceRetention` permissão podem usar o `x-amz-bypass-governance-retention: true` cabeçalho da solicitação para ignorar as configurações de retenção.<br>• Esses usuários podem excluir uma versão de objeto antes que a data de retenção seja atingida.<br>• Esses usuários podem aumentar, diminuir ou remover a retain-until-date de um objeto. |
| Conformidade | • O objeto não pode ser excluído até que sua retain-until-date seja atingida.<br>• A data de retenção do objeto pode ser aumentada, mas não pode ser diminuída.<br>• A data de retenção do objeto não pode ser removida até que essa data seja atingida.<br><br>**Nota**: O administrador da sua grid deve permitir que você use o modo de conformidade. |

6. Se a **retenção padrão** estiver ativada, especifique o **período de retenção padrão** para o bucket.

   O **período de retenção padrão** indica por quanto tempo os novos objetos adicionados a este bucket devem ser retidos, a partir do momento em que são ingeridos. Especifique um valor menor ou igual ao período máximo de retenção para o tenant, conforme definido pelo administrador do grid.

   Um período de retenção *máximo*, que pode ser um valor de 1 dia a 100 anos, é definido quando o administrador do grid cria o tenant. Quando você define um período de retenção *padrão*, ele não pode exceder o valor definido para o período de retenção máximo. Se necessário, solicite ao seu administrador do grid para aumentar ou diminuir o período de retenção máximo.

7. Selecione **Save changes**.

### Configure CORS para buckets S3 no StorageGRID

Você pode configurar o compartilhamento de recursos entre origens (CORS) para um bucket do S3 se você quiser que esse bucket e os objetos nele sejam acessíveis a aplicativos web em outros domínios.

#### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Para solicitações de configuração CORS GET, você pertence a um grupo de usuários que possui "Gerenciar todos os buckets ou visualizar todos os buckets". Essas permissões substituem as configurações de permissões nas políticas de grupo ou bucket.
- Para solicitações de configuração CORS do tipo PUT, você pertence a um grupo de usuários que possui a permissão "Gerenciar todas as permissões de buckets". Essa permissão substitui as configurações de permissões nas políticas de grupo ou bucket.
- O "Permissão de acesso root" fornece acesso a todas as solicitações de configuração CORS.

#### Sobre esta tarefa

O compartilhamento de recursos de origem cruzada (CORS) é um mecanismo de segurança que permite que aplicativos web cliente em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket do S3 chamado `Images` para armazenar gráficos. Ao configurar o CORS para o bucket `Images`, você pode permitir que as imagens nesse bucket sejam exibidas no site `http://www.example.com`.

##### Habilite o CORS para um bucket

#### Passos

1. Utilize um editor de texto para criar o XML necessário. Este exemplo mostra o XML usado para habilitar o CORS em um bucket do S3. Especificamente:
    - Permite que qualquer domínio envie solicitações GET para o bucket
    - Permite que apenas o domínio `http://www.example.com` envie solicitações GET, POST e DELETE
    - Todos os cabeçalhos de solicitação são permitidos

```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

Para obter mais informações sobre o XML de configuração CORS, consulte "Documentação da Amazon Web Services (AWS): Guia do Usuário do Amazon Simple Storage Service".

2. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do bucket na tabela.

   A página de detalhes do bucket é exibida.

4. Na aba **Acesso ao bucket**, selecione o acordeão **Compartilhamento de recursos de origem cruzada (CORS)**.
5. Selecione a caixa de seleção **Enable CORS**.
6. Cole o XML de configuração CORS na caixa de texto.
7. Selecione **Save changes**.

#### Modificar configuração CORS

**Passos**

1. Atualize o XML de configuração CORS na caixa de texto ou selecione **Limpar** para começar de novo.
2. Selecione **Save changes**.

#### Desativar a configuração CORS

**Passos**

1. Desmarque a caixa de seleção **Ativar CORS**.
2. Selecione **Save changes**.

**Informações relacionadas**

"Configurar o CORS do StorageGRID para uma interface de gerenciamento"

### Excluir objetos de um bucket S3 do StorageGRID

Você pode usar o Gerenciador de Locatários para excluir os objetos em um ou mais buckets.

#### Considerações e requisitos

Antes de executar esses passos, observe o seguinte:

- Ao excluir objetos em um bucket, StorageGRID remove permanentemente todos os objetos e todas as versões de objetos em cada bucket selecionado de todos os nós e sites no seu sistema StorageGRID. StorageGRID também remove todos os metadados relacionados aos objetos. Você não poderá recuperar essas informações.
- Excluir todos os objetos em um bucket pode levar minutos, dias ou até semanas, dependendo do número de objetos, cópias de objetos e operações simultâneas.
- Se um bucket tiver "Bloqueio de objeto S3 ativado", ele poderá permanecer no estado **Excluindo objetos: somente leitura** por *anos*.

> Um bucket que utiliza o S3 Object Lock permanecerá no estado **Excluindo objetos: somente leitura** até que a data de retenção seja atingida para todos os objetos e quaisquer bloqueios legais sejam removidos.

- Enquanto os objetos estão sendo excluídos, o estado do bucket é **Excluindo objetos: somente leitura**. Nesse estado, você não pode adicionar novos objetos ao bucket.
- Quando todos os objetos forem excluídos, o bucket permanecerá em estado somente leitura. Você pode fazer uma das seguintes ações:
  - Retorne o bucket ao modo de escrita e reutilize-o para novos objetos
  - Exclua o bucket
  - Mantenha o bucket em modo somente leitura para reservar seu nome para uso futuro
- Se um bucket tiver o versionamento de objetos ativado, os marcadores de exclusão criados no StorageGRID 11.8 ou posterior podem ser removidos usando as operações "Excluir objetos no bucket".
- Se um bucket tiver o versionamento de objetos ativado, a operação de exclusão de objetos não removerá os marcadores de exclusão criados no StorageGRID 11.7 ou anterior. Consulte informações sobre como excluir objetos em um bucket em "Como os objetos versionados do S3 são excluídos".
- Se você usar "replicação entre grids", observe o seguinte:
  - Usar essa opção não exclui nenhum objeto do bucket na outra grid.
  - Se você selecionar esta opção para o bucket de origem, o alerta **Falha na replicação entre grades** será acionado se você adicionar objetos ao bucket de destino na outra grade. Se não for possível garantir que ninguém adicionará objetos ao bucket na outra grade, "desativar a replicação entre grids" para esse bucket antes de excluir todos os objetos do bucket.

#### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui a "Permissão de acesso root". Essa permissão substitui as configurações de permissões nas políticas de grupo ou bucket.

#### Passos

1. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.

A página Buckets é exibida e mostra todos os buckets S3 existentes.

2. Use o menu **Ações** ou a página de detalhes de um bucket específico.

**Menu de ações**

a. Selecione a caixa de seleção para cada bucket do qual você deseja excluir objetos.

b. Selecione **Actions** > **Delete objects in bucket**.

**Página de detalhes**

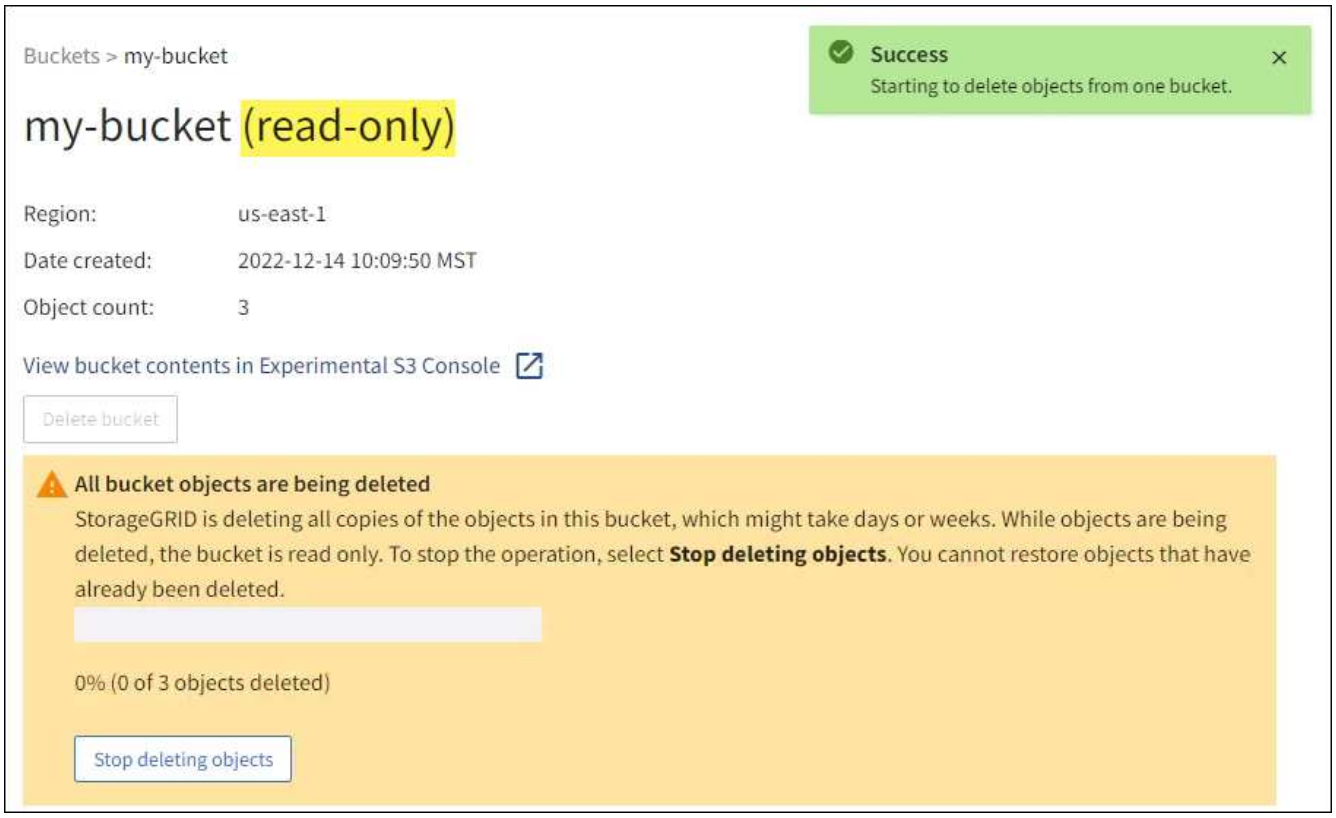
a. Selecione o nome do bucket para exibir seus detalhes.

b. Selecione **Excluir objetos no bucket**.

3. Quando a caixa de diálogo de confirmação aparecer, revise os detalhes, digite **Yes** e selecione **OK**.
4. Aguarde o início da operação de exclusão.

Após alguns minutos:

- Uma faixa amarela de status aparece na página de detalhes do bucket. A barra de progresso representa qual porcentagem de objetos foi excluída.
- **(somente leitura)** aparece após o nome do bucket na página de detalhes do bucket.
- **(Excluindo objetos: somente leitura)** aparece ao lado do nome do bucket na página Buckets.



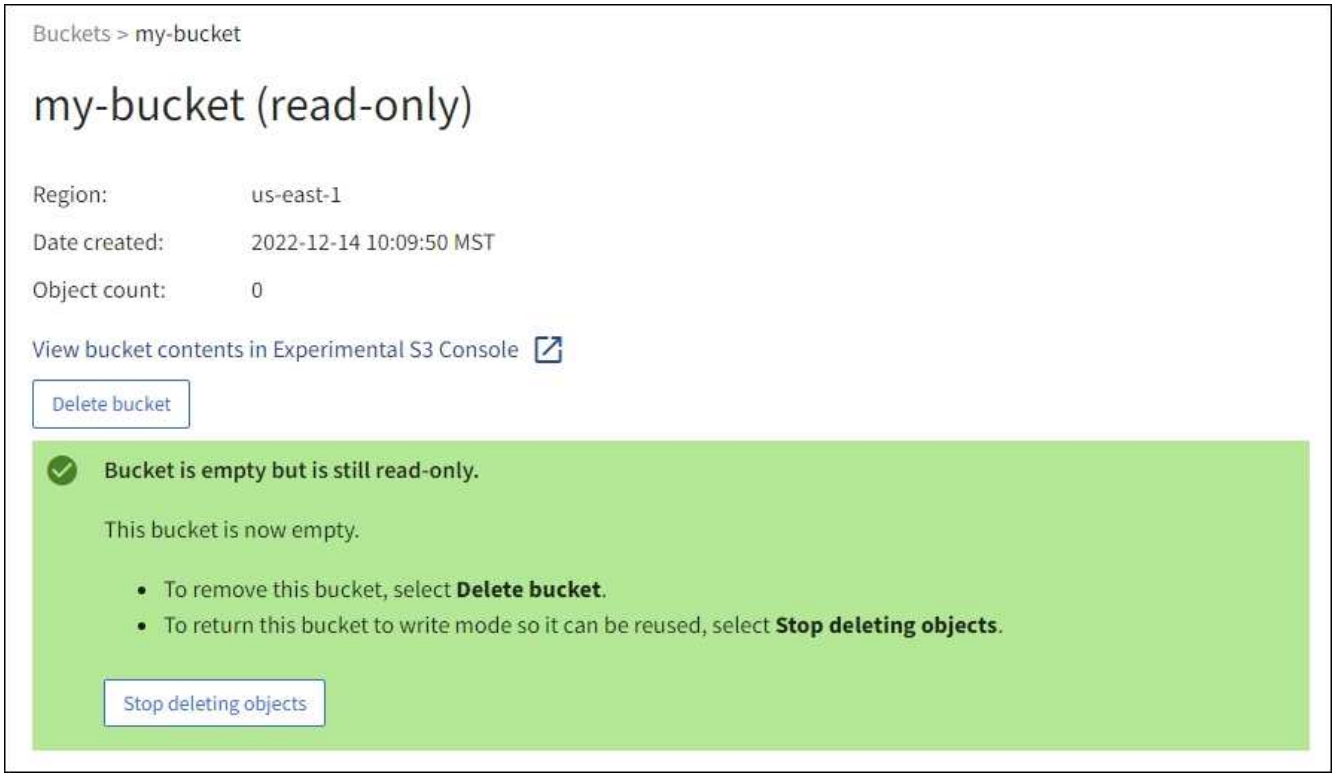

5. Se necessário, durante a execução da operação, selecione **Parar exclusão de objetos** para interromper o processo. Em seguida, opcionalmente, selecione **Excluir objetos no bucket** para retomar o processo.

Ao selecionar **Parar de excluir objetos**, o bucket retorna ao modo de gravação; no entanto, você não

pode acessar ou restaurar nenhum objeto que tenha sido excluído.

6. Aguarde a conclusão da operação.

   Quando o bucket estiver vazio, o banner de status é atualizado, mas o bucket permanece em modo somente leitura.




7. Faça um dos seguintes procedimentos:
   - Saia da página para manter o bucket em modo somente leitura. Por exemplo, você pode manter um bucket vazio em modo somente leitura para reservar o nome do bucket para uso futuro.
   - Exclua o bucket. Você pode selecionar **Excluir bucket** para excluir um único bucket ou retornar à página Buckets e selecionar **Ações** > **Excluir** buckets para remover mais de um bucket.

     Se você não conseguir excluir um bucket versionado após todos os objetos terem sido excluídos, os marcadores de exclusão podem permanecer. Para excluir o bucket, você deve remover todos os marcadores de exclusão restantes.

   - Retorne o bucket ao modo de gravação e, opcionalmente, reutilize-o para novos objetos. Você pode selecionar **Parar de excluir objetos** para um único bucket ou retornar à página Buckets e selecionar **Ação** > **Parar de excluir objetos** para mais de um bucket.

### Excluir um bucket S3 do StorageGRID

Você pode usar o Gerenciador de Locatários para excluir um ou mais buckets S3 que estejam vazios.

#### Antes de começar

- Você está conectado ao Tenant Manager usando um "navegador web compatível".

- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissões nas políticas de grupo ou bucket.
- Os buckets que você deseja excluir estão vazios. Se os buckets que você deseja excluir *não* estiverem vazios, "excluir objetos do bucket".

**Sobre esta tarefa**

Estas instruções descrevem como excluir um bucket do S3 usando o Tenant Manager. Você também pode excluir buckets do S3 usando o "API de gerenciamento de inquilinos" ou o "S3 API REST".

Não é possível excluir um bucket do S3 se ele contiver objetos, versões de objetos não atuais ou marcadores de exclusão. Para obter informações sobre como os objetos versionados do S3 são excluídos, consulte "Como os objetos são excluídos".

**Passos**

1. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.

   A página Buckets é exibida e mostra todos os buckets S3 existentes.

2. Use o menu **Ações** ou a página de detalhes de um bucket específico.

   **Menu de ações**

   a. Selecione a caixa de seleção para cada bucket que você deseja excluir.

   b. Selecione **Ações** > **Excluir buckets**.

   **Página de detalhes**

   a. Selecione o nome do bucket para exibir seus detalhes.

   b. Selecione **Excluir bucket**.

3. Quando a caixa de diálogo de confirmação aparecer, selecione **Sim**.

   StorageGRID confirma que cada bucket está vazio e, em seguida, exclui cada bucket. Essa operação pode levar alguns minutos.

   Se um bucket não estiver vazio, uma mensagem de erro será exibida. Você deve "exclua todos os objetos e quaisquer marcadores de exclusão no bucket" antes de poder excluí-lo.

**Use o S3 Console no StorageGRID**

## Você pode usar o Console do S3 para visualizar e gerenciar os objetos em um bucket do S3.

O S3 Console permite que você:

- Carregar, baixar, renomear, copiar, mover e excluir objetos
- Visualizar, reverter, baixar e excluir versões de objetos
- Pesquisar objetos por prefixo
- Gerenciar tags de objeto

- Exibir metadados do objeto
- Visualizar, criar, renomear, copiar, mover e excluir pastas

> O S3 Console oferece uma experiência de usuário aprimorada para os casos mais comuns. Ele não foi projetado para substituir as operações de CLI ou API em todas as situações.
>
> Se o uso do Console S3 resultar em operações demoradas demais (por exemplo, minutos ou horas), considere:
>
> - Reduzindo o número de objetos selecionados
> - Utilizando métodos não gráficos (API ou CLI) para acessar seus dados

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Se você deseja gerenciar objetos, você pertence a um grupo de usuários que possui a permissão de acesso Root. Alternativamente, você pertence a um grupo de usuários que possui a permissão Usar a guia Console do S3 e a permissão Exibir todos os buckets ou Gerenciar todos os buckets. Consulte "Permissões de gerenciamento de tenant".
- Uma política de Grupo ou Bucket do S3 foi configurada para o usuário. Consulte "Use políticas de acesso a buckets e grupos".
- Você conhece o ID da chave de acesso e a chave de acesso secreta do usuário. Opcionalmente, você tem um `.csv` arquivo contendo essas informações. Veja o "Instruções para criar chaves de acesso".

**Passos**

1. Selecione **Storage** > **Buckets** > ***nome do bucket***.
2. Selecione a aba S3 Console.
3. Cole o ID da chave de acesso e a chave de acesso secreta nos campos. Caso contrário, selecione **Carregar chaves de acesso** e selecione seu `.csv` arquivo.
4. Selecione **Sign in**.
5. A tabela de objetos do bucket é exibida. Você pode gerenciar os objetos conforme necessário.

**Informações adicionais**

- **Pesquisa por prefixo**: A função de pesquisa por prefixo busca apenas objetos que começam com uma palavra específica relativa à pasta atual. A pesquisa não inclui objetos que contenham a palavra em outros locais. Essa regra também se aplica a objetos dentro de pastas. Por exemplo, uma pesquisa por `folder1/folder2/somefile-` retornaria objetos que estão dentro da `folder1/folder2/` pasta e começam com a palavra `somefile-`.
- **Arrastar e soltar**: Você pode arrastar e soltar arquivos do gerenciador de arquivos do seu computador para o S3 Console. No entanto, não é possível carregar pastas.
- **Operações em pastas**: Ao mover, copiar ou renomear uma pasta, todos os objetos na pasta são atualizados um de cada vez, o que pode levar algum tempo.
- **Exclusão permanente quando o versionamento de buckets está desativado**: Quando você sobrescreve ou exclui um objeto em um bucket com o versionamento desativado, a operação é permanente. Consulte "Alterar o versionamento de objetos para um bucket".

# Gerenciar serviços da plataforma S3

## Serviços da plataforma S3

### Saiba mais sobre os serviços de plataforma para StorageGRID

Antes de implementar os serviços da plataforma, revise a visão geral e as considerações para o uso desses serviços.

Para obter informações sobre S3, consulte "Utilize a API REST S3".

### Visão geral dos serviços da plataforma

Os serviços da plataforma StorageGRID podem ajudar você a implementar uma estratégia de nuvem híbrida, permitindo o envio de notificações de eventos e cópias de objetos S3 e metadados de objetos para destinos externos.

Como o local de destino dos serviços de plataforma geralmente é externo à sua implementação do StorageGRID, os serviços de plataforma oferecem a você o poder e a flexibilidade que advêm do uso de recursos de storage externos, serviços de notificação e serviços de pesquisa ou análise para seus dados.

É possível configurar qualquer combinação de serviços de plataforma para um único bucket do S3. Por exemplo, você pode configurar tanto o "Serviço CloudMirror" quanto o "notificações" em um bucket do StorageGRID S3 para espelhar objetos específicos no Amazon Simple Storage Service (S3), enquanto envia uma notificação sobre cada objeto para um aplicativo de monitoramento de terceiros para ajudar você a acompanhar seus gastos com a AWS.

O uso dos serviços da plataforma deve ser habilitado para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a API de Gerenciamento do Grid.

### Como os serviços da plataforma são configurados

Os serviços da plataforma comunicam-se com endpoints externos que você configura usando o "Tenant Manager" ou o "API de gerenciamento de inquilinos". Cada endpoint representa um destino externo, como um bucket do StorageGRID S3, um bucket do Amazon Web Services, um tópico do Amazon SNS, um endpoint de webhook ou um cluster Elasticsearch hospedado localmente, na AWS ou em outro lugar.

Após criar um endpoint externo, você pode habilitar um serviço de plataforma para um bucket adicionando uma configuração XML ao bucket. A configuração XML identifica os objetos sobre os quais o bucket deve atuar, a ação que o bucket deve executar e o endpoint que o bucket deve usar para o serviço.

Você deve adicionar configurações XML separadas para cada serviço de plataforma que deseja configurar. Por exemplo:

- Se você deseja que todos os objetos cujas chaves começam com `/images` sejam replicados para um bucket do Amazon S3, você deve adicionar uma configuração de replicação ao bucket de origem.
- Se você também quiser enviar notificações quando esses objetos forem armazenados no bucket, você deve adicionar uma configuração de notificações.
- Se você deseja indexar os metadados desses objetos, deve adicionar a configuração de notificação de metadados usada para implementar a integração de pesquisa.

O formato do XML de configuração é regido pelas APIs REST do S3 usadas para implementar os serviços da plataforma StorageGRID:

| Serviço de plataforma | S3 API REST | Consulte |
| --- | --- | --- |
| CloudMirror replicação | • GetBucketReplication<br>• PutBucketReplication | • "CloudMirror replicação"<br>• "Operações em buckets" |
| Notificações | • GetBucketNotificationConfiguration<br>• PutBucketNotificationConfiguration | • "Notificações"<br>• "Operações em buckets" |
| Integração de pesquisa | • GET Configuração de notificação de metadados do bucket<br>• PUT Configuração de notificação de metadados do bucket | • "Integração de pesquisa"<br>• "Operações personalizadas do StorageGRID" |

**Considerações sobre o uso de serviços de plataforma**

| Consideração | Detalhes |
| --- | --- |
| Monitoramento do endpoint de destino | Você deve monitorar a disponibilidade de cada ponto de extremidade de destino. Se a conectividade com o ponto de extremidade de destino for perdida por um período prolongado e houver um grande acúmulo de solicitações, solicitações adicionais do cliente (como solicitações PUT) para o StorageGRID falharão. Você deve tentar novamente essas solicitações com falha quando o ponto de extremidade de destino estiver acessível. |
| Limitação de endpoint de destino | O software StorageGRID pode limitar as solicitações S3 recebidas para um bucket se a taxa de envio das solicitações exceder a taxa na qual o endpoint de destino pode recebê-las. A limitação só ocorre quando há um acúmulo de solicitações aguardando para serem enviadas ao endpoint de destino.<br><br>O único efeito visível é que as solicitações S3 recebidas levarão mais tempo para serem executadas. Se você começar a detectar um desempenho significativamente mais lento, você deve reduzir a taxa de ingestão ou usar um endpoint com maior capacidade. Se o acúmulo de solicitações continuar crescendo, as operações do cliente S3 (como solicitações PUT) eventualmente falharão.<br><br>As solicitações do CloudMirror têm mais probabilidade de serem afetadas pelo desempenho do endpoint de destino, porque normalmente envolvem mais transferência de dados do que as solicitações de integração de pesquisa ou de notificação de eventos. |

| Consideração | Detalhes |
| --- | --- |
| Garantias de ordenação | StorageGRID garante a ordem das operações em um objeto dentro de um site. Contanto que todas as operações em um objeto sejam realizadas no mesmo site, o estado final do objeto (para replicação) será sempre igual ao estado no StorageGRID.<br><br>StorageGRID faz o possível para ordenar as solicitações quando as operações são realizadas entre sites do StorageGRID. Por exemplo, se você gravar um objeto inicialmente no site A e depois sobrescrever o mesmo objeto no site B, não há garantia de que o objeto final replicado pelo CloudMirror para o bucket de destino seja o objeto mais recente. |
| Exclusões de objetos controladas por ILM | Para corresponder ao comportamento de exclusão do AWS CRR e do Amazon Simple Notification Service, solicitações de CloudMirror e de notificação de eventos não são enviadas quando um objeto no bucket de origem é excluído devido às regras do ILM do StorageGRID. Por exemplo, nenhuma solicitação de CloudMirror ou de notificação de evento é enviada se uma regra do ILM excluir um objeto após 14 dias.<br><br>Em contrapartida, as solicitações de integração de pesquisa são enviadas quando objetos são excluídos devido ao ILM. |
| Usando endpoints do Kafka | Para endpoints do Kafka, o TLS mútuo não é suportado. Como resultado, se você tiver `ssl.client.auth` definido como `required` na configuração do seu broker Kafka, isso pode causar problemas na configuração do endpoint do Kafka.<br><br>A autenticação dos endpoints do Kafka utiliza os seguintes tipos de autenticação. Esses tipos são diferentes daqueles usados para a autenticação de outros endpoints, como Amazon SNS, e exigem credenciais de nome de usuário e senha.<br><br>• SASL/PLAIN<br>• SASL/SCRAM-SHA-256<br>• SASL/SCRAM-SHA-512<br><br>**Nota:** As configurações de proxy de armazenamento configuradas não se aplicam aos endpoints dos serviços da plataforma Kafka. |

**Considerações sobre o uso do serviço de replicação CloudMirror**

| Consideração | Detalhes |
| --- | --- |
| Status de replicação | StorageGRID não suporta o `x-amz-replication-status` header. |

| Consideração | Detalhes |
| --- | --- |
| Tamanho do objeto | O tamanho máximo para objetos que podem ser replicados para um bucket de destino pelo serviço de replicação CloudMirror é de 5 TiB, que é o mesmo que o tamanho máximo de objeto *suportado*.<br><br>**Nota**: O tamanho máximo *recomendado* para uma única operação PutObject é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multipart. |
| Versionamento de buckets e IDs de versão | Se o bucket S3 de origem no StorageGRID tiver o versionamento ativado, você também deve ativar o versionamento para o bucket de destino.<br><br>Ao usar o versionamento, observe que a ordem das versões dos objetos no bucket de destino é feita da melhor maneira possível e não é garantida pelo serviço CloudMirror, devido a limitações no protocolo S3.<br><br>**Nota**: Os IDs de versão do bucket de origem no StorageGRID não estão relacionados aos IDs de versão do bucket de destino. |
| Marcação para versões de objetos | O serviço CloudMirror não replica nenhuma solicitação PutObjectTagging ou DeleteObjectTagging que forneça um ID de versão, devido a limitações do protocolo S3. Como os IDs de versão da origem e do destino não estão relacionados, não há como garantir que uma atualização de tag para um ID de versão específico seja replicada.<br><br>Em contrapartida, o serviço CloudMirror replica solicitações PutObjectTagging ou solicitações DeleteObjectTagging que não especificam um ID de versão. Essas solicitações atualizam as tags para a chave mais recente (ou a versão mais recente, se o bucket for versionado). Ingestões normais com tags (não atualizações de tags) também são replicadas. |
| Envios multipartes e `ETag`valores | Ao espelhar objetos que foram carregados usando um upload multipart, o serviço CloudMirror não preserva as partes. Como resultado, o `ETag` valor do objeto espelhado será diferente do `ETag` valor do objeto original. |
| Objetos criptografados com SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente) | O serviço CloudMirror não suporta objetos que são criptografados com SSE-C. Se você tentar ingerir um objeto no bucket de origem para a replicação CloudMirror e a solicitação incluir os cabeçalhos de solicitação SSE-C, a operação falhará. |
| Bucket com S3 Object Lock ativado | A replicação não é compatível para buckets de origem ou destino com o S3 Object Lock ativado. |

#### Saiba mais sobre o serviço de replicação StorageGRID CloudMirror

Você pode habilitar a replicação CloudMirror para um bucket do S3 se quiser que o StorageGRID replique objetos específicos adicionados ao bucket para um ou mais buckets de destino externos.

Por exemplo, você pode usar a replicação CloudMirror para espelhar registros específicos de clientes no Amazon S3 e, em seguida, aproveitar os serviços da AWS para realizar análises em seus dados.

> CloudMirror a replicação não é suportada se o bucket de origem tiver o S3 Object Lock ativado.

### CloudMirror e ILM

CloudMirror replication opera independentemente das políticas ILM ativas do grid. O serviço CloudMirror replica os objetos à medida que são armazenados no bucket de origem e os entrega ao bucket de destino o mais rápido possível. A entrega dos objetos replicados é acionada quando a ingestão do objeto é bem-sucedida.

### CloudMirror e replicação entre grades

CloudMirror replication apresenta importantes semelhanças e diferenças com o recurso de replicação entre grades. Consulte "Compare a replicação entre grades e a replicação CloudMirror".

### CloudMirror e buckets S3

CloudMirror A replicação geralmente é configurada para usar um bucket S3 externo como destino. No entanto, você também pode configurar a replicação para usar outra implantação do StorageGRID ou qualquer serviço compatível com S3.

#### Buckets existentes

Ao habilitar a replicação CloudMirror para um bucket existente, somente os novos objetos adicionados a esse bucket são replicados. Quaisquer objetos já existentes no bucket não são replicados. Para forçar a replicação de objetos existentes, você pode atualizar os metadados do objeto existente realizando uma cópia do objeto.

> Se você estiver usando a replicação CloudMirror para copiar objetos para um destino Amazon S3, esteja ciente de que o Amazon S3 limita o tamanho dos metadados definidos pelo usuário em cada cabeçalho de solicitação PUT a 2 KB. Se um objeto tiver metadados definidos pelo usuário maiores que 2 KB, esse objeto não será replicado.

#### Vários buckets de destino

Para replicar objetos de um único bucket para vários buckets de destino, especifique o destino para cada regra no XML de configuração de replicação. Você não pode replicar um objeto para mais de um bucket ao mesmo tempo.

#### Buckets versionados ou não versionados

Você pode configurar a replicação CloudMirror em buckets versionados ou não versionados. Os buckets de destino podem ser versionados ou não versionados. Você pode usar qualquer combinação de buckets versionados e não versionados. Por exemplo, você pode especificar um bucket versionado como destino para um bucket de origem não versionado, ou vice-versa. Você também pode replicar entre buckets não versionados.

### Exclusão, loops de replicação e eventos

#### Comportamento de exclusão

É o mesmo comportamento de exclusão do serviço Amazon S3, Cross-Region Replication (CRR). Excluir um objeto em um bucket de origem nunca exclui um objeto replicado no destino. Se ambos os buckets de origem e de destino forem versionados, o marcador de exclusão será replicado. Se o bucket de destino não for versionado, excluir um objeto no bucket de origem não replica o marcador de exclusão para o

bucket de destino nem exclui o objeto de destino.

**Proteção contra loops de replicação**

À medida que os objetos são replicados para o bucket de destino, StorageGRID os marca como "réplicas". Um bucket de destino do StorageGRID não replicará novamente os objetos marcados como réplicas, protegendo você de loops de replicação acidentais. Essa marcação de réplica é interna ao StorageGRID e não impede que você utilize o AWS CRR ao usar um bucket Amazon S3 como destino.

> ⓘ O cabeçalho personalizado usado para marcar uma réplica é `x-ntap-sg-replica`. Essa marcação impede um espelhamento em cascata. StorageGRID oferece suporte a um CloudMirror bidirecional entre duas grids.

**Eventos no bucket de destino**

A unicidade e a ordem dos eventos no bucket de destino não são garantidas. Mais de uma cópia idêntica de um objeto de origem pode ser entregue ao destino como resultado de operações realizadas para garantir o sucesso da entrega. Em casos raros, quando o mesmo objeto é atualizado simultaneamente a partir de dois ou mais sites StorageGRID diferentes, a ordem das operações no bucket de destino pode não corresponder à ordem dos eventos no bucket de origem.

#### Saiba mais sobre as notificações de eventos do StorageGRID para buckets do S3

Você pode habilitar a notificação de eventos para um bucket do S3 se quiser que o StorageGRID envie notificações sobre eventos específicos para um destino, cluster Kafka, endpoint de webhook ou Amazon Simple Notification Service.

Por exemplo, você pode configurar alertas para serem enviados aos administradores sobre cada objeto adicionado a um bucket, onde os objetos representam arquivos de log associados a um evento crítico do sistema.

As notificações de eventos são criadas no bucket de origem, conforme especificado na configuração de notificação, e entregues ao destino. Se um evento associado a um objeto for bem-sucedido, uma notificação sobre esse evento é criada e enfileirada para entrega.

A exclusividade e a ordem das notificações não são garantidas. Mais de uma notificação de um evento pode ser entregue ao destino como resultado de operações realizadas para garantir o sucesso da entrega. E como a entrega é assíncrona, a ordem temporal das notificações no destino não é garantida para corresponder à ordem dos eventos no bucket de origem, especialmente para operações originadas em diferentes sites do StorageGRID. Você pode usar a chave `sequencer` na mensagem do evento para determinar a ordem dos eventos para um objeto específico, conforme descrito na documentação do Amazon S3.

As notificações de eventos do StorageGRID seguem a API do Amazon S3, com algumas limitações.

- Os seguintes tipos de eventos são suportados:
  - s3:ObjectCreated:
  - s3:ObjectCreated:Put
  - s3:ObjectCreated:Post
  - s3:ObjectCreated:Copy
  - s3:ObjectCreated:CompleteMultipartUpload
  - s3:ObjectRemoved:
  - s3:ObjectRemoved:Excluir

- s3:ObjectRemoved:DeleteMarkerCreated
- s3:ObjectRestore:Post

- As notificações de eventos enviadas pelo StorageGRID usam o formato JSON padrão, mas não incluem algumas chaves e usam valores específicos para outras, conforme mostrado na tabela:

| Nome da chave | Valor do StorageGRID |
|---|---|
| eventSource | `sgws:s3` |
| awsRegion | *não incluído* |
| x-amz-id-2 | *não incluído* |
| arn | `urn:sgws:s3:::bucket_name` |

**Saiba mais sobre o serviço de integração de pesquisa do StorageGRID**

## Você pode habilitar a integração de pesquisa para um bucket do S3 se você quiser usar um serviço externo de pesquisa e análise de dados para os metadados dos seus objetos.

O serviço de integração de pesquisa é um serviço personalizado do StorageGRID que envia automaticamente e de forma assíncrona os metadados de objetos S3 para um endpoint de destino sempre que um objeto é criado ou excluído, ou quando seus metadados ou tags são atualizados. Você pode então usar ferramentas sofisticadas de pesquisa, análise de dados, visualização ou aprendizado de máquina fornecidas pelo serviço de destino para pesquisar, analisar e obter insights a partir dos dados dos seus objetos.

Por exemplo, você pode configurar seus buckets para enviar metadados de objetos S3 para um serviço Elasticsearch remoto. Em seguida, você pode usar o Elasticsearch para realizar buscas em todos os buckets e executar análises sofisticadas de padrões presentes nos metadados dos seus objetos.

Embora a integração com o Elasticsearch possa ser configurada em um bucket com o S3 Object Lock ativado, os metadados do S3 Object Lock (incluindo Retain Until Date e o status de Legal Hold) dos objetos não serão incluídos nos metadados enviados ao Elasticsearch.

> Como o serviço de integração de pesquisa faz com que metadados de objetos sejam enviados para um destino, seu XML de configuração é chamado de "XML de configuração de notificação de metadados". Este XML de configuração é diferente do "XML de configuração de notificação" usado para habilitar notificações de eventos.

**Integração de pesquisa e buckets S3**

Você pode habilitar o serviço de integração de pesquisa para qualquer bucket versionado ou não versionado. A integração de pesquisa é configurada associando um arquivo XML de configuração de notificação de metadados ao bucket, que especifica em quais objetos agir e o destino dos metadados do objeto.

As notificações de metadados são geradas na forma de um documento JSON nomeado com o nome do bucket, o nome do objeto e o ID da versão, se houver. Cada notificação de metadados contém um conjunto padrão de metadados do sistema para o objeto, além de todas as tags e metadados do usuário do objeto.

Para tags e metadados de usuário, StorageGRID envia 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 dinâmico de campos e para mapeamento de formatos de data. Você deve habilitar os mapeamentos dinâmicos de campos 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.

### Notificações de pesquisa

As notificações de metadados são geradas e enfileiradas para entrega sempre que:

- Um objeto é criado.
- Um objeto é excluído, inclusive quando objetos são excluídos como resultado da operação da política ILM da grid.
- Metadados ou tags dos objetos são adicionados, atualizados ou excluídos. O conjunto completo de metadados e tags é sempre enviado na atualização, não apenas os valores alterados.

Depois de adicionar o XML de configuração de notificação de metadados a um bucket, as notificações são enviadas para quaisquer novos objetos que você criar e para quaisquer objetos que você modificar atualizando seus dados, metadados de usuário ou tags. No entanto, as notificações não são enviadas para quaisquer objetos que já estavam no bucket. Para garantir que os metadados de objeto de todos os objetos no bucket sejam enviados ao destino, você deve fazer uma das seguintes ações:

- Configure o serviço de integração de pesquisa imediatamente após criar o bucket e antes de adicionar quaisquer objetos.
- Execute uma ação em todos os objetos já presentes no bucket que acionará o envio de uma mensagem de notificação de metadados para o destino.

### Serviço de integração de pesquisa e Elasticsearch

O serviço de integração de pesquisa do StorageGRID suporta um cluster Elasticsearch como destino. Assim como nos outros serviços da plataforma, o destino é especificado no endpoint cujo URN é usado no XML de configuração do serviço. Use o "NetApp Ferramenta de Matriz de Interoperabilidade" para determinar as versões suportadas do Elasticsearch.

## Gerenciar endpoints de serviços de plataforma

#### Configure os endpoints dos serviços da plataforma no StorageGRID

Antes de configurar um serviço de plataforma para um bucket, você deve configurar pelo menos um endpoint como destino para o serviço de plataforma.

O acesso aos serviços da plataforma é habilitado individualmente para cada locatário por um administrador do StorageGRID. Para criar ou usar um endpoint de serviços da plataforma, você deve ser um usuário do locatário com permissão de gerenciar endpoints ou acesso root, em um grid cuja rede tenha sido configurada para permitir que os Storage Nodes acessem recursos de endpoint externos. Para um único locatário, você pode configurar no máximo 500 endpoints de serviços da plataforma. Entre em contato com seu administrador do StorageGRID para obter mais informações.

### O que é um endpoint de serviços de plataforma?

Um endpoint de serviços de plataforma especifica as informações que StorageGRID precisa para acessar o destino externo.

Por exemplo, se você quiser replicar objetos de um bucket do StorageGRID para um bucket do Amazon S3, você cria um endpoint de serviços de plataforma que inclui as informações e credenciais que o StorageGRID precisa para acessar o bucket de destino na Amazon.

Cada tipo de serviço de plataforma requer seu próprio endpoint, portanto, você deve configurar pelo menos um endpoint para cada serviço de plataforma que planeja usar. Após definir um endpoint de serviço de plataforma, você usa o URN do endpoint como destino no XML de configuração usado para habilitar o serviço.

Você pode usar o mesmo endpoint como destino para mais de um bucket de origem. Por exemplo, você pode configurar vários buckets de origem para enviar metadados de objetos para o mesmo endpoint de integração de pesquisa, assim você pode realizar buscas em vários buckets. Você também pode configurar um bucket de origem para usar mais de um endpoint como destino, o que permite, por exemplo, enviar notificações sobre a criação de objetos para um tópico do Amazon Simple Notification Service (Amazon SNS) e notificações sobre a exclusão de objetos para um segundo tópico do Amazon SNS.

#### Pontos finais para replicação CloudMirror

StorageGRID suporta endpoints de replicação que representam buckets do S3. Esses buckets podem estar hospedados na Amazon Web Services, na mesma implantação do StorageGRID, em uma implantação remota do StorageGRID ou em outro serviço.

#### Pontos de extremidade para notificações

StorageGRID é compatível com Amazon SNS, Kafka e endpoints de webhook. Simple Queue Service (SQS) e AWS Lambda endpoints não são compatíveis.

Para endpoints do Kafka, o TLS mútuo não é suportado. Como resultado, se você tiver `ssl.client.auth` definido como `required` na configuração do seu broker Kafka, isso pode causar problemas na configuração do endpoint do Kafka.

#### Pontos de extremidade para o serviço de integração de pesquisa

StorageGRID oferece suporte a endpoints de integração de pesquisa que representam clusters Elasticsearch. Esses clusters Elasticsearch podem estar em um data center local, hospedados em uma nuvem AWS ou em outro local.

O endpoint de integração de pesquisa se refere a um índice e tipo específicos do Elasticsearch. Você deve criar o índice no Elasticsearch antes de criar o endpoint no StorageGRID, ou a criação do endpoint falhará. Você não precisa criar o tipo antes de criar o endpoint. O StorageGRID criará o tipo, se necessário, quando enviar os metadados do objeto para o endpoint.

#### Informações relacionadas

"Administrar StorageGRID"

##### Especifique um URN para um endpoint de serviços de plataforma StorageGRID

Ao criar um endpoint de serviços de plataforma, você deve especificar um Nome de Recurso Único (URN). Você usará o URN para referenciar o endpoint ao criar um arquivo XML de configuração para o serviço de plataforma. O URN de cada endpoint deve ser

único.

StorageGRID valida os endpoints dos serviços da plataforma à medida que você os cria. Antes de criar um endpoint de serviço da plataforma, confirme que o recurso especificado no endpoint existe e que ele pode ser acessado.

**Elementos URN**

O URN para um endpoint de serviços de plataforma deve começar com `arn:aws` ou `urn:mysite`, conforme mostrado a seguir:

- Se o serviço estiver hospedado na Amazon Web Services (AWS), use `arn:aws`
- Se o serviço estiver hospedado no Google Cloud Platform (GCP), use `arn:aws`
- Se o serviço estiver hospedado localmente, use `urn:mysite`

Por exemplo, se você estiver especificando o URN para um CloudMirror endpoint hospedado no StorageGRID, o URN pode começar com `urn:sgws`.

O próximo elemento do URN especifica o tipo de serviço de plataforma, da seguinte forma:

| Serviço | Tipo |
|---|---|
| CloudMirror replicação | `s3` |
| Notificações | `sns`, `kafka`, ou `webhook` |
| Integração de pesquisa | `es` |

Por exemplo, para continuar especificando o URN para um CloudMirror endpoint hospedado no StorageGRID, você adicionaria `s3` para obter `urn:sgws:s3`.

Para a maioria dos endpoints, o elemento final do URN identifica o recurso de destino específico no URI de destino, por exemplo, `sns-topic-name`.

Para endpoints de webhook, o recurso de destino é o próprio URI de destino.

| Serviço | Recurso específico |
|---|---|
| CloudMirror replicação | `bucket-name` |
| Notificações | `sns-topic-name` ou `kafka-topic-name`<br><br>**Nota:** Para endpoints de webhook, o elemento final do URN pode ser qualquer string, desde que o URN do endpoint seja único. |

| Serviço | Recurso específico |
| --- | --- |
| Integração de pesquisa | `domain-name/index-name/type-name`<br><br>**Observação:** Se o cluster Elasticsearch **não** estiver configurado para criar índices automaticamente, você deve criar o índice manualmente antes de criar o endpoint. |

#### URNs para serviços hospedados na AWS e no GCP

Para entidades AWS e GCP, o URN completo é um ARN AWS válido. Por exemplo:

- CloudMirror replicação:

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

- Notificações:

