# Use uma conta de locatário

StorageGRID

NetApp
March 12, 2025

# Índice

# Use uma conta de locatário

## Use uma conta de locatário: Visão geral

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

### O que é uma conta de locatário?

Cada conta de locatário tem seus próprios grupos federados ou locais, usuários, buckets do S3 ou contentores Swift e objetos.

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

- **Caso de uso corporativo:** se o sistema StorageGRID estiver sendo usado dentro de uma empresa, o armazenamento de objetos da grade pode ser segregado pelos diferentes departamentos da organização. Por exemplo, pode haver contas de inquilino para o departamento de marketing, o departamento de suporte ao cliente, o departamento de recursos humanos e assim por diante.

  > Se você usar o protocolo cliente S3, também poderá