```
arn:aws:sns:region:account-id:topic-name
```

- Integração de pesquisa:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> Para um endpoint de integração de pesquisa da AWS, o `domain-name` deve incluir a string literal `domain/`, conforme mostrado aqui.

#### URNs para serviços hospedados localmente

Ao usar serviços hospedados localmente em vez de serviços em nuvem, você pode especificar o URN de qualquer forma que crie um URN válido e exclusivo, desde que o URN inclua os elementos obrigatórios na terceira e na última posição. Você pode deixar os elementos indicados como opcionais em branco ou especificá-los de qualquer forma que ajude você a identificar o recurso e tornar o URN exclusivo. Por exemplo:

- CloudMirror replicação:

```
urn:mysite:s3:optional:optional:bucket-name
```

Para um CloudMirror endpoint hospedado no StorageGRID, você pode especificar um URN válido que comece com `urn:sgws`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notificações:

  Especifique um endpoint do Amazon Simple Notification Service:

  ```
  urn:mysite:sns:optional:optional:sns-topic-name
  ```

  Especifique um endpoint do Kafka:

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-name
  ```

  Especifique um endpoint de webhook:

  ```
  urn:mysite:webhook:optional:optional:webhook-name
  ```

- Integração de pesquisa:

  ```
  urn:mysite:es:optional:optional:domain-name/index-name/type-name
  ```

  > Para endpoints de integração de pesquisa hospedados localmente, o `domain-name` elemento pode ser qualquer string, desde que o URN do endpoint seja único.

#### Crie um endpoint de serviços da plataforma StorageGRID

Você precisa criar pelo menos um endpoint do tipo correto antes de poder habilitar um serviço de plataforma.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Os serviços da plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você pertence a um grupo de usuários que possui o "Gerenciar endpoints ou permissão de acesso root".
- O recurso referenciado pelo endpoint dos serviços da plataforma foi criado:
  - CloudMirror replicação: bucket S3
  - Notificação de evento: tópico do Amazon Simple Notification Service (Amazon SNS), tópico do Kafka ou endpoint de webhook
  - Notificação de pesquisa: índice do Elasticsearch, caso o cluster de destino não esteja configurado para criar índices automaticamente.
- Você possui as informações sobre o recurso de destino:
  - Host e porta para o Identificador Uniforme de Recursos (URI)

Se você planeja usar um bucket hospedado em um sistema StorageGRID como endpoint para replicação CloudMirror, entre em contato com o administrador do grid para determinar os valores que você precisa inserir.

- Nome único de recurso (URN)

  "Especifique o URN para o endpoint dos serviços da plataforma"

- Credenciais de autenticação (se necessário):

  **Pontos de extremidade de integração de pesquisa**

  Para endpoints de integração de pesquisa, você pode usar as seguintes credenciais:

  - Chave de acesso: ID da chave de acesso e chave de acesso secreta
  - HTTP básico: nome de usuário e senha

  **CloudMirror endpoints de replicação**

  Para os endpoints de replicação CloudMirror, você pode usar as seguintes credenciais:

  - Chave de acesso: ID da chave de acesso e chave de acesso secreta
  - CAP (Portal de Acesso C2S): URL de credenciais temporárias, certificados de servidor e cliente, chaves de cliente e uma frase secreta opcional para a chave privada do cliente.

  **Pontos de extremidade do Amazon SNS**

  Para endpoints do Amazon SNS, você pode usar as seguintes credenciais:

  - Chave de acesso: ID da chave de acesso e chave de acesso secreta

  **Pontos de extremidade do Kafka**

  Para endpoints do Kafka, você pode usar as seguintes credenciais:

  - SASL/PLAIN: nome de usuário e senha
  - SASL/SCRAM-SHA-256: nome de usuário e senha
  - SASL/SCRAM-SHA-512: nome de usuário e senha

- Certificado de segurança (se for necessária a verificação do certificado)

- Se os recursos de segurança do Elasticsearch estiverem ativados, você terá o privilégio de monitorar o cluster para testes de conectividade e o privilégio de gravar índice ou ambos os privilégios de indexar e excluir índice para atualizações de documentos.

**Passos**

1. Selecione **ARMAZENAMENTO (S3)** > **Pontos de extremidade dos serviços da plataforma**. A página Pontos de extremidade dos serviços da plataforma é exibida.
2. Selecione **Criar endpoint**.
3. Insira um nome de exibição para descrever brevemente o endpoint e sua finalidade.

   O tipo de serviço de plataforma que o endpoint suporta é exibido ao lado do nome do endpoint quando ele é listado na página Endpoints, então você não precisa incluir essa informação no nome.

4. No campo **URI**, especifique o Identificador Único de Recurso (URI) do endpoint.

   Utilize um dos seguintes formatos:

   ```
   https://host:port
   http://host:port
   ```

   Se você não especificar uma porta, as seguintes portas padrão serão usadas:

   - Porta 443 para URIs HTTPS e porta 80 para URIs HTTP (maioria dos endpoints)
   - Porta 9092 para URIs HTTPS e HTTP (somente endpoints do Kafka)

   Por exemplo, o URI de um bucket hospedado no StorageGRID pode ser:

   ```
   https://s3.example.com:10443
   ```

   Neste exemplo, `s3.example.com` representa a entrada DNS para o IP virtual (VIP) do grupo de alta disponibilidade (HA) do StorageGRID, e `10443` representa a porta definida no endpoint do balanceador de carga.

   > Sempre que possível, você deve se conectar a um grupo de alta disponibilidade (HA) de nós de balanceamento de carga para evitar um ponto único de falha.

   Da mesma forma, o URI para um bucket hospedado na AWS pode ser:

   ```
   https://s3-aws-region.amazonaws.com
   ```

   > Se o endpoint for usado para o serviço de replicação CloudMirror, não inclua o nome do bucket no URI. Inclua o nome do bucket no campo **URN**.

5. Insira o Nome Único do Recurso (URN) para o endpoint.

   > Não é possível alterar o URN de um endpoint depois que ele foi criado.

6. Selecione **Continue**.
7. Selecione um valor para **Tipo de autenticação**.

   > Se você deseja autenticação para endpoints de webhook, configure Mutual Transport Layer Security (mTLS) em Etapa 9.

**Pontos de extremidade de integração de pesquisa**

Insira ou carregue as credenciais para um endpoint de integração de pesquisa.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

| Tipo de autenticação | Descrição | Credenciais |
|---|---|---|
| Anônimo | Fornece acesso anônimo ao destino. Funciona apenas para endpoints com segurança desativada. | Sem autenticação. |
| Chave de acesso | Utiliza credenciais no estilo AWS para autenticar conexões com o destino. | • ID da chave de acesso<br>• Chave de acesso secreta |
| HTTP básico | Utiliza um nome de usuário e senha para autenticar conexões com o destino. | • Nome de usuário<br>• Senha |

**CloudMirror endpoints de replicação**

Insira ou carregue as credenciais para um ponto de extremidade de replicação CloudMirror.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

| Tipo de autenticação | Descrição | Credenciais |
|---|---|---|
| Anônimo | Fornece acesso anônimo ao destino. Funciona apenas para endpoints com segurança desativada. | Sem autenticação. |
| Chave de acesso | Utiliza credenciais no estilo AWS para autenticar conexões com o destino. | • ID da chave de acesso<br>• Chave de acesso secreta |
| CAP (Portal de Acesso C2S) | Utiliza certificados e chaves para autenticar conexões com o destino. | • URL de credenciais temporárias<br>• Certificado CA do servidor (upload de arquivo PEM)<br>• Certificado do cliente (upload de arquivo PEM)<br>• Chave privada do cliente (upload de arquivo PEM, formato criptografado OpenSSL ou formato de chave privada não criptografada)<br>• Senha da chave privada do cliente (opcional) |

**Pontos de extremidade do Amazon SNS**

Insira ou carregue as credenciais para um endpoint do Amazon SNS.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

| Tipo de autenticação | Descrição | Credenciais |
|---|---|---|
| Anônimo | Fornece acesso anônimo ao destino. Funciona apenas para endpoints com segurança desativada. | Sem autenticação. |
| Chave de acesso | Utiliza credenciais no estilo AWS para autenticar conexões com o destino. | • ID da chave de acesso<br>• Chave de acesso secreta |

**Pontos de extremidade do Kafka**

Insira ou carregue as credenciais para um endpoint do Kafka.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

| Tipo de autenticação | Descrição | Credenciais |
|---|---|---|
| Anônimo | Fornece acesso anônimo ao destino. Funciona apenas para endpoints com segurança desativada. | Sem autenticação. |
| SASL/PLAIN | Utiliza um nome de usuário e senha em texto simples para autenticar conexões com o destino. | • Nome de usuário<br>• Senha |
| SASL/SCRAM-SHA-256 | Utiliza um nome de usuário e senha usando um protocolo de desafio-resposta e hash SHA-256 para autenticar conexões com o destino. | • Nome de usuário<br>• Senha |
| SASL/SCRAM-SHA-512 | Utiliza um nome de usuário e senha usando um protocolo de desafio-resposta e hash SHA-512 para autenticar conexões com o destino. | • Nome de usuário<br>• Senha |

Selecione **Usar autenticação tomada por delegação** se o nome de usuário e a senha forem derivados de um token de delegação obtido de um cluster Kafka.

8. Selecione **Continue**.
9. Selecione um botão de opção para **Verificar certificados** para escolher como a conexão TLS com o endpoint é verificada.

**A maioria dos endpoints**

Verifique a conexão TLS para integração de pesquisa, CloudMirror replication, Amazon SNS ou endpoints Kafka.

| Tipo de verificação de certificado | Descrição |
|---|---|
| TLS | Valida o certificado do servidor para conexões TLS com o recurso de endpoint. |
| Desabilitado | A verificação de certificado está desativada. Esta opção não é segura. |
| Use um certificado CA personalizado | O certificado CA personalizado é usado para verificar a identidade do servidor ao conectar-se ao endpoint. |
| Use o certificado CA do sistema operacional | Utilize o certificado padrão da Autoridade de Certificação (CA) do Grid instalado no sistema operacional para proteger as conexões. |

**Apenas endpoints de webhook**

Verifique a conexão TLS para os endpoints do webhook.

| Tipo de verificação de certificado | Descrição |
|---|---|
| TLS | Valida o certificado do servidor para conexões TLS com o recurso de endpoint. |
| mTLS | Valida os certificados do cliente e do servidor para conexões TLS mútuas com o recurso de endpoint. |
| Desabilitado | A verificação de certificado está desativada. Esta opção não é segura. |
| Use um certificado CA personalizado | O certificado CA personalizado é usado para verificar a identidade do servidor ao conectar-se ao endpoint. |

Ao selecionar **mTLS**, essas opções ficam disponíveis.

| Tipo de verificação de certificado | Descrição |
|---|---|
| Não verificar o certificado do servidor | Desativa a verificação do certificado do servidor, o que significa que a identidade do servidor não é verificada. Esta opção não é segura. |
| Certificado do cliente | O certificado do cliente é usado para verificar a identidade do cliente ao se conectar ao endpoint. |

| Tipo de verificação de certificado | Descrição |
| --- | --- |
| Chave privada do cliente | A chave privada do certificado do cliente. Se criptografada, deve usar o formato tradicional PKCS #1 (o formato PKCS #8 não é suportado). |
| Senha da chave privada do cliente | A senha para descriptografar a chave privada do cliente. Se a chave privada não estiver criptografada, deixe este campo em branco. |

10. Selecione **Test and create endpoint**.
    - Uma mensagem de sucesso é exibida se o endpoint puder ser acessado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada site.
    - Uma mensagem de erro aparece se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **Retornar aos detalhes do endpoint** e atualize as informações. Depois, selecione **Testar e criar endpoint**.

> ⓘ A criação do endpoint falha se os serviços da plataforma não estiverem habilitados para sua conta de locatário. Entre em contato com o administrador do StorageGRID.

Após configurar um endpoint, você pode usar seu URN para configurar um serviço de plataforma.

**Informações relacionadas**

- "Especifique o URN para o endpoint dos serviços da plataforma"
- "Configurar a replicação CloudMirror"
- "Configurar notificações de eventos"
- "Configurar serviço de integração de pesquisa"

#### Teste a conexão para um endpoint de serviços de plataforma StorageGRID

Caso a conexão com um serviço da plataforma tenha sido alterada, você pode testar a conexão com o endpoint para validar se o recurso de destino existe e se pode ser acessado usando as credenciais que você especificou.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Gerenciar endpoints ou permissão de acesso root".

**Sobre esta tarefa**

StorageGRID não valida se as credenciais possuem as permissões corretas.

**Passos**

1. Selecione **STORAGE (S3)** > **Pontos de extremidade de serviços da plataforma**.

   A página de endpoints dos serviços da plataforma é exibida e mostra a lista de endpoints dos serviços da plataforma que já foram configurados.

2. Selecione o endpoint cuja conexão você deseja testar.

   A página de detalhes do endpoint é exibida.

3. Selecione **Test connection**.
   - Uma mensagem de sucesso é exibida se o endpoint puder ser acessado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada site.
   - Uma mensagem de erro é exibida se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **Configuração** e atualize as informações. Em seguida, selecione **Testar e salvar alterações**.

#### Editar um endpoint de serviços de plataforma no StorageGRID

Você pode editar a configuração de um endpoint de serviços da plataforma para alterar seu nome, URI ou outros detalhes. Por exemplo, pode ser necessário atualizar credenciais expiradas ou alterar a URI para apontar para um índice de backup do Elasticsearch para failover. Você não pode alterar o URN de um endpoint de serviços da plataforma.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Gerenciar endpoints ou permissão de acesso root".

**Passos**

1. Selecione **STORAGE (S3)** > **Pontos de extremidade de serviços da plataforma**.

   A página de endpoints dos serviços da plataforma é exibida e mostra a lista de endpoints dos serviços da plataforma que já foram configurados.

2. Selecione o endpoint que você deseja editar.

   A página de detalhes do endpoint é exibida.

3. Selecione **Configuração**.
4. Conforme necessário, altere a configuração do endpoint.

   > Não é possível alterar o URN de um endpoint depois que ele foi criado.

   a. Para alterar o nome de exibição do endpoint, selecione o ícone de edição .
   b. Altere o URI conforme necessário.
   c. Se necessário, altere o tipo de autenticação.
      - Para autenticação de Access Key, altere a chave conforme necessário selecionando **Editar chave S3** e colando um novo access key ID e secret access key. Se você precisar cancelar suas alterações, selecione **Reverter edição da chave S3**.
      - Para autenticação CAP (C2S Access Portal), altere a URL das credenciais temporárias ou a senha opcional da chave privada do cliente e carregue novos arquivos de certificado e chave, conforme necessário.

> A chave privada do cliente deve estar no formato criptografado OpenSSL ou no formato de chave privada não criptografada.

d. Conforme necessário, altere o método para verificar certificados.

5. Selecione **Test and save changes**.
   - Uma mensagem de sucesso é exibida se o endpoint puder ser acessado usando as credenciais especificadas. A conexão com o endpoint é verificada a partir de um nó em cada site.
   - Uma mensagem de erro será exibida se a validação do endpoint falhar. Modifique o endpoint para corrigir o erro e, em seguida, selecione **Test and save changes**.

#### Excluir um endpoint de serviços da plataforma StorageGRID

Você pode excluir um endpoint se não quiser mais usar o serviço de plataforma associado.

**Antes de começar**

- Você está conectado ao Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Gerenciar endpoints ou permissão de acesso root".

**Passos**

1. Selecione **STORAGE (S3)** > **Pontos de extremidade de serviços da plataforma**.

   A página de endpoints dos serviços da plataforma é exibida e mostra a lista de endpoints dos serviços da plataforma que já foram configurados.

2. Selecione a caixa de seleção para cada endpoint que você deseja excluir.

> Se você excluir um endpoint de serviços de plataforma que esteja em uso, o serviço de plataforma associado será desativado para qualquer bucket que use esse endpoint. Quaisquer solicitações que ainda não tenham sido concluídas serão descartadas. Novas solicitações continuarão sendo geradas até que você altere a configuração do seu bucket para não referenciar mais o URN excluído. StorageGRID reportará essas solicitações como erros irrecuperáveis.

3. Selecione **Ações** > **Excluir endpoint**.

   Uma mensagem de confirmação é exibida.

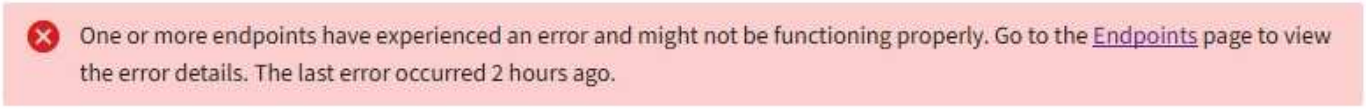
4. Selecione **Excluir endpoint**.

#### Solucione erros de endpoint dos serviços da plataforma StorageGRID

Se ocorrer um erro quando StorageGRID tentar se comunicar com um endpoint de serviços da plataforma, uma mensagem será exibida no painel. Na página Endpoints de serviços da plataforma, a coluna Último erro indica há quanto tempo o erro ocorreu. Nenhum erro é exibido se as permissões associadas às credenciais de um endpoint estiverem incorretas.

### Determine se ocorreu algum erro

Se ocorrerem erros nos endpoints dos serviços da plataforma nos últimos 7 dias, o painel do Tenant Manager exibirá uma mensagem de alerta. Você pode acessar a página de endpoints dos serviços da plataforma para ver mais detalhes sobre o erro.




O mesmo erro que aparece no painel também aparece na parte superior da página de endpoints dos serviços da plataforma. Para visualizar uma mensagem de erro mais detalhada:

**Passos**

1. Na lista de endpoints, selecione o endpoint que apresenta o erro.
2. Na página de detalhes do endpoint, selecione **Conexão**. Esta aba exibe apenas o erro mais recente para um endpoint e indica há quanto tempo o erro ocorreu. Erros que incluem o ícone X vermelho ocorreram nos últimos 7 dias.

### Verifique se o erro ainda persiste

Alguns erros podem continuar sendo exibidos na coluna **Último erro** mesmo após serem resolvidos. Para verificar se um erro ainda está ativo ou para forçar a remoção de um erro resolvido da tabela:

**Passos**

1. Selecione o endpoint.

   A página de detalhes do endpoint é exibida.

2. Selecione **Conexão** > **Testar conexão**.

Selecionar **Test connection** faz com que o StorageGRID valide se o endpoint dos serviços da plataforma existe e se pode ser acessado com as credenciais atuais. A conexão com o endpoint é validada a partir de um nó em cada site.

### Resolver erros de endpoint

Você pode usar a mensagem **Último erro** na página de detalhes do endpoint para ajudar a determinar o que está causando o erro. Alguns erros podem exigir que você edite o endpoint para resolver o problema. Por exemplo, um erro CloudMirroring pode ocorrer se StorageGRID não conseguir acessar o bucket S3 de destino porque não possui as permissões de acesso corretas ou a chave de acesso expirou. A mensagem é "As credenciais do endpoint ou o acesso ao destino precisam ser atualizados" e os detalhes são "AccessDenied" ou "InvalidAccessKeyId".

Se você precisar editar o endpoint para corrigir um erro, selecionar **Testar e salvar alterações** fará com que o StorageGRID valide o endpoint atualizado e confirme que ele pode ser acessado com as credenciais atuais. A conexão com o endpoint é validada a partir de um nó em cada site.

**Passos**

1. Selecione o endpoint.
2. Na página de detalhes do endpoint, selecione **Configuration**.
3. Edite a configuração do endpoint conforme necessário.

4. Selecione **Conexão** > **Testar conexão**.

### Credenciais de endpoint com permissões insuficientes

Quando StorageGRID valida um endpoint de serviços da plataforma, ele confirma se as credenciais do endpoint podem ser usadas para contatar o recurso de destino e realiza uma verificação básica de permissões. No entanto, StorageGRID não valida todas as permissões necessárias para determinadas operações de serviços da plataforma. Por esse motivo, se você receber um erro ao tentar usar um serviço da plataforma (como "403 Forbidden"), verifique as permissões associadas às credenciais do endpoint.

### Informações relacionadas

- **Administrar StorageGRID › Solucionar problemas dos serviços da plataforma**
- "Criar endpoint de serviços de plataforma"
- "Teste de conexão para o endpoint de serviços da plataforma"
- "Editar endpoint de serviços da plataforma"

## Configure a replicação CloudMirror no StorageGRID

Para habilitar a replicação CloudMirror para um bucket, você cria e aplica um arquivo XML de configuração de replicação de bucket válido.

### Antes de começar

- Os serviços da plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket para servir como fonte de replicação.
- O ponto de extremidade que você pretende usar como destino para CloudMirror replication já existe e você possui o seu URN.
- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Locatários.

### Sobre esta tarefa

CloudMirror replica objetos de um bucket de origem para um bucket de destino especificado em um endpoint.

Para informações gerais sobre replicação de buckets e como configurá-la, consulte "Documentação do Amazon Simple Storage Service (S3): replicação de objetos". Para informações sobre como StorageGRID implementa GetBucketReplication, DeleteBucketReplication e PutBucketReplication, consulte o "Operações em buckets".

> ⓘ A replicação CloudMirror apresenta semelhanças e diferenças importantes em relação ao recurso de replicação entre grades. Para saber mais, consulte "Compare a replicação entre grades e a replicação CloudMirror".

Observe os seguintes requisitos e características ao configurar a replicação CloudMirror:

- Ao criar e aplicar um XML de configuração de replicação de bucket válido, é necessário usar o URN de um endpoint de bucket S3 para cada destino.
- A replicação não é compatível para buckets de origem ou destino com o S3 Object Lock ativado.
- Se você habilitar a replicação CloudMirror em um bucket que contém objetos, os novos objetos

adicionados ao bucket serão replicados, mas os objetos existentes no bucket não serão replicados. Você precisa atualizar os objetos existentes para acionar a replicação.

- Se você especificar uma classe de armazenamento no XML de configuração de replicação, StorageGRID usará essa classe ao executar operações no endpoint S3 de destino. O endpoint de destino também deve ser compatível com a classe de armazenamento especificada. Certifique-se de seguir as recomendações fornecidas pelo fornecedor do sistema de destino.

**Passos**

1. Ative a replicação para o seu bucket de origem:
   - Utilize um editor de texto para criar o XML de configuração de replicação necessário para habilitar a replicação, conforme especificado na API de replicação do S3.
   - Ao configurar o XML:
     - Observe que StorageGRID suporta apenas V1 da configuração de replicação. Isso significa que StorageGRID não suporta o uso do `Filter` elemento para regras e segue as convenções de V1 para exclusão de versões de objetos. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes.
     - Utilize o URN de um endpoint de bucket S3 como destino.
     - Opcionalmente, adicione o `<StorageClass>` elemento e especifique uma das seguintes opções:
       - `STANDARD`: A classe de armazenamento padrão. Se você não especificar uma classe de armazenamento ao carregar um objeto, a `STANDARD`classe de armazenamento padrão será usada.
       - `STANDARD_IA`: (Padrão - acesso pouco frequente.) Use esta classe de armazenamento para dados que são acessados com menos frequência, mas que ainda exigem acesso rápido quando necessário.
       - `REDUCED_REDUNDANCY`: Utilize esta classe de armazenamento para dados não críticos e reproduzíveis que podem ser armazenados com menos redundância do que a `STANDARD` classe de armazenamento.
     - Se você especificar um `Role` no XML de configuração, ele será ignorado. Esse valor não é usado pelo StorageGRID.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do bucket de origem.

A página de detalhes do bucket é exibida.

4. Selecione **Serviços da plataforma** > **Replicação**.
5. Selecione a caixa de seleção **Ativar replicação**.
6. Cole o XML de configuração de replicação na caixa de texto e selecione **Salvar alterações**.

> Os serviços da plataforma devem ser ativados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a Grid Management API. Entre em contato com o administrador do StorageGRID se ocorrer um erro ao salvar o XML de configuração.

7. Verifique se a replicação está configurada corretamente:
   a. Adicione um objeto ao bucket de origem que atenda aos requisitos de replicação especificados na configuração de replicação.

      No exemplo mostrado anteriormente, os objetos que correspondem ao prefixo "2020" são replicados.

   b. Confirme se o objeto foi replicado para o bucket de destino.

      Para objetos pequenos, a replicação ocorre rapidamente.

**Informações relacionadas**

"Criar endpoint de serviços de plataforma"

### Configure as notificações de eventos no StorageGRID

Você habilita as notificações para um bucket criando um arquivo XML de configuração de notificações e usando o Tenant Manager para aplicar o XML a um bucket.

**Antes de começar**

- Os serviços da plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket para servir como fonte de notificações.
- O endpoint que você pretende usar como destino para notificações de eventos já existe e você possui seu URN.
- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Locatários.

**Sobre esta tarefa**

Você configura as notificações de eventos associando um arquivo XML de configuração de notificações a um bucket de origem. O arquivo XML de configuração de notificações segue as convenções do S3 para configurar notificações de buckets, com o destino Amazon SNS topic, Kafka topic ou endpoint do webhook especificado como o URN de um endpoint.

Para informações gerais sobre notificações de eventos e como configurá-las, consulte a "Documentação da Amazon". Para informações sobre como o StorageGRID implementa a API de configuração de notificações do bucket S3, consulte a "Instruções para implementar aplicativos cliente S3".

Observe os seguintes requisitos e características ao configurar notificações de eventos para um bucket:

- Ao criar e aplicar um XML de configuração de notificação válido, é necessário usar o URN de um endpoint de notificações de eventos para cada destino.
- Embora seja possível configurar a notificação de eventos em um bucket com o S3 Object Lock ativado, os metadados do S3 Object Lock (incluindo Retain Until Date e o status de Legal Hold) dos objetos não serão incluídos nas mensagens de notificação.
- Após configurar as notificações de eventos, sempre que um evento específico ocorrer para um objeto no bucket de origem, uma notificação será gerada e enviada para o tópico Amazon SNS, tópico Kafka ou endpoint webhook usado como destino.
- Se você ativar as notificações de eventos para um bucket que contém objetos, as notificações serão enviadas apenas para ações realizadas após o salvamento da configuração de notificação.

**Passos**

1. Ative as notificações para seu bucket de origem:
   - Utilize um editor de texto para criar o XML de configuração de notificações necessário para habilitar as notificações de eventos, conforme especificado na API de notificações do S3.
   - Ao configurar o XML, utilize o URN de um endpoint de notificações de eventos como o tópico de destino.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. No Tenant Manager, selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do bucket de origem.

   A página de detalhes do bucket é exibida.

4. Selecione **Serviços da plataforma** > **Notificações de eventos**.
5. Selecione a caixa de seleção **Ativar notificações de eventos**.
6. Cole o XML de configuração de notificação na caixa de texto e selecione **Salvar alterações**.

Os serviços da plataforma devem ser ativados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a Grid Management API. Entre em contato com o administrador do StorageGRID se ocorrer um erro ao salvar o XML de configuração.

7. Verifique se as notificações de eventos estão configuradas corretamente:

   a. Execute uma ação em um objeto no bucket de origem que atenda aos requisitos para acionar uma notificação conforme configurado no XML de configuração.

      No exemplo, uma notificação de evento é enviada sempre que um objeto é criado com o `images/` prefixo.

   b. Confirme que uma notificação foi entregue ao destino Amazon SNS topic, Kafka topic ou endpoint do webhook.

      Por exemplo, se o seu tópico de destino estiver hospedado no Amazon SNS, você pode configurar o serviço para enviar um e-mail quando a notificação for entregue.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


+
Se a notificação for recebida no tópico de destino, você configurou com sucesso seu bucket de origem para notificações do StorageGRID.

**Informações relacionadas**

- "Entenda as notificações para buckets"
- "Utilize a API REST S3"

- "Criar endpoint de serviços de plataforma"

### Configure o serviço de integração de pesquisa em StorageGRID

Você habilita a integração de pesquisa para um bucket criando um XML de integração de pesquisa e usando o Tenant Manager para aplicar o XML ao bucket.

#### Antes de começar

- Os serviços da plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket S3 cujo conteúdo você deseja indexar.
- O endpoint que você pretende usar como destino para o serviço de integração de pesquisa já existe e você possui seu URN.
- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Locatários.

#### Sobre esta tarefa

Após configurar o serviço de integração de pesquisa para um bucket de origem, a criação de um objeto ou a atualização dos metadados ou tags de um objeto aciona o envio dos metadados do objeto para o endpoint de destino.

Se você ativar o serviço de integração de pesquisa para um bucket que já contém objetos, as notificações de metadados não serão enviadas automaticamente para os objetos existentes. Atualize esses objetos existentes para garantir que seus metadados sejam adicionados ao índice de pesquisa de destino.

#### Passos

1. Ativar a integração de pesquisa para um bucket:
    - Utilize um editor de texto para criar o XML de notificação de metadados necessário para habilitar a integração de pesquisa.
    - Ao configurar o XML, use o URN de um endpoint de integração de pesquisa como destino.

      Os objetos podem ser filtrados pelo prefixo do nome do objeto. Por exemplo, você pode enviar metadados para objetos com o prefixo `images` para um destino e metadados para objetos com o prefixo `videos` para outro. Configurações com prefixos sobrepostos não são válidas e são rejeitadas no momento do envio. Por exemplo, uma configuração que inclua uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não é permitida.

      Se necessário, consulte o exemplos para o XML de configuração de metadados.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

Elementos no XML de configuração da notificação de metadados:

| Nome | Descrição | Obrigatório |
|---|---|---|
| MetadataNotificationConfiguration | Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados.<br><br>Contém um ou mais elementos de Rule. | Sim |
| Regra | Etiqueta de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice específico.<br><br>Regras com prefixos sobrepostos são rejeitadas.<br><br>Incluído no elemento MetadataNotificationConfiguration. | Sim |
| ID | Identificador único para a regra.<br><br>Incluído no elemento Rule. | Não |
| Status | O status pode ser 'Ativado' ou 'Desativado'. Nenhuma ação é executada para regras desativadas.<br><br>Incluído no elemento Rule. | Sim |
| Prefixo | Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado.<br><br>Para corresponder a todos os objetos, especifique um prefixo vazio.<br><br>Incluído no elemento Rule. | Sim |
| Destino | Etiqueta de contêiner para o destino de uma regra.<br><br>Incluído no elemento Rule. | Sim |

| Nome | Descrição | Obrigatório |
| --- | --- | --- |
| Urna | URN do destino para onde os metadados do objeto são enviados. Deve ser o URN de um endpoint do StorageGRID com as seguintes propriedades:<br>• `es`deve ser o terceiro elemento.<br>• O URN deve terminar com o índice e o tipo onde os metadados estão armazenados, no formato `domain-name/myindex/mytype`.<br>Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles têm o seguinte formato:<br>• `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype`<br>• `urn:mysite:es:::mydomain/myindex/mytype`<br>O endpoint deve ser configurado antes do envio do XML de configuração, ou a configuração falhará com um erro 404.<br>O URN está incluído no elemento destino. | Sim |

2. No Gerenciador de Locatários, selecione **ARMAZENAMENTO (S3)** > **Buckets**.
3. Selecione o nome do bucket de origem.

   A página de detalhes do bucket é exibida.

4. Selecione **Serviços da plataforma** > **Integração de pesquisa**
5. Selecione a caixa de seleção **Enable search integration**.
6. Cole a configuração de notificação de metadados na caixa de texto e selecione **Salvar alterações**.

   Os serviços da plataforma devem ser ativados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a Management API. Entre em contato com seu administrador do StorageGRID se ocorrer um erro ao salvar o XML de configuração.

7. Verifique se o serviço de integração de pesquisa está configurado corretamente:
   a. Adicione um objeto ao bucket de origem que atenda aos requisitos para acionar uma notificação de metadados, conforme especificado no XML de configuração.

      No exemplo mostrado anteriormente, todos os objetos adicionados ao bucket acionam uma notificação de metadados.

   b. Confirme se um documento JSON contendo os metadados e as tags do objeto foi adicionado ao índice de pesquisa especificado no endpoint.

**Depois que você terminar**

Se necessário, você pode desativar a integração de pesquisa para um bucket usando um dos seguintes métodos:

- Selecione **STORAGE (S3)** > **Buckets** e desmarque a caixa de seleção **Enable search integration**.
- Se você estiver usando a API S3 diretamente, use uma solicitação DELETE Bucket metadata notification. Veja as instruções para implementar aplicativos cliente S3.

#### Exemplo: configuração de notificação de metadados que se aplica a todos os objetos

Neste exemplo, os metadados dos objetos são enviados para o mesmo destino.

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

#### Exemplo: configuração de notificação de metadados com duas regras

Neste exemplo, os metadados dos objetos que correspondem ao prefixo `/images` são enviados para um destino, enquanto os metadados dos objetos que correspondem ao prefixo `/videos` são enviados para um segundo destino.

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

#### Formato de notificação de metadados

Ao ativar o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado para o endpoint de destino sempre que os metadados ou tags de um objeto são adicionados, atualizados ou excluídos.

Este exemplo mostra um exemplo do JSON que poderia ser gerado quando um objeto com a chave `SGWS/Tagging.txt` é criado em um bucket chamado `test`. O `test` bucket não é versionado, portanto 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"
  }
}
```

**Campos incluídos no documento JSON**

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

**Informações sobre buckets e objetos**

`bucket`: Nome do bucket

`key`: nome da chave do objeto

`versionID`: Versão do objeto, para objetos em buckets versionados

`region`: Região do bucket, por exemplo `us-east-1`

**Metadados do sistema**

`size`: Tamanho do objeto (em bytes) conforme visível para um cliente HTTP

`md5`: hash de objeto

**Metadados do usuário**

`metadata`: Todos os metadados do usuário para o objeto, como pares de chave-valor

`key:value`

**Tags**

`tags`: Todas as tags de objeto definidas para o objeto, como pares chave-valor

```
key:value
```

**Como visualizar resultados no Elasticsearch**

Para tags e metadados do usuário, StorageGRID envia 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 dinâmico de campos e para mapeamento de formatos de data. Habilite os mapeamentos dinâmicos de campos 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.

# Utilize a API REST S3

## Versões e atualizações compatíveis da API REST S3 do StorageGRID

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

O suporte à API REST S3 permite que você conecte aplicativos orientados a serviços, desenvolvidos para serviços web do S3, com storage de objetos local que utiliza o sistema StorageGRID. São necessárias alterações mínimas no uso atual das chamadas à API REST S3 pelo aplicativo cliente.

**Versões suportadas**

StorageGRID suporta as seguintes versões específicas de STS, S3 e HTTP:

| Item | Versão |
| --- | --- |
| Especificação da API STS AssumeRole | "Documentação da Amazon Web Services (AWS): Referência da API Amazon Assumerole"<br><br>Para obter mais informações sobre AssumeRole, consulte "Configurar AssumeRole". |
| Especificação da API S3 | "Documentação da AWS: Referência da API do Amazon Simple Storage Service" |
| HTTP | 1,1<br><br>Para obter mais informações sobre HTTP, consulte HTTP/1.1 (RFCs 7230-35).<br><br>"IETF RFC 2616: Protocolo de Transferência de Hipertexto (HTTP/1.1)"<br><br>**Nota**: StorageGRID não suporta HTTP/1.1 pipelining. |

### Atualizações no suporte à API REST do S3

| Release | Comentários |
|---|---|
| 12,0 | • Adicionada a funcionalidade de compartilhamento de recursos entre origens (CORS) para uma interface de gerenciamento, permitindo que outro domínio acesse dados no StorageGRID usando APIs de gerenciamento. "Saiba mais".<br>• Adicionado suporte para STS AssumeRole e política de sessão. Consulte "um exemplo de política de sessão". Você pode configurar AssumeRole em grupos de locatários. |
| 11,9 | • Adicionamos suporte para valores de checksum SHA-256 pré-calculados para as seguintes solicitações e cabeçalhos compatíveis. Você pode usar este recurso para verificar a integridade dos objetos enviados:<br>◦ CompleteMultipartUpload: `x-amz-checksum-sha256`<br>◦ CreateMultipartUpload: `x-amz-checksum-algorithm`<br>◦ GetObject: `x-amz-checksum-mode`<br>◦ HeadObject: `x-amz-checksum-mode`<br>◦ ListParts<br>◦ PutObject: `x-amz-checksum-sha256`<br>◦ UploadPart: `x-amz-checksum-sha256`<br>• Adicionada a capacidade para o administrador da grid controlar as configurações de retenção e Compliance em nível de tenant. Essas configurações afetam as configurações de S3 Object Lock.<br>◦ Modo de retenção padrão do bucket e modo de retenção do objeto: governança ou conformidade, se permitido pelo administrador do grid.<br>◦ Período de retenção padrão do bucket e data de retenção do objeto: devem ser menores ou iguais ao permitido pelo período de retenção máximo definido pelo administrador do grid.<br>• Suporte aprimorado para `aws-chunked`codificação de conteúdo e streaming `x-amz-content-sha256` valores. Limitações:<br>◦ Se presente, `chunk-signature`é opcional e não é validado<br>◦ Se presente, `x-amz-trailer` o conteúdo é ignorado |
| 11,8 | Atualizamos os nomes das operações do S3 para corresponder aos nomes usados no "Documentação da Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service". |

| Release | Comentários |
| --- | --- |
| 11,7 | • Adicionado "Referência rápida: solicitações de API S3 compatíveis".<br>• Adicionado suporte para o uso do modo GOVERNANCE com S3 Object Lock.<br>• Adicionado suporte ao cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status` para solicitações GET Object e HEAD Object. Este cabeçalho fornece o status de replicação de um objeto para replicação entre grids.<br>• SelectObjectContent requests agora suportam objetos Parquet. |
| 11,6 | • Adicionado suporte para usar o `partNumber`parâmetro request em solicitações GET Object e HEAD Object.<br>• Adicionado suporte para um modo de retenção padrão e um período de retenção padrão no nível do bucket para o S3 Object Lock.<br>• Adicionado suporte para a chave de condição de política `s3:object-lock-remaining-retention-days` para definir o intervalo de períodos de retenção permitidos para seus objetos.<br>• Alteramos o tamanho máximo *recomendado* para uma única operação PUT Object para 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use upload multipart. |
| 11,5 | • Adicionado suporte para gerenciamento de criptografia de bucket.<br>• Adicionado suporte para S3 Object Lock e descontinuadas as solicitações de Compliance legadas.<br>• Adicionado suporte para usar DELETE Multiple Objects em buckets versionados.<br>• O `Content-MD5`cabeçalho da solicitação agora é suportado corretamente. |
| 11,4 | • Adicionado suporte para DELETE Bucket tagging, GET Bucket tagging e PUT Bucket tagging. Tags de alocação de custos não são suportadas.<br>• Para buckets criados no StorageGRID 11.4, restringir os nomes das chaves de objeto para atender às melhores práticas de desempenho não é mais necessário.<br>• Adicionado suporte para notificações de bucket no tipo de evento `s3:ObjectRestore:Post`.<br>• Os limites de tamanho da AWS para partes multipartes agora são aplicados. Cada parte em um upload multipart deve ter entre 5 MiB e 5 GiB. A última parte pode ser menor que 5 MiB.<br>• Adicionado suporte para TLS 1.3 |

| Release | Comentários |
| --- | --- |
| 11,3 | • Adicionado suporte para criptografia do lado do servidor dos dados de objetos com chaves fornecidas pelo cliente (SSE-C).<br>• Adicionado suporte para as operações de ciclo de vida do bucket DELETE, GET e PUT (somente ação de expiração) e para o cabeçalho de resposta `x-amz-expiration`.<br>• Atualizamos os artigos PUT Object, PUT Object - Copy e Multipart Upload para descrever o impacto das regras de gerenciamento do ciclo de vida das informações (ILM) que utilizam posicionamento síncrono na ingestão.<br>• Os algoritmos de criptografia TLS 1.1 não são mais suportados. |
| 11,2 | Adicionado suporte para restauração de objeto via POST 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 do StorageGRID continuarão sendo suportadas.<br><br>**Nota:** Os usos de ARN/URN em outros arquivos de configuração JSON/XML, incluindo aqueles usados em recursos personalizados do StorageGRID, não foram alterados. |
| 11,1 | Adicionado suporte para compartilhamento de recursos entre origens (CORS), HTTP para conexões de clientes S3 com nós de grid e configurações de conformidade em buckets. |
| 11,0 | Adicionamos suporte para configurar serviços de plataforma (CloudMirror replicação, notificações e integração de pesquisa com o Elasticsearch) para buckets. Também adicionamos suporte para restrições de localização de marcação de objetos para buckets e para a consistência de disponibilidade. |
| 10,4 | Adicionado suporte para verificação ILM de alterações no controle de versão, atualizações da página de nomes de domínio de endpoints, condições e variáveis em políticas, exemplos de políticas e a permissão PutOverwriteObject. |
| 10,3 | Adicionado suporte para versionamento. |
| 10,2 | Adicionado suporte para políticas de acesso a grupos e buckets, e para cópia multipart (Upload Part - Copy). |
| 10,1 | Adicionado suporte para upload multipart, solicitações no estilo de hospedagem virtual e autenticação v4. |
| 10,0 | Suporte inicial da API REST S3 pelo sistema StorageGRID. A versão atualmente suportada da *Simple Storage Service API Reference* é 2006-03-01. |

## Solicitações de API S3 suportadas no StorageGRID

Esta página resume como StorageGRID oferece suporte às APIs do Amazon Simple

## Storage Service (S3).

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

Para visualizar a documentação da AWS para cada operação, selecione o link no cabeçalho.

**Parâmetros de consulta URI comuns e cabeçalhos de solicitação**

Salvo indicação em contrário, os seguintes parâmetros de consulta URI comuns são suportados:

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

Salvo indicação em contrário, os seguintes cabeçalhos de solicitação comuns são suportados:

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

**Informações relacionadas**

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

### "AbortMultipartUpload"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todos os parâmetros e cabeçalhos comuns para esta solicitação, além deste parâmetro de consulta URI adicional:

- `uploadId`

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações para uploads multipartes"

### "CompleteMultipartUpload"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todos os parâmetros e cabeçalhos comuns para esta solicitação, além deste parâmetro de consulta URI adicional:

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

**Tags XML do corpo da requisição**

StorageGRID suporta estas tags XML no corpo da requisição:

- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

**Documentação do StorageGRID**

"CompleteMultipartUpload"

### "CopyObject"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

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

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

- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"CopyObject"

### "CreateBucket"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

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

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

**Corpo da solicitação**

StorageGRID suporta todos os parâmetros do corpo da requisição definidos pela Amazon S3 REST API no momento da implementação.

**Documentação do StorageGRID**

"Operações em buckets"

### "CreateMultipartUpload"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

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

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

- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"CreateMultipartUpload"

### "DeleteBucket"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Documentação do StorageGRID**

"Operações em buckets"

### "DeleteBucketCors"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "DeleteBucketEncryption"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "DeleteBucketLifecycle"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

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

### "DeleteBucketPolicy"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "DeleteBucketReplication"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "DeleteBucketTagging"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "DeleteObject"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todos os parâmetros e cabeçalhos comuns para esta solicitação, além deste cabeçalho de solicitação adicional:

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

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em objetos"

### "DeleteObjects"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todos os parâmetros e cabeçalhos comuns para esta solicitação, além deste cabeçalho de solicitação adicional:

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

**Corpo da solicitação**

StorageGRID suporta todos os parâmetros do corpo da requisição definidos pela Amazon S3 REST API no momento da implementação.

**Documentação do StorageGRID**

"Operações em objetos"

### "DeleteObjectTagging"

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em objetos"

### "GetBucketAcl"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "GetBucketCors"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "GetBucketEncryption"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "GetBucketLifecycleConfiguration"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

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

### "GetBucketLocation"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "GetBucketNotificationConfiguration"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "GetBucketPolicy"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "GetBucketReplication"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "GetBucketTagging"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "GetBucketVersioning"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "GetObject"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

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

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

E estes cabeçalhos de solicitação adicionais:

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

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

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"GetObject"

### "GetObjectAcl"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em objetos"

### "GetObjectLegalHold"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Use a API REST S3 para configurar o S3 Object Lock"

### "GetObjectLockConfiguration"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Use a API REST S3 para configurar o S3 Object Lock"

### "GetObjectRetention"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Use a API REST S3 para configurar o S3 Object Lock"

### "GetObjectTagging"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em objetos"

### "HeadBucket"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "HeadObject"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

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

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

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"HeadObject"

### "ListBuckets"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

**Operações no serviço › ListBuckets**

### "ListMultipartUploads"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID suporta todos parâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

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

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"ListMultipartUploads"

### "ListObjects"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID suporta todos parâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

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

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "ListObjectsV2"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID suporta todos parâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

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

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "ListObjectVersions"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID suporta todos parâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

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

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"Operações em buckets"

### "ListParts"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID suporta todos parâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros

adicionais:

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

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"ListMultipartUploads"

### "PutBucketCors"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

StorageGRID suporta todos os parâmetros do corpo da requisição definidos pela Amazon S3 REST API no momento da implementação.

**Documentação do StorageGRID**

"Operações em buckets"

### "PutBucketEncryption"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Tags XML do corpo da requisição**

StorageGRID suporta estas tags XML no corpo da requisição:

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

**Documentação do StorageGRID**

"Operações em buckets"

### "PutBucketLifecycleConfiguration"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Tags XML do corpo da requisição**

StorageGRID suporta estas tags XML no corpo da requisição:

- `And`

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

**Documentação do StorageGRID**

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

### "PutBucketNotificationConfiguration"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Tags XML do corpo da requisição**

StorageGRID suporta estas tags XML no corpo da requisição:

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`

- `TopicConfiguration`
- `Value`

**Documentação do StorageGRID**

"Operações em buckets"

### "PutBucketPolicy"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

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

### "PutBucketReplication"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Tags XML do corpo da requisição**

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

**Documentação do StorageGRID**

"Operações em buckets"

### "PutBucketTagging"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

StorageGRID suporta todos os parâmetros do corpo da requisição definidos pela Amazon S3 REST API no momento da implementação.

**Documentação do StorageGRID**

"Operações em buckets"

### "PutBucketVersioning"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Parâmetros do corpo da requisição**

StorageGRID suporta estes parâmetros no corpo da requisição:

- `VersioningConfiguration`
- `Status`

**Documentação do StorageGRID**

"Operações em buckets"

### "PutObject"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

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

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

**Corpo da solicitação**

- Dados binários do objeto

**Documentação do StorageGRID**

"PutObject"

### "PutObjectLegalHold"

#### Parâmetros de consulta URI e cabeçalhos de solicitação

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

#### Corpo da solicitação

StorageGRID suporta todos os parâmetros do corpo da requisição definidos pela Amazon S3 REST API no momento da implementação.

#### Documentação do StorageGRID

"Use a API REST S3 para configurar o S3 Object Lock"

### "PutObjectLockConfiguration"

#### Parâmetros de consulta URI e cabeçalhos de solicitação

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

#### Corpo da solicitação

StorageGRID suporta todos os parâmetros do corpo da requisição definidos pela Amazon S3 REST API no momento da implementação.

#### Documentação do StorageGRID

"Use a API REST S3 para configurar o S3 Object Lock"

### "PutObjectRetention"

#### Parâmetros de consulta URI e cabeçalhos de solicitação

StorageGRID oferece suporte a todos os parâmetros e cabeçalhos comuns para esta solicitação, além deste cabeçalho adicional:

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

#### Corpo da solicitação

StorageGRID suporta todos os parâmetros do corpo da requisição definidos pela Amazon S3 REST API no momento da implementação.

#### Documentação do StorageGRID

"Use a API REST S3 para configurar o S3 Object Lock"

### "PutObjectTagging"

#### Parâmetros de consulta URI e cabeçalhos de solicitação

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

#### Corpo da solicitação

StorageGRID suporta todos os parâmetros do corpo da requisição definidos pela Amazon S3 REST API no momento da implementação.

#### Documentação do StorageGRID

"Operações em objetos"

### "RestoreObject"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

Para obter detalhes sobre os campos de corpo suportados, consulte "RestoreObject".

### "SelectObjectContent"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

StorageGRID oferece suporte a todas parâmetros e cabeçalhos comuns para esta solicitação.

**Corpo da solicitação**

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

- "Use o S3 Select"
- "SelectObjectContent"

### "UploadPart"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

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

- `partNumber`
- `uploadId`

E estes cabeçalhos de solicitação adicionais:

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

**Corpo da solicitação**

- Dados binários da parte

**Documentação do StorageGRID**

"UploadPart"

### "UploadPartCopy"

**Parâmetros de consulta URI e cabeçalhos de solicitação**

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

- `partNumber`
- `uploadId`

E estes cabeçalhos de solicitação adicionais:

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

**Corpo da solicitação**

Nenhum

**Documentação do StorageGRID**

"UploadPartCopy"

## Teste a configuração da API REST S3 do StorageGRID

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

**Antes de começar**

- Você baixou e instalou a AWS CLI a partir de "aws.amazon.com/cli".
- Opcionalmente, você tem "criou um endpoint de balanceador de carga". Caso contrário, você sabe o endereço IP do Storage Node ao qual deseja se conectar e o número da porta a ser usado. Consulte "Endereços IP e portas para conexões de clientes".
- Você tem "Criou uma conta de locatário S3".
- Você fez login no tenant e "criou uma chave de acesso".

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

**Passos**

1. Configure as definições da AWS CLI para utilizar a conta que você criou no sistema StorageGRID:
   a. Entre no modo de configuração: `aws configure`
   b. Insira o ID da chave de acesso da conta que você criou.
   c. Digite a chave de acesso secreta da conta que você criou.
   d. Insira a região padrão a ser usada. Por exemplo, `us-east-1`.

e. Digite o formato de saída padrão a ser usado ou pressione **Enter** para selecionar JSON.

2. Crie um bucket.

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

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

   Se o bucket for criado com sucesso, a localização do bucket é retornada, como pode ser visto no exemplo a seguir:

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

3. Faça o upload de 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. Exclua o bucket.

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

## Como StorageGRID implementa a API REST S3

### Como a StorageGRID API REST resolve solicitações conflitantes do cliente

Solicitações conflitantes de clientes, como dois clientes escrevendo na mesma chave, são resolvidas com base no princípio "o mais recente vence".

O momento da avaliação "latest-wins" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

### Como StorageGRID API REST S3 equilibra disponibilidade e consistência

A consistência proporciona um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes Storage Nodes e sites. Você pode alterar a consistência conforme necessário para sua aplicação.

Por padrão, StorageGRID garante a consistência de leitura após gravação para objetos recém-criados. Qualquer GET subsequente a um PUT concluído com sucesso poderá ler os dados recém-gravados. Sobrescritas de objetos existentes, atualizações de metadados e exclusões são eventualmente consistentes.

Se você deseja executar operações de objetos com um nível de consistência diferente, você pode:

- Especifique uma consistência para cada bucket.
- Especifique uma consistência para cada operação de API.
- Altere a consistência padrão de toda a grade executando uma das seguintes tarefas:
  - No Grid Manager, acesse **Configuração** > **Sistema** > **Configurações de armazenamento** > **Consistência padrão do bucket**.
  - .

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

#### Valores de consistência

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

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

- **Todos**: Todos os nós recebem metadados de objeto imediatamente ou a solicitação falhará.
- **Strong-global**: Garante a consistência de leitura após gravação para todas as solicitações do cliente em todos os sites. Quando a semântica de Quorum está configurada, os seguintes comportamentos se aplicam:
  - Permite tolerância a falha do local para solicitações de clientes quando as grades têm três ou mais sites. Grades com dois sites não terão tolerância a falha do local.
  - As seguintes operações do S3 não serão bem-sucedidas com um site inativo:
    - DeleteBucketEncryption
    - PutBucketBranch

- PutBucketEncryption
- PutBucketVersioning
- PutObjectLegalHold
- PutObjectLockConfiguration
- PutObjectRetention

Se necessário, você pode "configurar a semântica de quorum do StorageGRID para consistência global forte".

- **Strong-site**: os metadados do objeto são distribuídos imediatamente para outros nós no site. Garante a consistência de leitura após gravação para todas as solicitações do cliente dentro de um site.
- **Leitura após nova gravação**: Oferece consistência de leitura após gravação para novos objetos e consistência eventual para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
- **Disponível**: Oferece consistência eventual tanto para novos objetos quanto para atualizações de objetos. Para buckets do S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que são lidos raramente ou para operações HEAD ou GET em chaves que não existem). Não é compatível com buckets do S3 FabricPool.

#### Use as consistências "Read-after-new-write" e "Available"

Quando uma operação HEAD ou GET utiliza a consistência "Leitura após nova gravação", StorageGRID realiza a pesquisa em várias etapas, da seguinte forma:

- Primeiro, ele busca o objeto usando uma consistência baixa.
- Caso essa busca falhe, ela se repete no próximo valor de consistência até atingir uma consistência equivalente ao comportamento de strong-global.

Se uma operação HEAD ou GET usar a consistência "Read-after-new-write", mas o objeto não existir, a busca pelo objeto sempre atingirá uma consistência equivalente ao comportamento para strong-global. Como essa consistência exige que várias cópias dos metadados do objeto estejam disponíveis em cada site, você pode receber um grande número de erros 500 Internal Server se dois ou mais Storage Nodes no mesmo site estiverem indisponíveis.

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

#### Especifique a consistência para a operação da API

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

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

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

#### Especifique a consistência para o bucket

Para definir a consistência do bucket, você pode usar a solicitação "Consistência de PUT Bucket" do StorageGRID. Ou você pode "alterar a consistência de um bucket" a partir do Tenant Manager.

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

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

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

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

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

As seguintes "opções de ingestão" estão disponíveis para as regras do ILM:

**Commit duplo**
: StorageGRID cria imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

**Estrito**
: Todas as cópias especificadas na regra ILM devem ser feitas antes que a mensagem de sucesso seja retornada ao cliente.

**Equilibrado**
: StorageGRID tenta criar todas as cópias especificadas na regra ILM durante a ingestão; se isso não for possível, cópias provisórias são criadas e uma mensagem de sucesso é retornada ao cliente. As cópias especificadas na regra ILM são criadas sempre que possível.

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

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

- **Regra ILM**: Crie três cópias do objeto, uma no local e uma em cada local remoto. Use o comportamento de ingestão estrito.
- **Consistência**: Global forte (os metadados do objeto são distribuídos imediatamente para vários sites).

Quando um cliente armazena um objeto na grid, StorageGRID cria as três cópias do objeto e distribui os metadados para vários sites antes de retornar sucesso ao cliente.

O objeto fica totalmente protegido contra perda no momento em que a mensagem de ingestão bem-sucedida é recebida. Por exemplo, se o local remoto for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existirão nos locais remotos. O objeto poderá ser recuperado integralmente dos outros locais.

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

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

### Como StorageGRID usa o versionamento de objetos

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

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

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

O uso de MFA (autenticação multifator) com a função Delete não é suportado.

> O versionamento só pode ser ativado em buckets criados com StorageGRID versão 10.3 ou posterior.

#### ILM e versionamento

As políticas de ILM são aplicadas a cada versão de um objeto. Um processo de varredura de ILM examina continuamente todos os objetos e os reavalia em relação à política de ILM atual. Quaisquer alterações que você fizer nas políticas de ILM são aplicadas a todos os objetos previamente ingeridos. Isso inclui versões previamente ingeridas se o versionamento estiver habilitado. A varredura de ILM aplica as novas alterações de ILM aos objetos previamente ingeridos.

Para objetos S3 em buckets com versionamento habilitado, o suporte a versionamento permite que você crie

regras ILM que usam "Tempo não atual" como tempo de referência (selecione **Sim** para a pergunta "Aplicar esta regra somente a versões antigas do objeto?" em "Etapa 1 do assistente Criar uma regra ILM"). Quando um objeto é atualizado, suas versões anteriores se tornam não atuais. Usar um filtro de "Tempo não atual" permite que você crie políticas que reduzem o impacto de armazenamento das versões anteriores dos objetos.

> Ao carregar uma nova versão de um objeto usando uma operação de upload multipart, a hora não atual da versão original do objeto reflete o momento em que o upload multipart foi criado para a nova versão, não quando o upload multipart foi concluído. Em casos limitados, a hora não atual da versão original pode ser horas ou dias anterior à hora da versão atual.

**Informações relacionadas**

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

### Use a API REST S3 para configurar o S3 Object Lock do StorageGRID

Se a configuração global de Bloqueio de Objetos S3 estiver habilitada para o seu sistema StorageGRID, você pode criar buckets com o Bloqueio de Objetos S3 ativado. Você pode especificar o período de retenção padrão para cada bucket ou as configurações de retenção para cada versão de objeto.

#### Como habilitar o S3 Object Lock para um bucket

Se a configuração global de S3 Object Lock estiver ativada para o seu sistema StorageGRID, você pode, opcionalmente, ativar o S3 Object Lock ao criar cada bucket.

O Bloqueio de Objetos do S3 é uma configuração permanente que só pode ser ativada ao criar um bucket. Você não pode adicionar ou desativar o Bloqueio de Objetos do S3 depois que um bucket é criado.

Para ativar o S3 Object Lock para um bucket, use um destes métodos:

- Crie o bucket usando o Gerenciador de Locatários. Consulte "Criar bucket S3".
- Crie o bucket usando uma solicitação CreateBucket com o cabeçalho de solicitação `x-amz-bucket-object-lock-enabled`. Veja "Operações em buckets".

O S3 Object Lock requer o versionamento do bucket, que é ativado automaticamente quando o bucket é criado. Você não pode suspender o versionamento do bucket. Consulte "Versionamento de objetos".

#### Configurações de retenção padrão para um bucket

Quando o S3 Object Lock está habilitado para um bucket, você pode opcionalmente habilitar a retenção padrão para o bucket e especificar um modo de retenção padrão e um período de retenção padrão.

**Modo de retenção padrão**

- No modo COMPLIANCE:
  - O objeto não pode ser excluído até que sua retain-until-date seja atingida.
  - A data de retenção do objeto pode ser aumentada, mas não pode ser diminuída.
  - A data de retenção do objeto não pode ser removida até que essa data seja atingida.

- No modo GOVERNANÇA:
  - Usuários com a `s3:BypassGovernanceRetention` permissão podem usar o `x-amz-bypass-governance-retention: true` cabeçalho da solicitação para ignorar as configurações de retenção.
  - Esses usuários podem excluir uma versão de objeto antes que a data de retenção seja atingida.
  - Esses usuários podem aumentar, diminuir ou remover a retain-until-date de um objeto.

### Período de retenção padrão

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

#### Como definir a retenção padrão para um bucket

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

- Gerencie as configurações do bucket a partir do Tenant Manager. Consulte "Crie um bucket S3" e "Atualizar retenção padrão do S3 Object Lock".
- Envie uma solicitação PutObjectLockConfiguration para o bucket para especificar o modo padrão e o número padrão de dias ou anos.

### PutObjectLockConfiguration

A solicitação PutObjectLockConfiguration permite que você defina e modifique o modo de retenção padrão e o período de retenção padrão para um bucket com o S3 Object Lock ativado. Você também pode remover as configurações de retenção padrão previamente definidas.

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

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

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

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

### Exemplo de solicitação

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

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

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

#### Como determinar a retenção padrão para um bucket

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

- Veja o bucket no Tenant Manager. Consulte "Visualizar buckets do S3".
- Emita uma solicitação GetObjectLockConfiguration.

### GetObjectLockConfiguration

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

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

Você precisa ter a `s3:GetBucketObjectLockConfiguration` permissão, ou ser account root, para concluir esta operação.

### Exemplo de solicitação

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

**Exemplo de resposta**

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

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

#### Como especificar as configurações de retenção para um objeto

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

As configurações de retenção em nível de objeto são especificadas usando a API REST do S3. As configurações de retenção para um objeto substituem quaisquer configurações de retenção padrão para o bucket.

Você pode especificar as seguintes configurações para cada objeto:

- **Modo de retenção**: COMPLIANCE ou GOVERNANÇA.
- **Retain-until-date**: Uma data que especifica por quanto tempo a versão do objeto deve ser retida pelo StorageGRID.

    - No modo COMPLIANCE, se a retain-until-date for futura, o objeto poderá ser recuperado, mas não poderá ser modificado ou excluído. A retain-until-date pode ser aumentada, mas essa data não pode ser diminuída ou removida.
    - No modo GOVERNANÇA, usuários com permissões especiais podem ignorar a configuração de retain-until-date. Eles podem excluir uma versão de objeto antes que seu período de retenção tenha expirado. Eles também podem aumentar, diminuir ou até mesmo remover o retain-until-date.
- **Guarda legal**: Aplicar uma guarda legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar aplicar uma guarda legal a um objeto relacionado a uma investigação ou disputa legal. Uma guarda legal não tem data de expiração, mas permanece em vigor até ser explicitamente removida.

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

Para especificar as configurações de S3 Object Lock ao adicionar uma versão de objeto a um bucket, emita uma solicitação "PutObject", "CopyObject" ou "CreateMultipartUpload".

Você pode usar o seguinte:

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

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

- `x-amz-object-lock-retain-until-date`
    - O valor de retain-until-date deve estar no formato `2020-08-10T21:46:00Z`. Frações de segundo são permitidas, mas apenas 3 casas decimais são preservadas (precisão em milissegundos). Outros formatos ISO 8601 não são permitidos.
    - A data de retenção deve estar no futuro.
- `x-amz-object-lock-legal-hold`

  Se guarda legal estiver ON (diferencia maiúsculas de minúsculas), o objeto é colocado sob guarda legal. Se guarda legal estiver OFF, nenhuma guarda legal é aplicada. Qualquer outro valor resulta em um erro 400 Bad Request (InvalidArgument).

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

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

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

#### Como atualizar as configurações de retenção de um objeto

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

- `PutObjectLegalHold`

  Se o novo valor de guarda legal estiver ATIVADO, o objeto fica sujeito a guarda legal. Se o valor de guarda legal estiver DESATIVADO, a guarda legal é suspensa.

- `PutObjectRetention`
  - O valor do modo pode ser COMPLIANCE ou GOVERNANCE (diferencia maiúsculas de minúsculas).
  - O valor de retain-until-date deve estar no formato `2020-08-10T21:46:00Z`. Frações de segundo são permitidas, mas apenas 3 casas decimais são preservadas (precisão em milissegundos). Outros formatos ISO 8601 não são permitidos.
  - Se uma versão de um objeto já possui uma data de retenção definida, você só pode aumentá-la. O novo valor deve estar no futuro.

#### Como usar o modo GOVERNANCE

Usuários que têm a permissão `s3:BypassGovernanceRetention` podem ignorar as configurações de retenção ativa de um objeto que utiliza o modo GOVERNANCE. Quaisquer operações DELETE ou PutObjectRetention devem incluir o cabeçalho `x-amz-bypass-governance-retention:true` da solicitação. Esses usuários podem executar as seguintes operações adicionais:

- Execute operações DeleteObject ou DeleteObjects para excluir uma versão de objeto antes que seu período de retenção tenha expirado.

  Objetos que estão sob guarda legal não podem ser excluídos. A guarda legal deve estar DESATIVADA.

- Execute operações PutObjectRetention que alteram o modo de uma versão de objeto de GOVERNANCE para COMPLIANCE antes que o período de retenção tenha expirado.

  A mudança do modo de COMPLIANCE para GOVERNANCE nunca é permitida.

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

#### Informações relacionadas

- "Gerencie objetos com S3 Object Lock"
- "Use o S3 Object Lock para reter objetos"
- "Guia do usuário do Amazon Simple Storage Service: bloqueando objetos"

### Saiba mais sobre a configuração do ciclo de vida do S3 para StorageGRID

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

O exemplo simples nesta seção ilustra como uma configuração de ciclo de vida do S3 pode controlar quando

determinados objetos são excluídos (expirados) de buckets específicos do S3. O exemplo nesta seção é apenas para fins ilustrativos. Para obter detalhes completos sobre a criação de configurações de ciclo de vida do S3, consulte "Guia do usuário do Amazon Simple Storage Service: gerenciamento de ciclo de vida de objetos". Observe que StorageGRID oferece suporte apenas a ações de Expiração; não oferece suporte a ações de Transição.

#### O que é configuração de ciclo de vida

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

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

- Expiração: exclua um objeto quando uma data específica for atingida ou quando um número específico de dias for alcançado, a partir do momento em que o objeto foi ingerido.
- NoncurrentVersionExpiration: Exclua um objeto quando um número específico de dias for atingido, a partir do momento em que o objeto deixou de ser atual.
- Filtro (Prefixo, Tag)
- Status
- ID

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

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

> ⓘ A configuração de ciclo de vida do bucket pode ser usada com buckets que têm o S3 Object Lock ativado, mas a configuração de ciclo de vida do bucket não é compatível com buckets legados Compliant.

StorageGRID suporta o uso das seguintes operações de bucket para gerenciar configurações de ciclo de vida:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

#### Criar configuração de ciclo de vida

Como primeiro passo para criar 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 valor de `key2 tag2`. O parâmetro `Expiration` especifica que os objetos que correspondam 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 objetos que correspondem ao filtro expirarão 100 dias após serem ingeridos.

> As regras que especificam um número de dias são relativas à data de ingestão do objeto. Se a data atual for posterior à data de ingestão mais o número de dias, alguns objetos podem ser removidos do bucket 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"
        }
    ]
}
```

#### Aplicar configuração de ciclo de vida ao bucket

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

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

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

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

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

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

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

Você pode determinar se uma regra de expiração na configuração de ciclo de vida se aplica a um objeto específico ao emitir uma solicitação PutObject, HeadObject ou GetObject. Se uma regra se aplicar, a resposta incluirá um parâmetro `Expiration` 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` data exibida é a data real em que o objeto será excluído. Para obter detalhes, consulte "Como a retenção de objeto é determinada".

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

```
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 out 2020) e que corresponde à Regra 2 da configuração do ciclo de vida.

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

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

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

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

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

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

**Recomendações para implementar a API REST S3 com StorageGRID**

## Você deve seguir estas recomendações ao implementar a API REST para uso com StorageGRID.

#### Recomendações para HEADs para objetos inexistentes

Se sua aplicação verifica rotineiramente se um objeto existe em um caminho onde você não espera que ele exista, você deve usar a consistência "Disponível" "consistência". Por exemplo, você deve usar a consistência "Disponível" se sua aplicação executar um HEAD em um local antes de executar um PUT nele.

Caso contrário, se a operação HEAD não encontrar o objeto, você poderá receber um grande número de erros 500 Internal Server se dois ou mais nós de armazenamento no mesmo site estiverem indisponíveis ou se um local remoto estiver inacessível.

Você pode definir a consistência "Disponível" para cada bucket usando a "Consistência de PUT Bucket" solicitação, ou pode especificar a consistência no cabeçalho da solicitação para uma operação de API

individual.

#### Recomendações para chaves de objeto

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

**Buckets criados no StorageGRID 11.4 ou anterior**

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

  `mybucket/mydir/f8e3-image3132.jpg`

  Em vez deste formato:

  `mybucket/f8e3-image3132.jpg`

**Buckets criados no StorageGRID 11.4 ou posterior**

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

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

#### Recomendações para "leituras de intervalo"

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

Se intervalos forem lidos 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 do aplicativo.

## Suporte para Amazon S3 API REST

## Operações e limitações da API REST S3 no StorageGRID

O sistema StorageGRID implementa a API Simple Storage Service (API Version 2006-03-01) com suporte para a maioria das operações, e com algumas limitações. Você precisa entender os detalhes da implementação ao integrar aplicativos cliente da API REST do S3.

O sistema StorageGRID suporta tanto solicitações virtuais no estilo de hospedagem quanto solicitações no estilo de caminho.

### Tratamento de datas

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 quaisquer cabeçalhos que aceitam valores de data. A parte da hora da data pode ser especificada no formato de Greenwich Mean Time (GMT) ou no formato de Universal Coordinated Time (UTC) sem deslocamento de fuso horário (+0000 deve ser especificado). Se você incluir o `x-amz-date` cabeçalho na sua solicitação, ele substituirá qualquer valor especificado no cabeçalho Date da solicitação. Ao usar AWS Signature Version 4, o `x-amz-date` cabeçalho deve estar presente na solicitação assinada porque o cabeçalho Date não é compatível.

### Cabeçalhos de solicitação comuns

O sistema StorageGRID suporta os cabeçalhos de solicitação comuns definidos por "Referência da API do Amazon Simple Storage Service: cabeçalhos de solicitação comuns", com uma exceção.

| Cabeçalho da solicitação | Implementação |
|---|---|
| Autorização | Suporte completo para AWS Signature Version 2<br><br>Suporte para AWS Signature Version 4, com as seguintes exceções:<br><br>• Quando você fornece o valor real do checksum da carga em `x-amz-content-sha256`, o valor é aceito sem validação, como se o valor `UNSIGNED-PAYLOAD` tivesse sido fornecido para o cabeçalho. Quando você fornece um `x-amz-content-sha256` valor de cabeçalho que implica `aws-chunked` streaming (por exemplo, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), as assinaturas dos fragmentos não são verificadas em relação aos dados dos fragmentos. |

### Cabeçalhos de resposta comuns

O sistema StorageGRID suporta todos os cabeçalhos de resposta comuns definidos pela *Referência da API do Simple Storage Service*, com uma exceção.

| Cabeçalho de resposta | Implementação |
|---|---|
| x-amz-id-2 | Não utilizado |

### Como StorageGRID S3 API REST autentica solicitações

O sistema StorageGRID suporta tanto o acesso autenticado quanto o acesso anônimo a objetos usando a API S3.

A API S3 suporta Signature version 2 e Signature version 4 para autenticar solicitações da API S3.

As solicitações autenticadas devem ser assinadas usando seu access key ID e secret access key.

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

#### Use o cabeçalho Authorization HTTP

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

#### Use parâmetros de consulta

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

### Operações de serviço suportadas no StorageGRID

O sistema StorageGRID suporta as seguintes operações no serviço.

| Operação | Implementação |
|---|---|
| ListBuckets<br><br>(anteriormente chamado GET Service) | Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio. |
| GET Uso de Armazenamento | A solicitação "GET Uso de Armazenamento" StorageGRID 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 o caminho / e um parâmetro de consulta personalizado (`?x-ntap-sg-usage` adicionado. |
| OPÇÕES / | Os aplicativos cliente podem enviar `OPTIONS /`solicitações para a porta S3 em um nó de armazenamento, sem fornecer credenciais de autenticação S3, para determinar se o nó de armazenamento está disponível. Você pode usar essa solicitação para monitoramento ou para permitir que balanceadores de carga externos identifiquem quando um nó de armazenamento está inativo. |

### Operações e detalhes de implementação do bucket S3 no StorageGRID

O sistema StorageGRID suporta um máximo de 5.000 buckets por conta de locatário do

## S3.

Cada grid pode ter no máximo 100.000 buckets.

Para suportar 5.000 buckets, cada Storage Node na grid deve ter no mínimo 64 GB de RAM.

As restrições de nome de bucket seguem as restrições da região AWS US Standard, mas você deve restringi-las ainda mais às convenções de nomenclatura DNS para dar suporte a solicitações no estilo de hospedagem virtual do S3.

Veja a seguir para mais informações:

- "Guia do usuário do Amazon Simple Storage Service: cotas, restrições e limitações de buckets"
- "Configurar nomes de domínio de endpoint S3"

As operações ListObjects (GET Bucket) e ListObjectVersions (GET Bucket object versions) são compatíveis com StorageGRID "valores de consistência".

Você pode verificar se as atualizações do último tempo de acesso estão habilitadas ou desabilitadas para buckets individuais. Veja "Obter o último tempo de acesso do bucket".

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

| Operação | Implementação |
| --- | --- |
| CreateBucket | Cria um novo bucket. Ao criar o bucket, você se torna o proprietário dele.<br><br>• Os nomes dos buckets devem obedecer às seguintes regras:<br>◦ Deve ser único em cada sistema StorageGRID (e não apenas único dentro da conta do locatário).<br>◦ Deve ser compatível com DNS.<br>◦ Deve conter no mínimo 3 e no máximo 63 caracteres.<br>◦ Pode ser uma série de um ou mais rótulos, com rótulos adjacentes separados por um ponto. Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens.<br>◦ Não deve ter a aparência de um endereço IP formatado como texto.<br>◦ Não se deve usar pontos em solicitações no estilo de hospedagem virtual. Os pontos causarão problemas com a verificação do certificado curinga do servidor.<br>• Por padrão, os buckets são criados na `us-east-1` região; no entanto, você pode usar o `LocationConstraint` elemento no corpo da requisição para especificar uma região diferente. Ao usar o `LocationConstraint` elemento, você deve especificar o nome exato de uma região que tenha sido definida usando o Grid Manager ou a Grid Management API. Entre em contato com o administrador do sistema se não souber o nome da região que deve usar.<br><br>**Nota**: ocorrerá um erro se a sua solicitação CreateBucket usar uma região que não foi definida no StorageGRID.<br><br>• Você pode incluir o `x-amz-bucket-object-lock-enabled` cabeçalho da solicitação para criar um bucket com o S3 Object Lock ativado. Consulte "Use a API REST S3 para configurar o S3 Object Lock".<br><br>Você deve habilitar o S3 Object Lock ao criar o bucket. Você não pode adicionar ou desabilitar o S3 Object Lock depois que um bucket é criado. O S3 Object Lock requer o versionamento de buckets, que é habilitado automaticamente ao criar o bucket. |
| DeleteBucket | Exclui o bucket. |
| DeleteBucketCors | Remove a configuração CORS do bucket. |
| DeleteBucketEncryption | Remove a criptografia padrão do bucket. Os objetos criptografados existentes permanecem criptografados, mas quaisquer novos objetos adicionados ao bucket não são criptografados. |
| DeleteBucketLifecycle | Exclui a configuração de ciclo de vida do bucket. Consulte "Criar configuração de ciclo de vida do S3". |

| Operação | Implementação |
| --- | --- |
| DeleteBucketPolicy | Exclui a política associada ao bucket. |
| DeleteBucketReplication | Exclui a configuração de replicação associada ao bucket. |
| DeleteBucketTagging | Utiliza o `tagging` subrecurso para remover todas as tags de um bucket.<br><br>**Atenção**: Se uma tag de política ILM não padrão estiver definida para este bucket, haverá uma `NTAP-SG-ILM-BUCKET-TAG` tag de bucket com um valor atribuído a ela. Não envie uma solicitação DeleteBucketTagging se houver uma `NTAP-SG-ILM-BUCKET-TAG` tag de bucket. Em vez disso, envie uma solicitação PutBucketTagging contendo apenas a `NTAP-SG-ILM-BUCKET-TAG` tag e seu valor atribuído para remover todas as outras tags do bucket. Não modifique nem remova a `NTAP-SG-ILM-BUCKET-TAG` tag de bucket. |
| GetBucketAcl | Retorna uma resposta positiva e o ID, DisplayName e a permissão do proprietário do bucket, indicando que o proprietário tem acesso total ao bucket. |
| GetBucketCors | Retorna a `cors`configuração do bucket. |
| GetBucketEncryption | Retorna a configuração de criptografia padrão para o bucket. |
| GetBucketLifecycleConfiguration<br><br>(anteriormente chamado GET Bucket lifecycle) | Retorna a configuração do ciclo de vida do bucket. Consulte "Criar configuração de ciclo de vida do S3". |
| GetBucketLocation | Retorna a região que foi definida usando o elemento `LocationConstraint` na solicitação CreateBucket. Se a região do bucket for `us-east-1`, uma string vazia será retornada para a região. |
| GetBucketNotificationConfiguration<br><br>(anteriormente chamado de GET Bucket notification) | Retorna a configuração de notificação associada ao bucket. |
| GetBucketPolicy | Retorna a política associada ao bucket. |
| GetBucketReplication | Retorna a configuração de replicação associada ao bucket. |
| GetBucketTagging | Utiliza o `tagging` subrecurso para retornar todas as tags de um bucket.<br><br>**Atenção**: Se uma tag de política ILM não padrão estiver definida para este bucket, haverá uma tag de bucket `NTAP-SG-ILM-BUCKET-TAG` com um valor atribuído a ela. Não modifique nem remova esta tag. |

| Operação | Implementação |
| --- | --- |
| GetBucketVersioning | Esta implementação utiliza o `versioning` subrecurso para retornar o estado de versionamento de um bucket.<br>• *blank*: O versionamento nunca foi ativado (o bucket está "Não versionado")<br>• Ativado: o versionamento está ativado<br>• Suspenso: o versionamento estava ativado anteriormente e está suspenso |
| GetObjectLockConfiguration | Retorna o modo de retenção padrão do bucket e o período de retenção padrão, se configurados.<br>Consulte "Use a API REST S3 para configurar o S3 Object Lock". |
| HeadBucket | Determina se um bucket existe e se você tem permissão para acessá-lo.<br>Esta operação retorna:<br>• `x-ntap-sg-bucket-id`: o UUID do bucket no formato UUID.<br>• `x-ntap-sg-trace-id`: o ID de rastreamento exclusivo da solicitação associada. |
| ListObjects e ListObjectsV2<br>(anteriormente chamado GET Bucket) | Retorna alguns ou todos (até 1.000) os objetos em um bucket. A Storage Class para objetos pode ter um dos dois valores, mesmo que o objeto tenha sido ingerido com a `REDUCED_REDUNDANCY` storage class option:<br>• `STANDARD`, o que indica que o objeto está armazenado em um pool de storage composto por Storage Nodes.<br>• `GLACIER`, o que indica que o objeto foi movido para o bucket externo especificado pelo Cloud Storage Pool.<br>Se o bucket contiver um grande número de chaves excluídas com o mesmo prefixo, a resposta pode incluir algumas `CommonPrefixes` que não contêm chaves.<br>Para as solicitações HeadObject e ListObject, o StorageGRID retorna os timestamps LastModified com precisões diferentes, enquanto a AWS retorna os timestamps com a mesma precisão, como mostrado nos exemplos a seguir:<br>• StorageGRID HeadObject: ""LastModified": "2024-09-26T16:43:24+00:00"<br>• StorageGRID ListObject: "LastModified": "2024-09-26T16:43:24.931000+00:00"<br>• AWS HeadObject: "LastModified": "2023-10-17T00:19:54+00:00"<br>• AWS ListObject: "LastModified": "2023-10-17T00:19:54+00:00" |

| Operação | Implementação |
| --- | --- |
| ListObjectVersions<br><br>(anteriormente chamado de GET Bucket Object versions) | Com acesso de LEITURA em um bucket, usar essa operação com o `versions` subrecurso lista os metadados de todas as versões dos objetos no bucket. |
| PutBucketCors | Define a configuração CORS para um bucket, permitindo que ele atenda solicitações de origem cruzada. O compartilhamento de recursos de origem cruzada (CORS) é um mecanismo de segurança que permite que aplicativos web cliente em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket S3 chamado `images` para armazenar imagens. Ao definir a configuração CORS para o bucket `images`, você pode permitir que as imagens nesse bucket sejam exibidas no site `http://www.example.com`. |
| PutBucketEncryption | Define o estado de criptografia padrão de um bucket existente. Quando a criptografia no nível do bucket está habilitada, todos os novos objetos adicionados ao bucket são criptografados. O StorageGRID oferece suporte à criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID. Ao especificar a regra de configuração de criptografia do lado do servidor, defina o parâmetro `SSEAlgorithm` como `AES256` e não use o parâmetro `KMSMasterKeyID`.<br><br>A configuração de criptografia padrão do bucket é ignorada se a solicitação de upload do objeto já especificar criptografia (ou seja, se a solicitação incluir o `x-amz-server-side-encryption-*` cabeçalho de solicitação). |

| Operação | Implementação |
| --- | --- |
| PutBucketLifecycleConfiguration<br><br>(anteriormente denominado PUT Bucket lifecycle) | Cria uma nova configuração de ciclo de vida para o bucket ou substitui uma configuração de ciclo de vida existente. O StorageGRID suporta até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML:<br><br>• Validade (dias, data, ExpiredObjectDeleteMarker)<br>• NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays)<br>• Filtro (Prefixo, Tag)<br>• Status<br>• ID<br><br>StorageGRID não suporta estas ações:<br><br>• AbortIncompleteMultipartUpload<br>• Transição<br><br>Consulte "Criar configuração de ciclo de vida do S3". Para entender como a ação de expiração no ciclo de vida do bucket interage com as instruções de posicionamento do ILM, consulte "Como o ILM opera ao longo do ciclo de vida de um objeto".<br><br>**Nota**: a configuração do ciclo de vida do bucket pode ser usada com buckets que têm o S3 Object Lock ativado, mas a configuração do ciclo de vida do bucket não é compatível com buckets legados Compliant. |

| Operação | Implementação |
| --- | --- |
| PutBucketNotificationConfiguration<br><br>(anteriormente chamada de PUT Bucket notification) | Configura as notificações para o bucket usando o XML de configuração de notificações incluído no corpo da solicitação. Você deve estar ciente dos seguintes detalhes de implementação:<br><br>• StorageGRID suporta tópicos do Amazon Simple Notification Service (Amazon SNS), tópicos do Kafka ou endpoints de webhook como destinos. Endpoints do Simple Queue Service (SQS) ou do AWS Lambda não são suportados.<br>• O destino das notificações deve ser especificado como o URN de um endpoint do StorageGRID. Os endpoints podem ser criados usando o Tenant Manager ou a Tenant Management API.<br><br>O endpoint deve existir para que a configuração de notificação seja bem-sucedida. Se o endpoint não existir, um erro `400 Bad Request` é retornado com o código `InvalidArgument`.<br><br>• Não é possível configurar uma notificação para os seguintes tipos de evento. Esses tipos de evento **não** são suportados.<br>◦ `s3:ReducedRedundancyLostObject`<br>◦ `s3:ObjectRestore:Completed`<br>• As notificações de eventos enviadas pelo StorageGRID usam o formato JSON padrão, exceto que não incluem algumas chaves e usam valores específicos para outras, conforme mostrado na lista a seguir:<br>◦ **eventSource**<br><br>`sgws:s3`<br><br>◦ **awsRegion**<br><br>não incluído<br><br>◦ **x-amz-id-2**<br><br>não incluído<br><br>◦ **arn**<br><br>`urn:sgws:s3:::bucket_name` |
| PutBucketPolicy | Define a política associada ao bucket. Consulte "Use políticas de acesso a buckets e grupos". |

| Operação | Implementação |
| --- | --- |
| PutBucketReplication | Configura "StorageGRID CloudMirror replicação" para o bucket usando o XML de configuração de replicação fornecido no corpo da solicitação. Para a replicação CloudMirror, você deve estar ciente dos seguintes detalhes de implementação:<br><br>• StorageGRID suporta apenas a V1 da configuração de replicação. Isso significa que StorageGRID não suporta o uso do `Filter` elemento para regras e segue as convenções da V1 para exclusão de versões de objetos. Para obter detalhes, consulte "Guia do usuário do Amazon Simple Storage Service: configuração de replicação".<br>• A replicação de buckets pode ser configurada em buckets versionados ou não versionados.<br>• Você pode especificar um bucket de destino diferente em cada regra do XML de configuração de replicação. Um bucket de origem pode replicar para mais de um bucket de destino.<br>• Os buckets de destino devem ser especificados como o URN dos endpoints do StorageGRID, conforme especificado no Tenant Manager ou na API de Gerenciamento de Tenant. Consulte "Configurar a replicação CloudMirror".<br><br>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: URN`.<br><br>• Você não precisa especificar um `Role` no XML de configuração. Esse valor não é usado pelo StorageGRID e será ignorado se for enviado.<br>• Se você omitir a classe de armazenamento do XML de configuração, StorageGRID usará a classe de armazenamento `STANDARD` por padrão.<br>• Se você excluir um objeto do bucket de origem ou excluir o próprio bucket de origem, o comportamento da replicação entre regiões será o seguinte:<br>◦ Se você excluir o objeto ou bucket antes que ele seja replicado, o objeto/bucket não será replicado e você não será notificado.<br>◦ Se você excluir o objeto ou bucket após ele ter sido replicado, o StorageGRID segue o comportamento padrão de exclusão do Amazon S3 para a V1 da replicação entre regiões. |

| Operação | Implementação |
| --- | --- |
| PutBucketTagging | Utiliza o `tagging` sub-recurso para adicionar ou atualizar um conjunto de tags para um bucket. Ao adicionar tags ao bucket, esteja ciente das seguintes limitações:<br><br>• Tanto StorageGRID quanto Amazon S3 suportam até 50 tags por bucket.<br>• As tags associadas a um bucket devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode.<br>• Os valores das tags podem ter até 256 caracteres Unicode.<br>• As chaves e os valores diferenciam maiúsculas de minúsculas.<br><br>**Atenção**: Se uma tag de política ILM não padrão for definida para este bucket, haverá uma `NTAP-SG-ILM-BUCKET-TAG` tag de bucket com um valor atribuído a ela. Certifique-se de que a `NTAP-SG-ILM-BUCKET-TAG` tag de bucket esteja incluída com o valor atribuído em todas as solicitações PutBucketTagging. Não modifique nem remova esta tag.<br><br>**Nota**: Esta operação irá sobrescrever quaisquer tags existentes no bucket. Se alguma tag existente for omitida do conjunto, essa tag será removida do bucket. |
| PutBucketVersioning | Utiliza o `versioning` subrecurso para definir o estado de versionamento de um bucket existente. Você pode definir o estado de versionamento com um dos seguintes valores:<br><br>• Ativado: habilita o versionamento para os objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo.<br>• Suspenso: desativa o versionamento para os objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão `null`. |
| PutObjectLockConfiguration | Configura ou remove o modo de retenção padrão do bucket e o período de retenção padrão.<br><br>Se o período de retenção padrão for modificado, a data de retenção das versões existentes do objeto permanece a mesma e não é recalculada usando o novo período de retenção padrão.<br><br>Veja "Use a API REST S3 para configurar o S3 Object Lock" para obter informações detalhadas. |

### Operações em objetos

#### Como o StorageGRID implementa operações da API REST do S3 para objetos

Esta seção descreve como o sistema StorageGRID implementa as operações da API REST do S3 para objetos.

As seguintes condições aplicam-se a todas as operações de objeto:

- StorageGRID "valores de consistência" é compatível com todas as operações em objetos, com exceção

das seguintes:

- GetObjectAcl
- `OPTIONS /`
- PutObjectLegalHold
- PutObjectRetention
- SelectObjectContent

- Solicitações conflitantes de clientes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio "latest-wins". O momento da avaliação do "latest-wins" é determinado quando o sistema StorageGRID conclui uma determinada solicitação, e não quando os clientes S3 iniciam uma operação.
- Todos os objetos em um bucket do StorageGRID pertencem ao proprietário do bucket, incluindo objetos criados por um usuário anônimo ou por outra conta.

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

| Operação | Implementação |
| --- | --- |
| DeleteObject | Ao processar uma solicitação DeleteObject, StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais de armazenamento. Se for bem-sucedido, StorageGRID retorna uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas em 30 segundos (por exemplo, porque um local está temporariamente indisponível), StorageGRID coloca as cópias em fila para remoção e então indica sucesso ao cliente.<br><br>**Restrições**<br>• A autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados.<br>• Os `If-None` e `If-None-Match` cabeçalhos são aceitos, mas não funcionais.<br><br>**Controle de versões**<br>Para remover uma versão específica, o solicitante deve ser o proprietário do bucket e usar o `versionId` sub-recurso. Usar esse sub-recurso exclui permanentemente a versão. Se o `versionId` corresponder a um marcador de exclusão, o cabeçalho de resposta `x-amz-delete-marker` é retornado definido como `true`.<br>• Se um objeto for excluído sem o `versionId` sub-recurso em um bucket com versionamento ativado, isso resulta na geração de um marcador de exclusão. O `versionId` marcador de exclusão é retornado usando o `x-amz-version-id` cabeçalho de resposta, e o `x-amz-delete-marker` cabeçalho de resposta é retornado definido como `true`.<br>• Se um objeto for excluído sem o `versionId` sub-recurso em um bucket com versionamento suspenso, isso resulta na exclusão permanente de uma versão "null" já existente ou de um marcador de exclusão "null", e na geração de um novo marcador de exclusão "null". O cabeçalho de resposta `x-amz-delete-marker` é retornado definido como `true`.<br><br>**Nota**: Em certos casos, vários marcadores de exclusão podem existir para um objeto.<br><br>Veja "Use a API REST S3 para configurar o S3 Object Lock" para saber como excluir versões de objetos no modo GOVERNANÇA. |
| DeleteObjects<br><br>(anteriormente chamado de DELETE Multiple Objects) | A autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados.<br><br>Vários objetos podem ser excluídos na mesma mensagem de solicitação.<br><br>Veja "Use a API REST S3 para configurar o S3 Object Lock" para saber como excluir versões de objetos no modo GOVERNANÇA. |

| Operação | Implementação |
| --- | --- |
| DeleteObjectTagging | Utiliza o `tagging` subrecurso para remover todas as tags de um objeto.<br><br>**Controle de versões**<br><br>Se o `versionId`parâmetro de consulta não for especificado na solicitação, a operação exclui todas as tags da versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status " MethodNotAllowed " será retornado com o cabeçalho de resposta `x-amz-delete-marker` definido como `true`. |
| GetObject | "GetObject" |
| GetObjectAcl | Se as credenciais de acesso necessárias forem fornecidas para a conta, a operação retorna uma resposta positiva e o ID, DisplayName e a Permissão do proprietário do objeto, indicando que o proprietário tem acesso total ao objeto. |
| GetObjectLegalHold | "Use a API REST S3 para configurar o S3 Object Lock" |
| GetObjectRetention | "Use a API REST S3 para configurar o S3 Object Lock" |
| GetObjectTagging | Utiliza o `tagging` subrecurso para retornar todas as tags de um objeto.<br><br>**Controle de versões**<br><br>Se o `versionId` parâmetro de consulta não for especificado na solicitação, a operação retorna todas as tags da versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status " MethodNotAllowed " será retornado com o cabeçalho de resposta `x-amz-delete-marker` definido como `true`. |
| HeadObject | "HeadObject" |
| RestoreObject | "RestoreObject" |
| PutObject | "PutObject" |
| CopyObject<br><br>(anteriormente denominado PUT Object - Copy) | "CopyObject" |
| PutObjectLegalHold | "Use a API REST S3 para configurar o S3 Object Lock" |
| PutObjectRetention | "Use a API REST S3 para configurar o S3 Object Lock" |

| Operação | Implementação |
| --- | --- |
| PutObjectTagging | Utiliza o `tagging` subrecurso para adicionar um conjunto de tags a um objeto existente.<br><br>**Limites de tags de objeto**<br>Você pode adicionar tags a novos objetos ao carregá-los ou pode adicioná-las a objetos existentes. Tanto StorageGRID quanto Amazon S3 suportam até 10 tags por objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode e os valores de tag podem ter até 256 caracteres Unicode. Chaves e valores diferenciam maiúsculas de minúsculas.<br><br>**Atualizações de tags e comportamento de ingestão**<br>Quando você usa PutObjectTagging para atualizar as tags de um objeto, o StorageGRID não o ingere novamente. Isso significa que a opção de Comportamento de Ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento do objeto acionadas pela atualização são feitas quando o ILM é reavaliado pelos processos normais de ILM em segundo plano.<br><br>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-necessário não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível.<br><br>**Resolução de conflitos**<br>Solicitações conflitantes de clientes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio "latest-wins". O momento da avaliação do "latest-wins" é determinado quando o sistema StorageGRID conclui uma determinada solicitação, e não quando os clientes S3 iniciam uma operação.<br><br>**Controle de versões**<br>Se o `versionId`parâmetro de consulta não for especificado na solicitação, a operação adiciona tags à versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status ""MethodNotAllowed"" é retornado com o cabeçalho de resposta `x-amz-delete-marker`definido como `true`. |
| SelectObjectContent | "SelectObjectContent" |

#### Operações Amazon S3 Select suportadas no StorageGRID

StorageGRID oferece suporte às seguintes cláusulas SELECT do Amazon S3, tipos de dados e operadores para o "Comando SelectObjectContent".

Quaisquer itens não listados não são suportados.

Para sintaxe, consulte "SelectObjectContent". Para mais informações sobre S3 Select, consulte o "Documentação da AWS para S3 Select".

Somente contas de locatário com o S3 Select ativado podem emitir consultas SelectObjectContent. Consulte o "Considerações e requisitos para usar o S3 Select".

**Cláusulas**

- Lista de seleção
- Cláusula FROM
- Cláusula WHERE
- Cláusula LIMIT

**Tipos de dados**

- bool
- inteiro
- string
- float
- decimal, numérico
- carimbo de data/hora

**Operadores**

**Operadores lógicos**

- E
- NÃO
- OU

**Operadores de comparação**

- <
- >
- ⇐
- >=
- =
- =
- <>
- !=
- ENTRE
- EM

#### Operadores de correspondência de padrões

- CURTIR
- _
- %

#### Operadores unitários

- É NULO
- NÃO É NULO

#### Operadores matemáticos

- +
- -
- *
- /
- %

StorageGRID segue a precedência do operador Amazon S3 Select.

#### Funções agregadas

- AVG()
- COUNT(*)
- MAX()
- MIN()
- SOMA()

#### Funções condicionais

- CASO
- COALESCE
- NULLIF

#### Funções de conversão

- CAST (para tipo de dados suportado)

#### Funções de data

- DATE_ADD
- DATE_DIFF
- EXTRAIR
- TO_STRING
- TO_TIMESTAMP

- UTCNOW

**Funções de string**

- CHAR_LENGTH, CHARACTER_LENGTH
- MAIS BAIXO
- SUBSTRING
- TRIM
- SUPERIOR

#### Como StorageGRID usa criptografia do lado do servidor

A criptografia do lado do servidor permite que você proteja seus dados de objeto em repouso. StorageGRID criptografa os dados ao gravar o objeto e os descriptografa quando você acessa o objeto.

Se você deseja usar criptografia do lado do servidor, 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 envia uma solicitação S3 para armazenar um objeto, o StorageGRID criptografa o objeto com uma chave exclusiva. Quando você envia uma solicitação S3 para recuperar o objeto, o StorageGRID usa a chave armazenada para descriptografar o objeto.
- **SSE-C (server-side encryption with customer-provided keys)**: Ao enviar uma solicitação ao S3 para armazenar um objeto, você fornece sua própria chave de criptografia. Ao recuperar um objeto, você fornece a mesma chave de criptografia como parte da sua solicitação. Se as duas chaves de criptografia coincidirem, o objeto é descriptografado e seus dados do objeto são retornados.

  Embora o StorageGRID gerencie todas as operações de criptografia e descriptografia de objetos, você deve gerenciar as chaves de criptografia que fornecer.

  > 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 em nível de bucket ou de grid serão ignoradas.

**Use SSE**

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

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

O cabeçalho de solicitação SSE é compatível com as seguintes operações de objeto:

- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"

### Use SSE-C

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

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

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

- "GetObject"
- "HeadObject"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

### Considerações sobre o uso de criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

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

- Você deve usar https.

> StorageGRID rejeita quaisquer solicitações feitas via http ao usar SSE-C. Por questões de segurança, você deve considerar qualquer chave enviada acidentalmente via http como comprometida. Descarte a chave e faça a rotação conforme apropriado.

- O ETag na resposta não é o MD5 dos dados do objeto.
- Você deve gerenciar o mapeamento das chaves de criptografia para os objetos. StorageGRID não armazena chaves de criptografia. Você é responsável por controlar a chave de criptografia que fornecer para cada objeto.
- Se o seu bucket tiver o versionamento ativado, cada versão do objeto deverá ter sua própria chave de criptografia. Você é responsável por controlar a chave de criptografia usada para cada versão do objeto.
- Como você gerencia as chaves de criptografia no lado do cliente, também deve gerenciar quaisquer

medidas de segurança adicionais, como a rotação de chaves, no lado do cliente.

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

- Se a replicação entre grades ou a replicação CloudMirror estiver configurada para o bucket, você não poderá ingerir objetos SSE-C. A operação de ingestão falhará.

**Informações relacionadas**

"Guia do usuário do Amazon S3: usando criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)"

#### Crie uma cópia de um objeto no StorageGRID com a solicitação S3 CopyObject

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

**Resolver conflitos**

Solicitações conflitantes de clientes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio "latest-wins". O momento da avaliação do "latest-wins" é determinado quando o sistema StorageGRID conclui uma determinada solicitação, e não quando os clientes S3 iniciam uma operação.

**Tamanho do objeto**

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

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

> Se você atualizou do StorageGRID 11.6 ou anterior, o alerta "Tamanho do objeto S3 PUT muito grande" será acionado se você tentar fazer o upload de um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11.7 ou 11.8, o alerta não será acionado nesse caso. No entanto, para alinhar com o padrão AWS S3, as versões futuras do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

**Caracteres UTF-8 nos metadados do usuário**

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

StorageGRID não analisa nem interpreta caracteres UTF-8 escapados incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. 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.
- 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 nome-valor contendo metadados definidos pelo usuário
- `x-amz-metadata-directive`: O valor padrão é `COPY`, o que permite que você copie o objeto e os metadados associados.

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

- Cabeçalhos da solicitação S3 Object Lock:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular o modo de versão do objeto e a data de retenção. Consulte "Use a API REST S3 para configurar o S3 Object Lock".

- Cabeçalhos de solicitação SSE:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Consulte Cabeçalhos de solicitação para criptografia do lado do servidor

### Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `If-Match`

  O `If-Match header` é aceito, mas não funcional.

- `If-None-Match`

  O `If-None-Match header` é aceito, mas não funcional.

- `x-amz-checksum-algorithm`

  Ao copiar um objeto, se o objeto de origem tiver um checksum, StorageGRID não copia esse valor de checksum para o novo objeto. Esse comportamento se aplica independentemente de você tentar usar `x-amz-checksum-algorithm` na solicitação do objeto.

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

### Opções de classe de armazenamento

O `x-amz-storage-class`cabeçalho da solicitação é compatível e afeta quantas cópias de objetos o StorageGRID cria se a regra ILM correspondente usar o Dual commit ou Balanced "opção de ingestão".

- `STANDARD`

  (Padrão) Especifica uma operação de ingestão de confirmação dupla quando a regra ILM usa a opção Dual commit ou quando a opção Balanced recorre à criação de cópias intermediárias.

- `REDUCED_REDUNDANCY`

  Especifica uma operação de ingestão de confirmação única quando a regra ILM usa a opção de confirmação dupla ou quando a opção balanceada recorre à criação de cópias intermediárias.

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

### Usando x-amz-copy-source em CopyObject

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

Se a origem e o destino coincidirem 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, StorageGRID não reingere o objeto. Isso tem duas consequências importantes:

- Não é possível usar CopyObject para criptografar um objeto existente no local ou para alterar a criptografia de um objeto existente no local. Se você fornecer o `x-amz-server-side-encryption` cabeçalho ou o `x-amz-server-side-encryption-customer-algorithm` cabeçalho, StorageGRID rejeita a solicitação e retorna `XNotImplemented`.
- A opção de Comportamento de Ingestão especificada na regra ILM correspondente não é utilizada. Quaisquer alterações no posicionamento do objeto que sejam acionadas pela atualização são feitas quando o ILM é reavaliado pelos processos ILM normais 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-necessário não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível.

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

Se você "usar criptografia do lado do servidor" fizer isso, os cabeçalhos da solicitação que você fornecer dependerão de o objeto de origem estar criptografado e de você planejar criptografar o objeto de destino.

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

  > As chaves de criptografia fornecidas por você nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para "usando criptografia do lado do servidor".

- Se você deseja criptografar o objeto de destino (a cópia) com uma chave exclusiva gerenciada pelo StorageGRID (SSE), inclua este cabeçalho na solicitação CopyObject:
  - `x-amz-server-side-encryption`

O `server-side-encryption` 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 versões

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

#### Recuperar um objeto de um bucket no StorageGRID com a solicitação GetObject

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

### GetObject e objetos multipartes

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

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

### Caracteres UTF-8 nos metadados do usuário

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

### Cabeçalho de solicitação compatível

O seguinte cabeçalho de solicitação é compatível:

- `x-amz-checksum-mode`: especificar `ENABLED`

  O `Range`cabeçalho não é compatível com `x-amz-checksum-mode` para GetObject. Quando você inclui `Range` na solicitação com `x-amz-checksum-mode` ativado, StorageGRID não retorna um valor de checksum na resposta.

### Cabeçalho de solicitação não suportado

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

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

### Controle de versões

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

### Cabeçalhos de solicitação para criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Utilize os três cabeçalhos se o objeto estiver criptografado com uma chave exclusiva que você forneceu.

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

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em "Use criptografia do lado do servidor".

### Comportamento de GetObject para objetos do Cloud Storage Pool

Se um objeto foi armazenado em um "Pool de storage em nuvem", o comportamento de uma solicitação GetObject depende do estado do objeto. Veja "HeadObject" para mais detalhes.

> Se um objeto estiver armazenado em um Cloud Storage Pool e uma ou mais cópias do objeto também existirem na grid, as solicitações GetObject tentarão recuperar os dados da grid antes de recuperá-los do Cloud Storage Pool.

| Estado do objeto | Comportamento de GetObject |
|---|---|
| Objeto inserido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento | `200 OK`<br><br>Uma cópia do objeto é recuperada. |
| Objeto no pool de Cloud Storage, mas ainda não foi transferido para um estado não recuperável | `200 OK`<br><br>Uma cópia do objeto é recuperada. |
| Objeto passou para um estado não recuperável | `403 Forbidden`, `InvalidObjectState`<br><br>Utilize uma solicitação "RestoreObject" para restaurar o objeto a um estado recuperável. |
| Objeto em processo de restauração a partir de um estado irrecuperável | `403 Forbidden`, `InvalidObjectState`<br><br>Aguarde a conclusão da solicitação RestoreObject. |

| Estado do objeto | Comportamento de GetObject |
| --- | --- |
| Objeto totalmente restaurado ao pool de storage em nuvem | `200 OK`<br><br>Uma cópia do objeto é recuperada. |

#### Objetos multipartes ou segmentados em um pool de storage em nuvem

Se você carregou um objeto multipart ou se StorageGRID dividiu um objeto grande em segmentos, StorageGRID determina se o objeto está disponível no Cloud Storage Pool ao amostrar um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação GetObject pode retornar incorretamente `200 OK` quando algumas partes do objeto já foram transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não foram restauradas.

Nesses casos:

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

#### GetObject e replicação entre grades

Se você estiver usando "federação de grid" e "replicação entre grids" estiver habilitado para um bucket, o cliente pode verificar o status de replicação de um objeto emitindo uma solicitação GetObject. A resposta inclui o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

| Grid | Status de replicação |
| --- | --- |
| Fonte | • **CONCLUÍDO**: A replicação foi bem-sucedida.<br>• **PENDENTE**: O objeto ainda não foi replicado.<br>• **FALHA**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro. |
| Destino | **RÉPLICA**: O objeto foi replicado da grid de origem. |

> StorageGRID não suporta o `x-amz-replication-status` header.

##### Recuperar metadados de um objeto no StorageGRID com a solicitação S3 HeadObject

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

#### HeadObject e objetos multipartes

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

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

### Caracteres UTF-8 nos metadados do usuário

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

### Cabeçalho de solicitação compatível

O seguinte cabeçalho de solicitação é compatível:

- `x-amz-checksum-mode`

  O `partNumber`parâmetro e o `Range`cabeçalho não são suportados com `x-amz-checksum-mode`para HeadObject. Quando você os inclui na solicitação com `x-amz-checksum-mode`ativado, StorageGRID não retorna um valor de checksum na resposta.

### Cabeçalho de solicitação não suportado

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

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

### Controle de versões

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

### Cabeçalhos de solicitação para criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

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

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

> ⚠ As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em "Use criptografia do lado do servidor".

### HeadObject respostas para objetos do Cloud Storage Pool

Se o objeto estiver armazenado em um "Pool de storage em nuvem", 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 storage em nuvem, opcionalmente transitado para um estado não recuperável e restaurado.

| Estado do objeto | Resposta a HeadObject |
|---|---|
| Objeto inserido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento | `200 OK` (Nenhum cabeçalho de resposta especial é retornado.) |
| Objeto no pool de Cloud Storage, mas ainda não foi transferido para um estado não recuperável | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`<br><br>Até que o objeto seja levado a um estado irrecuperável, o valor para `expiry-date` é definido para um momento distante no futuro. O momento exato da transição não é controlado pelo sistema StorageGRID. |
| O objeto passou para um estado não recuperável, mas pelo menos uma cópia também existe na grid | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`<br><br>O valor para `expiry-date` é definido para um momento distante no futuro.<br><br>**Nota**: Se a cópia na grade não estiver disponível (por exemplo, se um Storage Node estiver inativo), você deve emitir uma "RestoreObject" solicitação para restaurar a cópia do Cloud Storage Pool antes de conseguir recuperar o objeto. |

| Estado do objeto | Resposta a HeadObject |
| --- | --- |
| O objeto passou para um estado não recuperável e não existe nenhuma cópia no grid | `200 OK`<br><br>`x-amz-storage-class: GLACIER` |
| Objeto em processo de restauração a partir de um estado irrecuperável | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="true"` |
| Objeto totalmente restaurado ao pool de storage em nuvem | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`<br><br>O `expiry-date` indica quando o objeto no pool de storage em nuvem será retornado a um estado não recuperável. |

### Objetos multipartes ou segmentados no Cloud Storage Pool

Se você carregou um objeto multipart ou se StorageGRID dividiu um objeto grande em segmentos, StorageGRID determina se o objeto está disponível no Cloud Storage Pool ao amostrar um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação HeadObject pode retornar incorretamente `x-amz-restore: ongoing-request="false"` quando algumas partes do objeto já foram transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não foram restauradas.

### HeadObject e replicação entre grades

Se você estiver usando "federação de grid" e "replicação entre grids" estiver habilitado para um bucket, o cliente S3 pode verificar o status de replicação de um objeto emitindo uma solicitação HeadObject. A resposta inclui o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

| Grid | Status de replicação |
| --- | --- |
| Fonte | • **CONCLUÍDO**: A replicação foi bem-sucedida.<br>• **PENDENTE**: O objeto ainda não foi replicado.<br>• **FALHA**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro. |
| Destino | **RÉPLICA**: O objeto foi replicado da grid de origem. |

StorageGRID não suporta o `x-amz-replication-status` header.

#### Adicionar um objeto a um bucket no StorageGRID com a solicitação S3 PutObject

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

### Resolver conflitos

Solicitações conflitantes de clientes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio "latest-wins". O momento da avaliação do "latest-wins" é determinado quando o sistema StorageGRID conclui uma determinada solicitação, e não quando os clientes S3 iniciam uma operação.

### Tamanho do objeto

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

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

Se você atualizou do StorageGRID 11.6 ou anterior, o alerta "Tamanho do objeto S3 PUT muito grande" será acionado se você tentar fazer o upload de um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11.7 ou 11.8, o alerta não será acionado nesse caso. No entanto, para alinhar com o padrão AWS S3, as versões futuras do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

### Tamanho dos metadados do usuário

Amazon S3 limita o tamanho dos metadados definidos pelo usuário em cada cabeçalho de solicitação PUT a 2 KB. StorageGRID limita os metadados do usuário a 24 KiB. O tamanho dos metadados definidos pelo usuário é medido pela soma do número de bytes na codificação UTF-8 de cada chave e valor.

### Caracteres UTF-8 nos metadados do usuário

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

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

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

### Limites de tags de objeto

Você pode adicionar tags a novos objetos ao carregá-los ou pode adicioná-las a objetos existentes. Tanto StorageGRID quanto Amazon S3 suportam até 10 tags por objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode e os valores de tag podem ter até 256 caracteres Unicode. Chaves e valores diferenciam maiúsculas de minúsculas.

### Propriedade do objeto

No StorageGRID, todos os objetos pertencem à conta proprietária do bucket, incluindo objetos criados por uma conta que não seja proprietária ou por um usuário anônimo.

### Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

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

  Ao especificar `aws-chunked`para `Content-Encoding`StorageGRID, o StorageGRID não verifica os seguintes itens:

  - StorageGRID não verifica o `chunk-signature` em relação aos dados em blocos.
  - StorageGRID não verifica o valor que você fornece para `x-amz-decoded-content-length` em relação ao objeto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  A codificação de transferência em partes é suportada se `aws-chunked` a assinatura da carga também for usada.
- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguido por um par nome-valor contendo metadados definidos pelo usuário.

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

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

  Se você deseja usar a opção **Hora de criação definida pelo usuário** como a hora de referência para uma regra ILM, você deve usar `creation-time` como o nome do metadado que registra quando o objeto foi criado. Por exemplo:

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

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

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

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

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular o modo de versão do objeto e a data de retenção. Consulte "Use a API REST S3 para configurar o S3 Object Lock".
- Cabeçalhos de solicitação SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Consulte Cabeçalhos de solicitação para criptografia do lado do servidor

#### Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `If-Match`

  O `If-Match header` é aceito, mas não funcional.
- `If-None-Match`

  O `If-None-Match header` é aceito, mas não funcional.
- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

  O `x-amz-website-redirect-location`cabeçalho retorna `XNotImplemented`.

#### Opções de classe de armazenamento

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

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

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

- `STANDARD` (Padrão)
  - **Confirmação dupla**: Se a regra ILM especificar a opção de confirmação dupla para o comportamento de ingestão, assim que um objeto for ingerido, uma segunda cópia desse objeto será criada e distribuída para um nó de armazenamento diferente (confirmação dupla). Quando a ILM é avaliada, o StorageGRID determina se essas cópias intermediárias iniciais atendem às instruções de posicionamento na regra. Se não atenderem, novas cópias do objeto podem precisar ser criadas em locais diferentes e as cópias intermediárias iniciais podem precisar ser excluídas.
  - **Balanceado**: Se a regra ILM especificar a opção Balanceado e StorageGRID não puder criar imediatamente todas as cópias especificadas na regra, StorageGRID faz duas cópias intermediárias em diferentes nós de armazenamento.

    Se StorageGRID puder criar imediatamente todas as cópias de objetos especificadas na regra ILM (posicionamento síncrono), o `x-amz-storage-class` cabeçalho não terá efeito.
- `REDUCED_REDUNDANCY`
  - **Confirmação dupla**: Se a regra ILM especificar a opção de confirmação dupla para o comportamento de ingestão, StorageGRID cria uma única cópia intermediária à medida que o objeto é ingerido (confirmação única).
  - **Balanceado**: Se a regra ILM especificar a opção Balanceado, StorageGRID cria uma única cópia intermediária somente se o sistema não puder criar imediatamente todas as cópias especificadas na regra. Se StorageGRID puder realizar o posicionamento síncrono, este cabeçalho não terá efeito. A `REDUCED_REDUNDANCY` opção é mais adequada quando a regra ILM correspondente ao objeto cria uma única cópia replicada. Nesse caso, usar `REDUCED_REDUNDANCY` essa opção elimina a criação e exclusão desnecessárias de uma cópia extra do objeto para cada operação de ingestão.

  O uso da `REDUCED_REDUNDANCY`opção não é recomendado em outras circunstâncias. `REDUCED_REDUNDANCY` Isso aumenta o risco de perda de dados de objeto durante a ingestão. Por exemplo, você pode perder dados se a cópia única for armazenada inicialmente em um Storage Node que falhe antes que a avaliação do ILM possa ocorrer.

> Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se existir apenas uma cópia replicada de um objeto, esse objeto é perdido se um Storage Node falhar ou apresentar um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como upgrades.

A especificação `REDUCED_REDUNDANCY`afeta apenas quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas ILM ativas e não resulta no armazenamento de dados em níveis mais baixos de redundância no sistema StorageGRID.

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

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

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

- **SSE**: Use o seguinte cabeçalho se você quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID.
  - `x-amz-server-side-encryption`

    Quando o `x-amz-server-side-encryption`cabeçalho não está incluído na solicitação PutObject, o "configuração de criptografia de objeto armazenado" é omitido da resposta PutObject.

- **SSE-C**: Utilize 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`: Especifique `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.

> As chaves de criptografia fornecidas por você nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para "usando criptografia do lado do servidor".

> Se um objeto for criptografado com SSE ou SSE-C, quaisquer configurações de criptografia em nível de bucket ou de grid serão ignoradas.

### Controle de versões

Se o versionamento estiver habilitado para um bucket, um identificador único `versionId` é gerado automaticamente para a versão do objeto armazenado. Esse `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho da resposta.

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

### Cálculos de assinatura para o cabeçalho Authorization

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

- StorageGRID não exige que os `host` cabeçalhos sejam incluídos em `CanonicalHeaders`.
- StorageGRID não precisa `Content-Type`ser incluído em `CanonicalHeaders`.
- StorageGRID não exige que os cabeçalhos `x-amz-*` sejam incluídos em `CanonicalHeaders`.

> Como prática recomendada geral, sempre inclua esses cabeçalhos dentro de `CanonicalHeaders` para garantir que sejam verificados; no entanto, se você excluir esses cabeçalhos, StorageGRID não retorna um erro.

Para obter detalhes, consulte "Cálculos de assinatura para o cabeçalho de autorização: transferência de carga em um único bloco (AWS Signature Version 4)".

**Informações relacionadas**

- "Gerencie objetos com ILM"
- "Referência da API do Amazon Simple Storage Service: PutObject"

#### Restaurar um objeto no StorageGRID com a solicitação S3 RestoreObject

Você pode usar a solicitação S3 RestoreObject para restaurar um objeto armazenado em um Cloud Storage Pool.

**Tipo de solicitação compatível**

StorageGRID suporta apenas solicitações RestoreObject para restaurar um objeto. Ele não suporta o tipo de restauração `SELECT`. As solicitações Select retornam `XNotImplemented`.

**Controle de versões**

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

**Comportamento de RestoreObject em objetos do Cloud Storage Pool**

Se um objeto foi armazenado em um "Pool de storage em nuvem", uma solicitação RestoreObject terá o seguinte comportamento, com base no estado do objeto. Veja "HeadObject" para mais detalhes.

> Se um objeto estiver armazenado em um Cloud Storage Pool e uma ou mais cópias desse objeto também existirem na grid, não é necessário restaurar o objeto emitindo uma solicitação RestoreObject. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação GetObject.

| Estado do objeto | Comportamento de RestoreObject |
|---|---|
| Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto não está em um Cloud Storage Pool | `403 Forbidden, InvalidObjectState` |
| Objeto no pool de Cloud Storage, mas ainda não foi transferido para um estado não recuperável | `200 OK`Nenhuma alteração foi feita.<br><br>**Nota**: Antes que um objeto tenha sido transferido para um estado não recuperável, você não pode alterar seu `expiry-date`. |

| Estado do objeto | Comportamento de RestoreObject |
| --- | --- |
| Objeto passou para um estado não recuperável | `202 Accepted`Restaura uma cópia recuperável do objeto no Cloud Storage Pool pelo número de dias especificado no corpo da solicitação. Ao final desse período, o objeto retorna a um estado não recuperável.<br><br>Opcionalmente, use o `Tier` elemento de solicitação para determinar quanto tempo a tarefa de restauração levará para ser concluída (`Expedited`, `Standard`, ou `Bulk`). Se você não especificar `Tier`, o `Standard` nível será usado.<br><br>**Importante**: Se um objeto tiver sido migrado para o S3 Glacier Deep Archive ou se o Cloud Storage Pool usar Azure Blob storage, você não poderá restaurá-lo usando a `Expedited` camada. 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 irrecuperável | `409 Conflict`, `RestoreAlreadyInProgress` |
| Objeto totalmente restaurado ao pool de storage em nuvem | `200 OK`<br><br>**Nota:** Se um objeto foi restaurado a um estado recuperável, você pode alterar seu `expiry-date` reenviando a solicitação RestoreObject com um novo valor para `Days`. A data de restauração é atualizada em relação ao momento da solicitação. |

#### Filtrar dados de objetos no StorageGRID com a solicitação S3 SelectObjectContent

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

Para obter mais informações, consulte "Referência da API do Amazon Simple Storage Service: SelectObjectContent".

**Antes de começar**

- A conta do locatário possui a permissão S3 Select.
- Você tem `s3:GetObject` permissão para o objeto que você deseja consultar.
- O objeto que você deseja consultar deve estar em um dos seguintes formatos:
  - **CSV**. Pode ser usado como está ou compactado em arquivos GZIP ou BZIP2.
  - **Parquet**. Requisitos adicionais para objetos Parquet:
    - O S3 Select suporta apenas compressão colunar usando GZIP ou Snappy. O S3 Select não suporta compressão de objeto inteiro para objetos Parquet.
    - O S3 Select não suporta saída em Parquet. Você deve especificar o formato de saída como CSV ou JSON.
    - O tamanho máximo de um grupo de linhas não compactadas é de 512 MB.
    - Você deve usar os tipos de dados especificados no esquema do objeto.

        - Não é possível usar os tipos lógicos INTERVAL, JSON, LIST, TIME ou UUID.
- Sua expressão SQL tem um comprimento máximo de 256 KB.
- Qualquer registro na entrada ou nos resultados tem um comprimento máximo de 1 MiB.

**Exemplo de sintaxe de solicitação CSV**

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

**Exemplo de sintaxe de solicitação Parquet**

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

**Exemplo de consulta SQL**

Esta consulta obtém o nome do estado, a população em 2010, a população estimada para 2015 e a porcentagem de variação a partir de dados do censo dos EUA. Registros no arquivo que não são estados são ignorados.

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

As primeiras linhas do arquivo a ser consultado, `SUB-EST2020_ALL.csv` são semelhantes a estas:

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

**Exemplo de uso do AWS-CLI (CSV)**

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

As primeiras linhas do arquivo de saída, `changes.csv`, têm a seguinte aparência:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

#### Exemplo de uso da AWS-CLI (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

As primeiras linhas do arquivo de saída, changes.csv, têm a seguinte aparência:

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

### Operações para uploads multipartes

#### Operações de upload multipart suportadas no StorageGRID

Esta seção descreve como StorageGRID oferece suporte a operações para uploads multipartes.

As seguintes condições e observações aplicam-se a todas as operações de upload multipart:

- Você não deve exceder 1.000 uploads multipart simultâneos para um único bucket, pois os resultados das consultas ListMultipartUploads para esse bucket podem retornar resultados incompletos.
- StorageGRID impõe limites de tamanho da AWS para partes multipartes. Os clientes S3 devem seguir estas diretrizes:
  - Cada parte em um upload multipart deve ter entre 5 MiB (5,242,880 bytes) e 5 GiB (5,368,709,120 bytes).
  - A última parte pode ser menor que 5 MiB (5,242,880 bytes).
  - Em geral, os tamanhos das partes devem ser os maiores possíveis. Por exemplo, use tamanhos de parte de 5 GiB para um objeto de 100 GiB. Como cada parte é considerada um objeto único, o uso de tamanhos de parte grandes reduz a sobrecarga de metadados do StorageGRID.
  - Para objetos menores que 5 GiB, considere usar o upload não multipart em vez disso.
- 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, caso a regra do ILM utilize Balanced ou Strict "opção de ingestão". Você deve estar ciente de como isso afeta o posicionamento do objeto e de suas partes:
  - Se o ILM for alterado durante um upload multipart do S3, algumas partes do objeto podem não atender aos requisitos atuais do ILM quando o upload multipart for concluído. Qualquer parte que não estiver posicionada corretamente é enfileirada para reavaliação do ILM e movida para o local correto

posteriormente.

    - Ao avaliar o ILM para uma parte, StorageGRID filtra pelo tamanho da parte, não pelo 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 especificar que todos os objetos com 10 GB ou mais sejam armazenados em DC1, enquanto todos os objetos menores sejam armazenados em DC2, cada parte de 1 GB de um upload multipart de 10 partes é armazenada em DC2 durante a ingestão. No entanto, quando o ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.

- Todas as operações de upload multipart são compatíveis com StorageGRID "valores de consistência".
- Quando um objeto é ingerido usando upload multipart, o "Limiar de segmentação de objetos (1 GiB)" não é aplicado.
- Conforme necessário, você pode usar "criptografia do lado do servidor" com uploads multipartes. Para usar SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID), você inclui o cabeçalho de solicitação `x-amz-server-side-encryption` apenas na solicitação CreateMultipartUpload. Para usar SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente), você especifica os mesmos três cabeçalhos de solicitação de chave de criptografia na solicitação CreateMultipartUpload e em cada solicitação subsequente UploadPart.
- Um objeto carregado em várias partes é incluído em um "bucket de branch" se a ingestão foi iniciada antes do carimbo de data/hora "Antes" do bucket base, independentemente de quando o upload for concluído.

| Operação | Implementação |
|---|---|
| AbortMultipartUpload | Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio. |
| CompleteMultipartUpload | Consulte "CompleteMultipartUpload" |
| CreateMultipartUpload<br><br>(anteriormente chamado de Initiate Multipart Upload) | Consulte "CreateMultipartUpload" |
| ListMultipartUploads | Consulte "ListMultipartUploads" |
| ListParts | Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio. |
| UploadPart | Consulte "UploadPart" |
| UploadPartCopy | Consulte "UploadPartCopy" |

#### Como StorageGRID S3 API REST conclui uploads multipartes

A operação CompleteMultipartUpload completa um upload de objeto em várias partes, montando as partes previamente carregadas.

StorageGRID suporta valores não consecutivos em ordem crescente para o parâmetro de solicitação `partNumber`CompleteMultipartUpload. O parâmetro pode começar com qualquer valor.

### Resolver conflitos

Solicitações conflitantes de clientes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio "latest-wins". O momento da avaliação do "latest-wins" é determinado quando o sistema StorageGRID conclui uma determinada solicitação, e não quando os clientes S3 iniciam uma operação.

### Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  O `x-amz-storage-class` cabeçalho afeta quantas cópias de objetos o StorageGRID cria se a regra ILM correspondente especificar o "Opção de confirmação dupla ou ingestão balanceada".

- `STANDARD`

  (Padrão) Especifica uma operação de ingestão de confirmação dupla quando a regra ILM usa a opção Dual commit ou quando a opção Balanced recorre à criação de cópias intermediárias.

- `REDUCED_REDUNDANCY`

  Especifica uma operação de ingestão de confirmação única quando a regra ILM usa a opção de confirmação dupla ou quando a opção balanceada recorre à criação de cópias intermediárias.

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

Se um upload multipart não for concluído em 15 dias, a operação é marcada como inativa e todos os dados associados são excluídos do sistema.

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

### Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `If-Match`

  O `If-Match header` é aceito, mas não funcional.

- `If-None-Match`

  O `If-None-Match header` é aceito, mas não funcional.

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

#### Controle de versões

Esta operação conclui um upload multipart. Se o versionamento estiver habilitado para um bucket, a versão do objeto é criada após a conclusão do upload multipart.

Se o versionamento estiver habilitado para um bucket, um identificador único `versionId` é gerado automaticamente para a versão do objeto armazenado. Esse `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho da resposta.

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

> Quando o versionamento está habilitado para um bucket, a conclusão de um upload multipart sempre cria uma nova versão, mesmo que haja uploads multipart simultâneos concluídos na mesma chave de objeto. Quando o versionamento não está habilitado para um bucket, é possível iniciar um upload multipart e depois outro upload multipart pode ser iniciado e concluído primeiro na mesma chave de objeto. Em buckets sem versionamento, o upload multipart que for concluído por último terá precedência.

#### Falha na replicação, notificação ou notificação de metadados

Se o bucket onde ocorre o upload multipart estiver configurado para um serviço de plataforma, o upload multipart será bem-sucedido mesmo que a replicação ou notificação associada falhe.

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

Consulte "Solucionar problemas de serviços da plataforma".

##### Cabeçalhos e opções de solicitação S3 CreateMultipartUpload no StorageGRID

## A operação CreateMultipartUpload (anteriormente chamada de Initiate Multipart Upload) inicia um upload multipart para um objeto e retorna um ID de upload.

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

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

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

- `STANDARD` (Padrão)

- **Confirmação dupla**: Se a regra ILM especificar a opção de ingestão de confirmação dupla, assim que um objeto for ingerido, uma segunda cópia desse objeto será criada e distribuída para um Storage Node diferente (confirmação dupla). Quando a ILM é avaliada, o StorageGRID determina se essas cópias intermediárias iniciais atendem às instruções de posicionamento na regra. Se não atenderem, novas cópias do objeto podem precisar ser criadas em locais diferentes e as cópias intermediárias iniciais podem precisar ser excluídas.
- **Balanceado**: Se a regra ILM especificar a opção Balanceado e StorageGRID não puder criar imediatamente todas as cópias especificadas na regra, StorageGRID faz duas cópias intermediárias em diferentes nós de armazenamento.

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

- `REDUCED_REDUNDANCY`
  - **Confirmação dupla**: Se a regra ILM especificar a opção de confirmação dupla, StorageGRID cria uma única cópia intermediária à medida que o objeto é ingerido (confirmação única).
  - **Balanceado**: Se a regra ILM especificar a opção Balanceado, StorageGRID cria uma única cópia intermediária somente se o sistema não puder criar imediatamente todas as cópias especificadas na regra. Se StorageGRID puder realizar o posicionamento síncrono, este cabeçalho não terá efeito. A `REDUCED_REDUNDANCY` opção é mais adequada quando a regra ILM correspondente ao objeto cria uma única cópia replicada. Nesse caso, usar `REDUCED_REDUNDANCY` essa opção elimina a criação e exclusão desnecessárias de uma cópia extra do objeto para cada operação de ingestão.

  O uso da `REDUCED_REDUNDANCY`opção não é recomendado em outras circunstâncias. `REDUCED_REDUNDANCY` Isso aumenta o risco de perda de dados de objeto durante a ingestão. Por exemplo, você pode perder dados se a cópia única for armazenada inicialmente em um Storage Node que falhe antes que a avaliação do ILM possa ocorrer.

> Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se existir apenas uma cópia replicada de um objeto, esse objeto é perdido se um Storage Node falhar ou apresentar um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como upgrades.

A especificação `REDUCED_REDUNDANCY`afeta apenas quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas ILM ativas e não resulta no armazenamento de dados em níveis mais baixos de redundância no sistema StorageGRID.

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

### Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Type`
- `x-amz-checksum-algorithm`

Atualmente, apenas o valor SHA256 para `x-amz-checksum-algorithm` é suportado.

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

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

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

  Se você deseja usar a opção **Hora de criação definida pelo usuário** como a hora de referência para uma regra ILM, você deve usar `creation-time` como o nome do metadado que registra quando o objeto foi criado. Por exemplo:

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

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

  > Adicionar `creation-time` como metadados definidos pelo usuário não é permitido se você estiver adicionando um objeto a um bucket com a Compliance legada ativada. Um erro será retornado.

- Cabeçalhos da solicitação S3 Object Lock:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

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

  "Use a API REST S3 para configurar o S3 Object Lock"

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

    Cabeçalhos de solicitação para criptografia do lado do servidor

    > Para obter informações sobre como StorageGRID lida com caracteres UTF-8, consulte "PutObject".

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

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

- **SSE**: Utilize o seguinte cabeçalho na solicitação CreateMultipartUpload se você quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações UploadPart.
  - `x-amz-server-side-encryption`
- **SSE-C**: Utilize todos os três cabeçalhos na solicitação CreateMultipartUpload (e em cada solicitação UploadPart subsequente) se você quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
  - `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.

> As chaves de criptografia fornecidas por você nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para "usando criptografia do lado do servidor".

#### Cabeçalhos de solicitação não suportados

O seguinte cabeçalho de solicitação não é compatível:

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

  O `x-amz-website-redirect-location`cabeçalho retorna `XNotImplemented`.

#### Controle de versões

O upload multipart consiste em operações separadas para iniciar o upload, listar os uploads, enviar as partes, montar as partes enviadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é realizada.

##### Operação S3 ListMultipartUploads e parâmetros suportados no StorageGRID

A operação ListMultipartUploads lista os uploads multipartes em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

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

- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

### Controle de versões

O upload multipart consiste em operações separadas para iniciar o upload, listar os uploads, enviar as partes, montar as partes enviadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é realizada.

#### Cabeçalhos de solicitação suportados e não suportados para operações UploadPart do S3 no StorageGRID

A operação UploadPart carrega uma parte em um upload multipartes de um objeto.

### Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

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

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

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

> As chaves de criptografia 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 dados de objetos, revise as considerações em "Use criptografia do lado do servidor".

Se você especificou um checksum SHA-256 durante a solicitação CreateMultipartUpload, também deverá incluir o seguinte cabeçalho de solicitação em cada solicitação UploadPart:

- `x-amz-checksum-sha256`: Especifique o checksum SHA-256 para esta parte.

### Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-sdk-checksum-algorithm`

- `x-amz-trailer`

#### Controle de versões

O upload multipart consiste em operações separadas para iniciar o upload, listar os uploads, enviar as partes, montar as partes enviadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é realizada.

##### Carregar uma parte de um objeto no StorageGRID com a operação S3 UploadPartCopy

A operação UploadPartCopy carrega uma parte de um objeto copiando dados de um objeto existente como fonte de dados.

A operação UploadPartCopy é implementada com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso prévio.

Esta solicitação lê e grava os dados do objeto especificados em `x-amz-copy-source-range` no 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 criptografia SSE-C para a solicitação CreateMultipartUpload, também deverá incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPartCopy:

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

Se o objeto de origem estiver criptografado usando uma chave fornecida pelo cliente (SSE-C), você deve incluir os três cabeçalhos a seguir na solicitação UploadPartCopy, para que o objeto possa ser descriptografado e copiado:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: especifique `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia que você forneceu ao criar o objeto de origem.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu ao criar 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 dados de objetos, revise as considerações em "Use criptografia do lado do servidor".

#### Controle de versões

O upload multipart consiste em operações separadas para iniciar o upload, listar os uploads, enviar as partes, montar as partes enviadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é realizada.

#### Respostas de erro da API REST do StorageGRID S3

O sistema StorageGRID suporta todas as respostas de erro padrão da API REST S3 aplicáveis. Além disso, a implementação do StorageGRID adiciona diversas respostas personalizadas.

##### Códigos de erro da API S3 suportados

| Nome | Status HTTP |
|---|---|
| AccessDenied | 403 Proibido |
| BadDigest | 400 Solicitação inválida |
| BucketAlreadyExists | 409 Conflito |
| BucketNotEmpty | 409 Conflito |
| IncompleteBody | 400 Solicitação inválida |
| InternalError | Erro interno do servidor 500 |
| InvalidAccessKeyId | 403 Proibido |
| InvalidArgument | 400 Solicitação inválida |
| InvalidBucketName | 400 Solicitação inválida |
| InvalidBucketState | 409 Conflito |
| InvalidDigest | 400 Solicitação inválida |
| InvalidEncryptionAlgorithmError | 400 Solicitação inválida |
| InvalidPart | 400 Solicitação inválida |

| Nome | Status HTTP |
| --- | --- |
| InvalidPartOrder | 400 Solicitação inválida |
| InvalidRange | 416 Intervalo solicitado não satisfatório |
| InvalidRequest | 400 Solicitação inválida |
| InvalidStorageClass | 400 Solicitação inválida |
| InvalidTag | 400 Solicitação inválida |
| URI inválido | 400 Solicitação inválida |
| KeyTooLong | 400 Solicitação inválida |
| XML malformado | 400 Solicitação inválida |
| MetadataTooLarge | 400 Solicitação inválida |
| MethodNotAllowed | 405 Método Não Permitido |
| MissingContentLength | 411 Comprimento necessário |
| MissingRequestBodyError | 400 Solicitação inválida |
| MissingSecurityHeader | 400 Solicitação inválida |
| NoSuchBucket | 404 Não encontrado |
| NoSuchKey | 404 Não encontrado |
| NoSuchUpload | 404 Não encontrado |
| NotImplemented | 501 Não Implementado |
| NoSuchBucketPolicy | 404 Não encontrado |
| ObjectLockConfigurationNotFoundError | 404 Não encontrado |
| PreconditionFailed | 412 Pré-condição falhou |
| RequestTimeTooSkewed | 403 Proibido |
| ServiceUnavailable | 503 Serviço indisponível |

| Nome | Status HTTP |
| --- | --- |
| SignatureDoesNotMatch | 403 Proibido |
| TooManyBuckets | 400 Solicitação inválida |
| UserKeyMustBeSpecified | 400 Solicitação inválida |

**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 Compliant legado | 400 Solicitação inválida |
| XBucketPolicyParseException | Falha ao analisar o JSON da política de bucket recebido. | 400 Solicitação inválida |
| XComplianceConflict | Operação negada devido a configurações de Compliance legadas. | 403 Proibido |
| XConformidadeRedundânciaReduzidaProibido | Redução de redundância não é permitida no bucket Compliant legado | 400 Solicitação inválida |
| XMaxBucketPolicyLengthExceeded | Sua política excede o comprimento máximo permitido para a política de bucket. | 400 Solicitação inválida |
| XMissingInternalRequestHeader | Falta um cabeçalho em uma solicitação interna. | 400 Solicitação inválida |
| XNoSuchBucketCompliance | O bucket especificado não tem Compliance legada ativada. | 404 Não encontrado |
| XNotAcceptable | A solicitação contém um ou mais cabeçalhos Accept que não puderam ser atendidos. | 406 Não Aceitável |
| XNãoImplementado | A solicitação que você forneceu implica uma funcionalidade que não está implementada. | 501 Não Implementado |

## Operações personalizadas do StorageGRID

### Operações de bucket personalizadas suportadas no StorageGRID

O sistema StorageGRID suporta operações personalizadas que são adicionadas à API

REST S3.

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

| Operação | Descrição |
|---|---|
| "GET consistência do bucket" | Retorna a consistência que está sendo aplicada a um determinado bucket. |
| "Consistência de PUT Bucket" | Define a consistência aplicada a um determinado bucket. |
| "Obter o último tempo de acesso do bucket" | Retorna se as atualizações de tempo de acesso estão habilitadas ou desabilitadas para um determinado bucket. |
| "Último tempo de acesso do PUT Bucket" | Permite que você ative ou desative as atualizações do tempo de acesso para um bucket específico. |
| "EXCLUIR configuração de notificação de metadados do bucket" | Exclui o arquivo XML de configuração de notificação de metadados associado a um bucket específico. |
| "GET Configuração de notificação de metadados do bucket" | Retorna o XML de configuração de notificação de metadados associado a um bucket específico. |
| "PUT Configuração de notificação de metadados do bucket" | Configura o serviço de notificação de metadados para um bucket. |
| "GET Uso de Armazenamento" | Mostra a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta. |
| "Obsoleto: CreateBucket com configurações de conformidade" | Obsoleto e sem suporte: você não pode mais criar novos buckets com Compliance ativado. |
| "Obsoleto: GET Bucket compliance" | Obsoleto, mas ainda suportado: retorna as configurações de conformidade atualmente em vigor para um bucket Compliant legado existente. |
| "Obsoleto: PUT Bucket compliance" | Obsoleto, mas ainda compatível: permite modificar as configurações de conformidade de um bucket legado compatível. |

#### Recupere o nível de consistência do bucket no StorageGRID com a solicitação GET Bucket consistency

A solicitação GET Bucket consistency permite determinar a consistência que está sendo aplicada a um bucket específico.

A consistência padrão está definida para garantir a leitura após a gravação de objetos recém-criados.

Você deve ter a permissão s3:GetBucketConsistency, ou ser o usuário raiz da conta, para concluir esta

operação.

#### Exemplo de solicitação

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

#### Resposta

Na resposta XML, `<Consistency>` retornará um dos seguintes valores:

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

#### Exemplo de resposta

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

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

**Informações relacionadas**

"Consistência"

### Especifique os níveis de consistência no StorageGRID com a solicitação PUT Bucket consistency

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

A consistência padrão está definida para garantir a leitura após a gravação de objetos recém-criados.

**Antes de começar**

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

**Solicitação**

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

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

| Consistência | Descrição |
| --- | --- |
| disponível | Garante consistência eventual tanto para novos objetos quanto para atualizações de objetos. Para buckets do S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que são lidos raramente ou para operações HEAD ou GET em chaves que não existem). Não é compatível com buckets do S3 FabricPool. |

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

#### Exemplo de solicitação

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

#### Informações relacionadas

"Consistência"

### Recupere o status do tempo de acesso ao bucket no StorageGRID com a solicitação GET Bucket last access time

A solicitação GET Bucket tempo de acesso permite que você determine se as atualizações de tempo de acesso estão ativadas ou desativadas para buckets individuais.

Você deve ter a permissão s3:GetBucketLastAccessTime, ou ser o usuário raiz da conta, para concluir esta operação.

#### Exemplo de solicitação

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

#### Exemplo de resposta

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

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

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

#### Ativar e desativar atualizações do tempo de acesso no StorageGRID com a solicitação PUT Bucket last access time

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

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

> ⓘ A partir da versão 10.3 do StorageGRID, as atualizações do tempo de acesso estão desativadas por padrão para todos os novos buckets. Se você tiver buckets criados com uma versão anterior do StorageGRID e quiser que eles sigam o novo comportamento padrão, você deve desativar explicitamente as atualizações do tempo de acesso para cada um desses buckets. Você pode ativar ou desativar as atualizações do tempo de acesso usando a solicitação PUT Bucket last access time ou na página de detalhes de um bucket no Tenant Manager. Consulte "Ativar ou desativar atualizações do tempo de acesso mais recente".

Se as atualizações de tempo de acesso estiverem desativadas para um bucket, o seguinte comportamento será aplicado às operações no bucket:

- GetObject, GetObjectAcl, GetObjectTagging, e HeadObject não atualizam o tempo de acesso. O objeto não é adicionado às filas para avaliação do gerenciamento do ciclo de vida das informações (ILM).
- CopyObject e PutObjectTagging solicitações que atualizam apenas os metadados também atualizam o tempo de acesso. O objeto é adicionado às filas para avaliação do ILM.
- Se as atualizações do último tempo de acesso estiverem desativadas para o bucket de origem, as solicitações CopyObject não atualizam o último tempo de acesso para o bucket de origem. O objeto copiado não é adicionado às filas de avaliação de ILM para o bucket de origem. No entanto, para o destino, as solicitações CopyObject sempre atualizam o último tempo de acesso. A cópia do objeto é adicionada às filas de avaliação de ILM.
- CompleteMultipartUpload solicitações atualizam o tempo de acesso. O objeto concluído é adicionado às filas para avaliação do ILM.

#### Exemplos de solicitação

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

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

Este exemplo desativa o tempo de acesso para um bucket.

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

### Desative o serviço de integração de pesquisa com a solicitação de configuração de notificação de metadados DELETE Bucket no StorageGRID

A solicitação DELETE Bucket metadata notification configuration permite que você desative o serviço de integração de pesquisa para buckets individuais, excluindo o XML de configuração.

Você precisa ter a permissão s3:DeleteBucketMetadataNotification para um bucket ou ser o administrador da conta para concluir esta operação.

#### Exemplo de solicitação

Este exemplo mostra como desativar o serviço de integração de pesquisa para um bucket.

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

### Configurar a integração de pesquisa no StorageGRID com a solicitação GET Bucket metadata notification configuration

A solicitação GET Bucket metadata notification configuration permite que você recupere o XML de configuração usado para configurar a integração de pesquisa para buckets individuais.

Você deve ter a permissão s3:GetBucketMetadataNotification, ou ser o usuário raiz da conta, para concluir esta operação.

#### Exemplo de solicitação

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

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

#### Resposta

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

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

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

| Nome | Descrição | Obrigatório |
|---|---|---|
| MetadataNotificationConfiguration | Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados.<br><br>Contém um ou mais elementos de Rule. | Sim |

| Nome | Descrição | Obrigatório |
| --- | --- | --- |
| Regra | Etiqueta de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice específico.<br><br>Regras com prefixos sobrepostos são rejeitadas.<br><br>Incluído no elemento MetadataNotificationConfiguration. | Sim |
| ID | Identificador único para a regra.<br><br>Incluído no elemento Rule. | Não |
| Status | O status pode ser 'Ativado' ou 'Desativado'. Nenhuma ação é executada para regras desativadas.<br><br>Incluído no elemento Rule. | Sim |
| Prefixo | Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado.<br><br>Para corresponder a todos os objetos, especifique um prefixo vazio.<br><br>Incluído no elemento Rule. | Sim |
| Destino | Etiqueta de contêiner para o destino de uma regra.<br><br>Incluído no elemento Rule. | Sim |

| Nome | Descrição | Obrigatório |
| --- | --- | --- |
| Urna | URN do destino para onde os metadados do objeto são enviados. Deve ser o URN de um endpoint do StorageGRID com as seguintes propriedades:<br>• `es`deve ser o terceiro elemento.<br>• O URN deve terminar com o índice e o tipo onde os metadados estão armazenados, no formato `domain-name/myindex/mytype`.<br>Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles têm o seguinte formato:<br>• `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype`<br>• `urn:mysite:es:::mydomain/myindex/mytype`<br>O endpoint deve ser configurado antes do envio do XML de configuração, ou a configuração falhará com um erro 404.<br>Urn está incluído no elemento Destination. | 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, os metadados do objeto estão sendo enviados para um índice do Elasticsearch chamado `current` e tipo chamado `2017` que está hospedado em um domínio da AWS chamado `records`.

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

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

**Informações relacionadas**

"Use uma conta de tenant"

### Habilite o serviço de integração de pesquisa no StorageGRID com a solicitação de configuração de notificação de metadados do bucket PUT

A solicitação PUT Bucket metadata notification configuration permite que você habilite 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 precisa ter a permissão s3:PutBucketMetadataNotification para um bucket ou ser o root da conta para concluir esta operação.

#### Solicitação

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

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

Configurações com prefixos sobrepostos não são válidas e são rejeitadas no momento do envio. Por exemplo, uma configuração que incluísse 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 o URN de um endpoint do StorageGRID. O endpoint deve existir

quando a configuração de notificação de metadados for enviada, ou a solicitação falhará como um `400 Bad Request`. A mensagem de erro indica: `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 da notificação de metadados.

| Nome | Descrição | Obrigatório |
|---|---|---|
| MetadataNotificationConfiguration | Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados.<br><br>Contém um ou mais elementos de Rule. | Sim |
| Regra | Etiqueta de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice específico.<br><br>Regras com prefixos sobrepostos são rejeitadas.<br><br>Incluído no elemento MetadataNotificationConfiguration. | Sim |
| ID | Identificador único para a regra.<br><br>Incluído no elemento Rule. | Não |
| Status | O status pode ser 'Ativado' ou 'Desativado'. Nenhuma ação é executada para regras desativadas.<br><br>Incluído no elemento Rule. | Sim |

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

#### Exemplos de solicitação

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

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

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

Neste exemplo, os metadados dos objetos que correspondem ao prefixo `/images` são enviados para um destino, enquanto os metadados dos objetos que correspondem ao prefixo `/videos` são enviados para um segundo destino.

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

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

#### JSON gerado pelo serviço de integração de pesquisa

Ao ativar o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado para o endpoint de destino sempre que os metadados ou tags de um objeto são adicionados, atualizados ou excluídos.

Este exemplo mostra um exemplo do JSON que poderia ser gerado quando um objeto com a chave `SGWS/Tagging.txt` é criado em um bucket chamado `test`. O `test` bucket não é versionado, portanto 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 objeto incluídos em notificações de metadados

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

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

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

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

Para tags e metadados de usuário, StorageGRID envia 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 dinâmico de campos e para mapeamento de formatos de data. Você deve habilitar os mapeamentos dinâmicos de campos no índice antes de configurar o serviço de integração de pesquisa. Depois que um documento é indexado, você não pode editar os tipos de campo do documento no índice.

**Informações relacionadas**

"Use uma conta de tenant"

### Recupere o uso de storage da conta e do bucket no StorageGRID com a solicitação GET Storage Usage

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

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

Por padrão, StorageGRID tenta recuperar informações de uso utilizando consistência global forte. Se a consistência global forte não puder ser alcançada, StorageGRID tenta recuperar as informações de uso com consistência de site forte.

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

#### Exemplo de solicitação

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

#### Exemplo de resposta

Este exemplo mostra uma conta que possui 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 versões

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

#### Informações relacionadas

"Consistência"

### Solicitações de bucket obsoletas para Compliance legada

#### Solicitações de bucket obsoletas para StorageGRID Compliance legado

Você pode precisar usar a API REST S3 do StorageGRID para gerenciar buckets que foram criados usando o recurso de Compliance legado.

### Recurso de conformidade descontinuado

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

Se você habilitou anteriormente a configuração de Conformidade global, a configuração de Bloqueio de Objeto S3 global também estará habilitada no StorageGRID 11.6. Você não pode mais criar novos buckets com a Conformidade habilitada; no entanto, se necessário, você pode usar a API REST S3 do StorageGRID para gerenciar quaisquer buckets legados em conformidade existentes.

- "Use a API REST S3 para configurar o S3 Object Lock"
- "Gerencie objetos com ILM"
- "NetApp Knowledge Base: como gerenciar buckets legados compatíveis no StorageGRID 11.5"

Solicitações de conformidade obsoletas:

- "Obsoleto - Modificações na solicitação PUT Bucket para fins de conformidade"

  O elemento XML SGCompliance está obsoleto. Anteriormente, você podia incluir esse elemento personalizado do StorageGRID no corpo da requisição XML opcional das solicitações PUT Bucket para criar um bucket em conformidade.

- "Obsoleto - GET Bucket compliance"

  A solicitação GET Bucket compliance foi descontinuada. No entanto, você pode continuar usando essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket legado Compliant.

- "Obsoleto - PUT Bucket compliance"

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

#### Elemento SGCompliance obsoleto no StorageGRID

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

> O recurso de conformidade do StorageGRID, disponível em versões anteriores do StorageGRID, foi descontinuado e substituído pelo S3 Object Lock. Veja mais detalhes a seguir:
>
> - "Use a API REST S3 para configurar o S3 Object Lock"
> - "NetApp Knowledge Base: como gerenciar buckets legados compatíveis no StorageGRID 11.5"

Não é mais possível criar novos buckets com a Compliance ativada. A seguinte mensagem de erro é exibida se você tentar usar as modificações de solicitação CreateBucket para compliance para criar um novo bucket em compliance:

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

#### Solicitação GET de conformidade de bucket obsoleta no StorageGRID

A solicitação GET Bucket compliance foi descontinuada. No entanto, você pode continuar usando essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket legado Compliant.

> O recurso de conformidade do StorageGRID, disponível em versões anteriores do StorageGRID, foi descontinuado e substituído pelo S3 Object Lock. Veja mais detalhes a seguir:
>
> - "Use a API REST S3 para configurar o S3 Object Lock"
> - "NetApp Knowledge Base: como gerenciar buckets legados compatíveis no StorageGRID 11.5"

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

**Exemplo de solicitação**

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

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

**Exemplo de resposta**

Na resposta XML, `<SGCompliance>` lista as configurações de conformidade em vigor para o bucket. Este exemplo de resposta mostra as configurações de conformidade para um bucket no qual cada objeto será retido por um ano (525.600 minutos), a partir do momento em que o objeto é inserido na grid. Atualmente, não há guarda legal neste bucket. Cada objeto será excluído automaticamente após um ano.

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

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

| Nome | Descrição |
| --- | --- |
| RetentionPeriodMinutes | O período de retenção dos objetos adicionados a este bucket, em minutos. O período de retenção começa quando o objeto é ingerido no grid. |
| LegalHold | • Verdadeiro: Este bucket está atualmente sob guarda legal. Os objetos neste bucket não podem ser excluídos até que a guarda legal seja suspensa, mesmo que o período de retenção tenha expirado.<br>• Falso: Este bucket não está atualmente sob guarda legal. Os objetos neste bucket podem ser excluídos quando o período de retenção expirar. |
| AutoDelete | • Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando o período de retenção expirar, a menos que o bucket esteja sob guarda legal.<br>• Falso: Os objetos neste bucket não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los. |

**Respostas de erro**

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

#### Solicitação PUT de conformidade de bucket obsoleta no StorageGRID

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

> O recurso de conformidade do StorageGRID, disponível em versões anteriores do StorageGRID, foi descontinuado e substituído pelo S3 Object Lock. Veja mais detalhes a seguir:
>
> • "Use a API REST S3 para configurar o S3 Object Lock"
> • "NetApp Knowledge Base: como gerenciar buckets legados compatíveis no StorageGRID 11.5"

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

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

**Exemplo de solicitação**

Esta solicitação de exemplo modifica as configurações de conformidade para o bucket denominado `mybucket`. Neste exemplo, os objetos em `mybucket` serão retidos por dois anos (1.051.200 minutos) em vez de um ano, a partir do momento em que o objeto for ingerido na grid. Não há guarda legal neste bucket. Cada

objeto será excluído automaticamente após dois anos.

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

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

| Nome | Descrição |
|---|---|
| RetentionPeriodMinutes | O período de retenção dos objetos adicionados a este bucket, em minutos. O período de retenção começa quando o objeto é ingerido no grid.<br><br>**Importante** Ao especificar um novo valor para RetentionPeriodMinutes, você deve especificar um valor igual ou maior que o período de retenção atual do bucket. Depois que o período de retenção do bucket for definido, você não poderá diminuir esse valor; você só poderá aumentá-lo. |
| LegalHold | • Verdadeiro: Este bucket está atualmente sob guarda legal. Os objetos neste bucket não podem ser excluídos até que a guarda legal seja suspensa, mesmo que o período de retenção tenha expirado.<br>• Falso: Este bucket não está atualmente sob guarda legal. Os objetos neste bucket podem ser excluídos quando o período de retenção expirar. |
| AutoDelete | • Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando o período de retenção expirar, a menos que o bucket esteja sob guarda legal.<br>• Falso: Os objetos neste bucket não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los. |

**Consistência para configurações de conformidade**

Ao atualizar as configurações de conformidade de um bucket S3 com uma solicitação PUT Bucket compliance, StorageGRID tenta atualizar os metadados do bucket em toda a grid. Por padrão, StorageGRID usa a consistência **Strong-global** para garantir que todos os sites do data center e todos os Storage Nodes que contêm metadados do bucket tenham consistência de leitura após gravação para as configurações de conformidade alteradas.

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

Se você receber esta resposta, entre em contato com o administrador da grid para garantir que os serviços de armazenamento necessários sejam disponibilizados o mais rápido possível. Caso o administrador da grid não consiga disponibilizar Storage Nodes suficientes em cada site, o suporte técnico pode orientar você a tentar novamente a solicitação com falha, forçando a consistência **Strong-site**.

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

Quando a consistência é reduzida para **Strong-site**, 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 este bucket até que todos os sites e Storage Nodes estejam disponíveis. As configurações inconsistentes podem resultar em comportamentos inesperados e indesejados. Por exemplo, se você estiver colocando um bucket sob guarda legal e forçar uma consistência menor, as configurações de conformidade anteriores do bucket (ou seja, guarda legal desativada) podem continuar em vigor em alguns sites do data center. Como resultado, objetos que você acredita estarem sob guarda legal podem ser excluídos quando o período de retenção expirar, seja pelo usuário ou pelo AutoDelete, se ativado.

Para forçar o uso da consistência **Strong-site**, reenvie a solicitação de conformidade do bucket PUT e inclua o `Consistency-Control` cabeçalho da solicitação HTTP, conforme mostrado a seguir:

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

#### Respostas de erro

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

#### Informações relacionadas

"Obsoleto: modificações de solicitação PUT Bucket para conformidade"

## Gerenciar políticas de acesso

#### Como StorageGRID usa políticas da AWS para controlar o acesso a buckets e objetos do S3

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

#### Visão geral da política de acesso

StorageGRID suporta três tipos de políticas de acesso:

- **Políticas de bucket**, que são gerenciadas usando as operações da API S3 GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy ou pelo Tenant Manager ou Tenant Management API. As políticas de bucket são associadas aos buckets, então são configuradas para controlar o acesso de usuários da conta proprietária do bucket ou de outras contas ao bucket e aos objetos nele. Uma política de bucket se aplica a apenas um bucket e, possivelmente, a vários grupos.
- **Políticas de grupo**, que são configuradas usando o Tenant Manager ou a Tenant Management API. As políticas de grupo são associadas a um grupo na conta, então são configuradas para permitir que esse grupo acesse recursos específicos pertencentes a essa conta. Uma política de grupo se aplica a apenas um grupo e possivelmente a vários buckets.
- **Políticas de sessão**, que são incluídas ao fazer uma solicitação AssumeRole. As políticas de sessão aplicam-se apenas à sessão em questão, definindo com mais detalhes as permissões que o usuário possui, além daquelas concedidas pelas políticas de grupo e de bucket.

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

As políticas de bucket e grupo 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 da declaração (Sid) (opcional)
- Efeito
- Principal/NotPrincipal
- Recurso/NotResource
- Ação/NotAction
- Condição (opcional)

As declarações de política são construídas usando esta estrutura para especificar permissões: conceder <Effect> para permitir/negar <Principal> executar <Action> em <Resource> quando <Condition> se aplica.

Cada elemento da política é usado para uma função específica:

| Elemento | Descrição |
|---|---|
| Sid | O elemento Sid é opcional. O Sid serve apenas como uma descrição para o usuário. Ele é armazenado, mas não interpretado pelo sistema StorageGRID. |
| Efeito | Use o elemento Effect para determinar se as operações especificadas são permitidas ou negadas. Você deve identificar as operações que permite (ou nega) em buckets ou objetos usando as palavras-chave do elemento Action. |

| Elemento | Descrição |
| --- | --- |
| Principal/NotPrincipal | 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 o principal. Por padrão, somente o root da conta tem acesso aos recursos pertencentes à conta.<br><br>Você só precisa especificar o elemento Principal em uma política de bucket. Para políticas de grupo, o grupo ao qual a política está associada é o elemento Principal implícito. |
| Recurso/NotResource | O elemento Resource identifica buckets e objetos. Você pode conceder ou negar permissões a buckets e objetos usando o Nome de Recurso da Amazon (ARN) para identificar o recurso. |
| Ação/NotAction | Os elementos Ação e Efeito são os dois componentes das permissões. Quando um grupo solicita um recurso, o acesso a ele é concedido ou negado. O acesso é negado a menos que você atribua permissões especificamente, mas você pode usar a negação explícita para substituir uma permissão concedida por outra política. |
| Condição | O elemento Condição é opcional. As condições permitem criar expressões para determinar quando uma política deve ser aplicada. |

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

```
s3:*Object
```

No elemento Resource, você pode usar os caracteres curinga (*) e (?). Enquanto o asterisco (*) corresponde a 0 ou mais caracteres, o ponto de interrogação (?) corresponde a qualquer caractere único.

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

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

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

No exemplo a seguir, a declaração utiliza os elementos Efeito, Principal, Ação e Recurso. Este exemplo mostra uma declaração de política de bucket completa que usa o Efeito "Permitir" para conceder aos Principais, ao grupo de administradores `federated-group/admin` e ao grupo de finanças `federated-group/finance`, permissões para executar a Ação `s3:ListBucket` no bucket nomeado `mybucket` e a Ação `s3:GetObject` em todos os objetos dentro desse bucket.

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

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

#### Consistência para políticas

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

Conforme necessário, você pode alterar as garantias de consistência para atualizações de políticas de bucket. Por exemplo, você pode querer que uma alteração em uma política de bucket esteja disponível durante uma falha no local.

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

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

#### O que é política de sessão?

Uma política de sessão é uma política de acesso que restringe temporariamente as permissões disponíveis durante uma sessão específica, como quando um usuário assume um grupo. Uma política de sessão só pode permitir um subconjunto de permissões e não pode conceder permissões adicionais. O próprio grupo pode ter

permissões mais amplas.

#### Use o ARN em declarações de política

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

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

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

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

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

Outras considerações:

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

  "Sintaxe URN da RFC 2141"

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

#### Especifique recursos em uma política

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

- Cada declaração de política requer um elemento Resource. Em uma política, os recursos são indicados pelo elemento `Resource`, ou, alternativamente, `NotResource` para exclusão.
- Você especifica recursos com um ARN de recurso S3. Por exemplo:

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

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

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

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

#### Especifique os principais em uma política

Utilize o elemento Principal para identificar o usuário, grupo ou conta de locatário que tem permissão/negação de acesso ao recurso pela declaração de política.

- Cada declaração de política em uma política de bucket deve incluir um elemento Principal. Declarações de política em uma política de grupo não precisam do elemento Principal porque o grupo é entendido como o principal.
- Em uma política, os principais são designados 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 da conta de locatário 27233906934684427525, que inclui a raiz da conta e todos os usuários da 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 ("Managers"):

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

- Você pode especificar um principal anônimo:

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

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

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

Por exemplo, suponha que Alex deixe a organização e o nome de usuário `Alex` seja excluído. Se um novo Alex entrar na organização e receber o mesmo `Alex` nome de usuário, o novo usuário poderá herdar involuntariamente as permissões concedidas ao usuário original.

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

#### Especifique as permissões em uma política

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

A tabela lista as permissões que se aplicam aos buckets e as permissões que se aplicam aos objetos.

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

> Uma exclusão é realizada quando uma operação de inserção (put) é usada para sobrescrever um valor existente.

#### Permissões que se aplicam aos buckets

| Permissões | Operações da API REST do S3 | Personalizado para StorageGRID |
|---|---|---|
| s3:CreateBucket | CreateBucket | Sim.<br><br>**Nota**: use somente em políticas de grupo. |
| s3:DeleteBucket | DeleteBucket | |
| s3:DeleteBucketMetadataNotification | EXCLUIR configuração de notificação de metadados do bucket | Sim |
| s3:DeleteBucketPolicy | DeleteBucketPolicy | |
| s3:DeleteReplicationConfiguration | DeleteBucketReplication | Sim, permissões separadas para PUT e DELETE |

| Permissões | Operações da API REST do S3 | Personalizado para StorageGRID |
| --- | --- | --- |
| s3:GetBucketAcl | GetBucketAcl | |
| s3:GetBucketCompliance | GET conformidade do bucket (obsoleto) | Sim |
| s3:GetBucketConsistency | GET consistência do bucket | Sim |
| s3:GetBucketCORS | GetBucketCors | |
| s3:GetEncryptionConfiguration | GetBucketEncryption | |
| s3:GetBucketLastAccessTime | Obter o último tempo de acesso do bucket | Sim |
| s3:GetBucketLocation | GetBucketLocation | |
| s3:GetBucketMetadataNotification | GET Configuração de notificação de metadados do bucket | Sim |
| s3:GetBucketNotification | GetBucketNotificationConfiguration | |
| s3:GetBucketObjectLockConfiguration | GetObjectLockConfiguration | |
| s3:GetBucketPolicy | GetBucketPolicy | |
| s3:GetBucketTagging | GetBucketTagging | |
| s3:GetBucketVersioning | GetBucketVersioning | |
| s3:GetLifecycleConfiguration | GetBucketLifecycleConfiguration | |
| s3:GetReplicationConfiguration | GetBucketReplication | |
| s3:ListAllMyBuckets | • ListBuckets<br>• GET Uso de Armazenamento | Sim, para GET Storage Usage.<br>**Nota**: use somente em políticas de grupo. |
| s3:ListBucket | • ListObjects<br>• HeadBucket<br>• RestoreObject | |

| Permissões | Operações da API REST do S3 | Personalizado para StorageGRID |
| --- | --- | --- |
| s3:ListBucketMultipartUploads | • ListMultipartUploads<br>• RestoreObject | |
| s3:ListBucketVersions | GET versões do Bucket | |
| s3:PutBucketCompliance | PUT Bucket compliance (obsoleto) | Sim |
| s3:PutBucketConsistency | Consistência de PUT Bucket | Sim |
| s3:PutBucketCORS | • DeleteBucketCors†<br>• PutBucketCors | |
| s3:PutEncryptionConfiguration | • DeleteBucketEncryption<br>• PutBucketEncryption | |
| s3:PutBucketLastAccessTime | Último tempo de acesso do PUT Bucket | Sim |
| s3:PutBucketMetadataNotification | PUT Configuração de notificação de metadados do bucket | Sim |
| s3:PutBucketNotification | PutBucketNotificationConfiguration | |
| s3:PutBucketObjectLockConfiguration | • CreateBucket com o `x-amz-bucket-object-lock-enabled: true` cabeçalho da solicitação (também requer a permissão s3:CreateBucket)<br>• PutObjectLockConfiguration | |
| s3:PutBucketPolicy | PutBucketPolicy | |
| s3:PutBucketTagging | • DeleteBucketTagging†<br>• PutBucketTagging | |
| s3:PutBucketVersioning | PutBucketVersioning | |
| s3:PutLifecycleConfiguration | • DeleteBucketLifecycle†<br>• PutBucketLifecycleConfiguration | |
| s3:PutReplicationConfiguration | PutBucketReplication | Sim, permissões separadas para PUT e DELETE |

**Permissões que se aplicam a objetos**

| Permissões | Operações da API REST do S3 | Personalizado para StorageGRID |
|---|---|---|
| s3:AbortMultipartUpload | • AbortMultipartUpload<br>• RestoreObject | |
| s3:BypassGovernanceRetention | • DeleteObject<br>• DeleteObjects<br>• PutObjectRetention | |
| s3:DeleteObject | • DeleteObject<br>• DeleteObjects<br>• RestoreObject | |
| s3:DeleteObjectTagging | DeleteObjectTagging | |
| s3:DeleteObjectVersionTagging | DeleteObjectTagging (uma versão específica do objeto) | |
| s3:DeleteObjectVersion | DeleteObject (uma versão específica do objeto) | |
| s3:GetObject | • GetObject<br>• HeadObject<br>• RestoreObject<br>• SelectObjectContent | |
| s3:GetObjectAcl | GetObjectAcl | |
| s3:GetObjectLegalHold | GetObjectLegalHold | |
| s3:GetObjectRetention | GetObjectRetention | |
| s3:GetObjectTagging | GetObjectTagging | |
| s3:GetObjectVersionTagging | GetObjectTagging (uma versão específica do objeto) | |
| s3:GetObjectVersion | GetObject (uma versão específica do objeto) | |
| s3:ListMultipartUploadParts | ListParts, RestoreObject | |

| Permissões | Operações da API REST do S3 | Personalizado para StorageGRID |
|---|---|---|
| s3:PutObject | • PutObject<br>• CopyObject<br>• RestoreObject<br>• CreateMultipartUpload<br>• CompleteMultipartUpload<br>• UploadPart<br>• UploadPartCopy | |
| s3:PutObjectLegalHold | PutObjectLegalHold | |
| s3:PutObjectRetention | PutObjectRetention | |
| s3:PutObjectTagging | PutObjectTagging | |
| s3:PutObjectVersionTagging | PutObjectTagging (uma versão específica do objeto) | |
| s3:PutOverwriteObject | • PutObject<br>• CopyObject<br>• PutObjectTagging<br>• DeleteObjectTagging<br>• CompleteMultipartUpload | Sim |
| s3:RestoreObject | RestoreObject | |

#### Use a permissão PutOverwriteObject

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

As configurações possíveis para essa permissão incluem:

- **Permitir**: O cliente pode sobrescrever um objeto. Esta é a configuração padrão.
- **Negar**: O cliente não pode sobrescrever um objeto. Quando definido 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 as etiquetas do objeto S3 não podem ser sobrescritos.
    - Todas as operações de ingestão em andamento são canceladas e um erro é retornado.
    - Se o versionamento do S3 estiver ativado, a configuração Deny impede que as operações

PutObjectTagging ou DeleteObjectTagging modifiquem o TagSet de um objeto e suas versões não atuais.

  - Se um objeto existente não for encontrado, esta permissão não terá efeito.
- Quando essa permissão não está presente, o efeito é o mesmo que se Allow estivesse definido.

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

#### Especificar condições em uma política

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

As condições utilizam pares de chave-valor para avaliação. Um elemento de condição pode conter múltiplas condições, e cada condição pode conter múltiplos pares de chave-valor. O bloco de condição utiliza o seguinte formato:

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

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

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

### Operadores de condição suportados

Os operadores condicionais são categorizados da seguinte forma:

- String
- Numérico
- Booleano
- Endereço IP
- Verificação de valor nulo

| Operadores de condição | Descrição |
| --- | --- |
| StringEquals | Compara uma chave com um valor de string com base na correspondência exata (diferencia maiúsculas de minúsculas). |
| StringNotEquals | Compara uma chave com um valor de string com base na correspondência negada (diferencia maiúsculas de minúsculas). |
| StringEqualsIgnoreCase | Compara uma chave com um valor de string com base em uma correspondência exata (ignora maiúsculas e minúsculas). |
| StringNotEqualsIgnoreCase | Compara uma chave com um valor de string com base na correspondência negada (ignora maiúsculas e minúsculas). |
| StringLike | Compara uma chave com um valor de string com base na correspondência exata (diferencia maiúsculas de minúsculas). Pode incluir os caracteres curinga * e ?. |
| StringNotLike | Compara uma chave com um valor de string com base na correspondência negada (diferencia maiúsculas de minúsculas). Pode incluir os caracteres curinga * e ?. |
| NumericEquals | Compara uma chave a um valor numérico com base em uma correspondência exata. |
| NumericNotEquals | Compara uma chave a um valor numérico com base na correspondência negada. |
| NumericGreaterThan | Compara uma chave a um valor numérico com base na correspondência "maior que". |
| NumericGreaterThanEquals | Compara uma chave a um valor numérico com base na correspondência "maior ou igual a". |
| NumericLessThan | Compara uma chave a um valor numérico com base na correspondência "menor que". |
| NumericLessThanEquals | Compara uma chave a um valor numérico com base na correspondência "menor ou igual a". |
| Bool | Compara uma chave a um valor booleano com base na correspondência "verdadeiro ou falso". |
| IpAddress | Compara uma chave a um endereço IP ou intervalo de endereços IP. |
| NotIpAddress | Compara uma chave a um endereço IP ou intervalo de endereços IP com base na correspondência negada. |

| Operadores de condição | Descrição |
| --- | --- |
| Nulo | Verifica se uma chave de condição está presente no contexto da solicitação atual. |
| IfExists | Adicionado a qualquer operador de condição, exceto a condição Null, para verificar a ausência da chave de condição. Retorna VERDADEIRO se a chave de condição não estiver presente. |

**Chaves de condição suportadas**

| Chaves de condição | Ações | Descrição |
| --- | --- | --- |
| aws:SourceIp | Operadores de IP | Será comparado ao endereço IP de onde a solicitação foi enviada. Pode ser usado para operações de bucket ou objeto.<br><br>**Nota:** Se a solicitação S3 foi enviada através do serviço Load Balancer nos nós Admin e Gateway, ela será comparada com o endereço IP upstream do serviço Load Balancer.<br><br>**Nota**: Se um balanceador de carga de terceiro não transparente for utilizado, a comparação será feita com o endereço IP desse balanceador de carga. Qualquer `X-Forwarded-For` cabeçalho será ignorado, pois sua validade não pode ser verificada. |
| aws:username | Recurso/Identidade | Será comparado ao nome de usuário do remetente da solicitação. Pode ser usado para operações de bucket ou objeto. |
| s3:delimitador | s3:ListBucket e<br><br>s3:ListBucketVersions permissões | Será comparado ao parâmetro delimitador especificado em uma solicitação ListObjects ou ListObjectVersions. |

| Chaves de condição | Ações | Descrição |
| --- | --- | --- |
| s3:ExistingObjectTag/<tag-key> | s3:DeleteObjectTagging<br><br>s3:DeleteObjectVersionTagging<br><br>s3:GetObject<br><br>s3:GetObjectAcl<br><br>3:GetObjectTagging<br><br>s3:GetObjectVersion<br><br>s3:GetObjectVersionAcl<br><br>s3:GetObjectVersionTagging<br><br>s3:PutObjectAcl<br><br>s3:PutObjectTagging<br><br>s3:PutObjectVersionAcl<br><br>s3:PutObjectVersionTagging | Será necessário que o objeto existente possua a chave e o valor de tag específicos. |
| s3:max-keys | s3:ListBucket e<br><br>s3:ListBucketVersions permissões | Será comparado ao parâmetro max-keys especificado em uma solicitação ListObjects ou ListObjectVersions. |
| s3:modo de bloqueio de objeto | s3:PutObject | Compara com o `object-lock-mode` expandido do cabeçalho da solicitação nas solicitações PutObject, CopyObject e CreateMultipartUpload. |
| s3:modo de bloqueio de objeto | s3:PutObjectRetention | Compara com a `object-lock-mode` expandida do corpo XML na solicitação PutObjectRetention. |
| s3:object-lock-remaining-retention-days | s3:PutObject | Compara com a data de retenção especificada no `x-amz-object-lock-retain-until-date`cabeçalho da solicitação ou calculada a partir do período de retenção padrão do bucket para garantir que esses valores estejam dentro do intervalo permitido para as seguintes solicitações:<br><br>• PutObject<br>• CopyObject<br>• CreateMultipartUpload |

| Chaves de condição | Ações | Descrição |
| --- | --- | --- |
| s3:object-lock-remaining-retention-days | s3:PutObjectRetention | Compara com a data de retenção especificada na solicitação PutObjectRetention para garantir que esteja dentro do intervalo permitido. |
| s3:prefix | s3:ListBucket e<br><br>s3:ListBucketVersions permissões | Será comparado ao parâmetro de prefixo especificado em uma solicitação ListObjects ou ListObjectVersions. |
| s3:RequestObjectTag/<tag-key> | s3:PutObject<br><br>s3:PutObjectTagging<br><br>s3:PutObjectVersionTagging | Será necessário especificar uma chave e um valor de tag quando a solicitação do objeto incluir tagging. |
| s3:x-amz-server-side-encryption-customer-algorithm | s3:PutObject | Compara com o `sse-customer-algorithm` ou com o `copy-source-sse-customer-algorithm` expandido do cabeçalho da solicitação nas solicitações PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy e CompleteMultipartUpload. |

#### Especifique variáveis em uma política

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

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

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

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

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

| Variável | Descrição |
| --- | --- |
| `${aws:SourceIp}` | Utiliza a chave SourceIp como a variável fornecida. |
| `${aws:username}` | Utiliza a chave de nome de usuário como a variável fornecida. |
| `${s3:prefix}` | Utiliza a chave de prefixo específica do serviço como variável fornecida. |
| `${s3:max-keys}` | Utiliza a chave max-keys específica do serviço como variável fornecida. |
| `${*}` | Caractere especial. Usa o caractere como um caractere literal *. |
| `${?}` | Caractere especial. Usa o caractere como um caractere literal "?" |
| `${$}` | Caractere especial. Usa o caractere como um caractere $ literal. |

#### Criar políticas que exigem tratamento especial

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

| Descrição da política | Tipo de política | Comportamento da Amazon | Comportamento do StorageGRID |
| --- | --- | --- | --- |
| Negue a si mesmo quaisquer permissões para a conta root | Bucket | Válido e aplicado, mas a conta de usuário raiz mantém permissão para todas as operações de política do bucket S3 | Mesmo |
| Negar a si mesmo quaisquer permissões para usuário/grupo | Grupo | Válido e em vigor | Mesmo |
| Permitir que um grupo de contas estrangeiras tenha qualquer permissão | Bucket | Principal inválido | Válido, mas as permissões para todas as operações de política do bucket S3 retornam um erro 405 Method Not Allowed quando permitidas por uma política |

| Descrição da política | Tipo de política | Comportamento da Amazon | Comportamento do StorageGRID |
|---|---|---|---|
| Permitir que o usuário raiz ou usuário de uma conta estrangeira tenha qualquer permissão | Bucket | Válido, mas as permissões para todas as operações de política do bucket S3 retornam um erro 405 Method Not Allowed quando permitidas por uma política | Mesmo |
| Permitir que todos tenham permissão para realizar todas as ações | Bucket | Válido, mas as permissões para todas as operações de política do bucket S3 retornam um erro 405 Method Not Allowed para o usuário raiz e usuários da conta externa | Mesmo |
| Negar permissões a todos para todas as ações | Bucket | Válido e aplicado, mas a conta de usuário raiz mantém permissão para todas as operações de política do bucket S3 | Mesmo |
| Principal é um usuário ou grupo inexistente | Bucket | Principal inválido | Válido |
| O recurso é um bucket S3 inexistente | Grupo | Válido | Mesmo |
| Principal é um grupo local | Bucket | Principal inválido | Válido |
| A política concede permissões a contas que não são proprietárias (incluindo contas anônimas) para colocar objetos. | Bucket | Válido. Os objetos pertencem à conta do criador e a política do bucket não se aplica. A conta do criador deve conceder permissões de acesso ao objeto usando ACLs de objeto. | Válido. Os objetos pertencem à conta proprietária do bucket. A política do bucket se aplica. |

#### Proteção WORM (gravação única e leitura múltipla)

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

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

- No Grid Manager, acesse **Configuração** > **Segurança** > **Configurações de segurança** > **Rede e objetos** e selecione a caixa de seleção **Impedir modificação do cliente**.
- Aplique as seguintes regras e políticas do S3:

- Adicione uma operação DENY PutOverwriteObject à política do S3.
- Adicione uma operação DENY DeleteObject à política do S3.
- Adicione uma operação ALLOW PutObject à política do S3.

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

> Mesmo quando todas essas regras e políticas são aplicadas, elas não impedem gravações simultâneas (veja a Situação A). Elas impedem sobrescritas sequenciais concluídas (veja a Situação B).

**Situação A**: Escritas simultâneas (sem proteção)

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

**Situação B**: Sobrescritas sequenciais concluídas (protegidas contra)

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

**Informações relacionadas**

- "Como as regras do StorageGRID ILM gerenciam objetos"
- "Exemplos de políticas de bucket"
- "Exemplos de políticas de grupo"
- "Exemplo de política de sessão"
- "Gerencie objetos com ILM"
- "Use uma conta de tenant"

### Exemplo de política de sessão da API REST do StorageGRID S3

Utilize o exemplo a seguir para criar uma política de sessão do StorageGRID.

#### Exemplo: configure uma política de sessão que permita a recuperação de objetos

Neste exemplo, o usuário principal da sessão só tem permissão para recuperar objetos do bucket1. Todas as outras ações são implicitamente negadas, exceto as ações específicas do StorageGRID, como o uso da "s3:PutOverwriteObject" permissão. A política de sessão pode ser fornecida como um arquivo JSON ao chamar a AssumeRole API.

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

#### Exemplos de políticas de bucket da API REST S3 do StorageGRID

## Utilize os exemplos desta seção para criar políticas de acesso do StorageGRID para buckets.

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

- "Tenant Manager".
- AWS CLI usando este comando (consulte "Operações em buckets"):

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

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

Neste exemplo, todos, incluindo anônimos, têm permissão para listar objetos no bucket e realizar operações GetObject em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que essa política pode não ser particularmente útil porque ninguém, exceto o usuário raiz, 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: permitir acesso total a todos em uma conta e acesso somente leitura a um bucket para todos em outra conta**

Neste exemplo, todos em uma conta específica têm permissão para acesso total a um bucket, enquanto todos em outra conta específica têm permissão apenas para listar o bucket e realizar operações GetObject em objetos no bucket que começam com o prefixo da chave do objeto `shared/`.

> No StorageGRID, os objetos criados por uma conta que não seja a proprietária (incluindo contas anônimas) pertencem à conta proprietária do bucket. A política do bucket se aplica a esses objetos.

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

#### Exemplo: permitir acesso somente leitura a um bucket para todos e acesso total para um grupo específico

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

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

#### Exemplo: permitir acesso de leitura e gravação a um bucket para todos os clientes se estiverem no intervalo de IP

Neste exemplo, todos, incluindo usuários anônimos, têm permissão para listar o bucket e executar quaisquer operações de objeto em todos os objetos do bucket, desde que as solicitações venham de um intervalo de IP especificado (54.240.143.0 a 54.240.143.255, exceto 54.240.143.188). Todas as outras operações serão negadas e todas as solicitações fora do intervalo de IP serão negadas.

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

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

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

```
{
  "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`Effect para PutOverwriteObject e DeleteObject garante que ninguém possa sobrescrever ou excluir os dados do objeto, os metadados definidos pelo usuário e a marcação do objeto 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/*"
    }
  ]
}
```

#### Exemplos de política de grupo da API REST do StorageGRID S3

Utilize os exemplos desta seção para criar políticas de acesso do StorageGRID para grupos.

As políticas de grupo especificam as permissões de acesso para o grupo ao qual a política está associada. Não há nenhum `Principal` elemento na política, pois ela é implícita. As políticas de grupo são configuradas usando o Tenant Manager ou a API.

#### Exemplo: defina a política de grupo usando o Tenant Manager

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

- **Sem acesso ao S3**: Opção padrão. Os usuários deste grupo não têm acesso aos recursos do S3, a menos que o acesso seja concedido por meio de uma política de bucket. Se você selecionar esta opção, somente o usuário raiz 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 deste grupo podem listar objetos e ler dados, metadados e tags dos objetos. Ao selecionar esta opção, a string JSON para uma política de grupo somente leitura aparece na caixa de texto. Você não pode editar esta string.
- **Acesso total**: Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Ao selecionar esta opção, a string JSON para uma política de grupo de acesso total aparece na caixa de texto. Você não pode editar esta string.
- **Mitigação de ransomware**: Esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários deste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que tenham o versionamento de objetos ativado.

  Os usuários do Tenant Manager que possuem a permissão Manage all buckets podem substituir esta política de grupo. Limite a permissão Manage all buckets a usuários confiáveis e utilize a autenticação multifator (MFA) quando disponível.

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

#### Exemplo: permitir que o grupo tenha acesso total a todos os buckets

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

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

#### Exemplo: permitir acesso somente leitura ao grupo em todos os buckets

Neste exemplo, todos os membros do grupo têm acesso somente leitura aos recursos do S3, a menos que seja explicitamente negado pela política do bucket. Por exemplo, os usuários deste grupo podem listar objetos e ler dados, metadados e tags dos 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: Permitir que os membros do grupo tenham acesso total apenas à sua "pasta" em um bucket**

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

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

## Operações S3 rastreadas nos logs de auditoria do StorageGRID

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

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

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- HeadBucket
- ListObjects
- ListObjectVersions
- Conformidade de bucket PUT
- PutBucketTagging
- PutBucketVersioning

**Operações de objetos registradas nos logs de auditoria**

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- HeadObject
- PutObject
- RestoreObject
- SelectObject
- UploadPart (quando uma regra ILM usa ingestão balanceada ou estrita)
- UploadPartCopy (quando uma regra ILM usa ingestão balanceada ou estrita)

**Informações relacionadas**

- "Acesse o arquivo de log de auditoria"
- "Cliente escreve mensagens de log de auditoria"
- "Mensagens de leitura do log de auditoria do cliente"

# Usar API REST (fim de vida útil)

## Suporte à API REST Swift no StorageGRID

O suporte para a API Swift chegou ao fim de sua vida útil e será removido em uma versão futura.

Detalhes sobre o Swift foram removidos desta versão do site de documentação. Veja "StorageGRID 11.8: usar API REST Swift".

## Informações sobre direitos autorais



## Informações sobre marcas comerciais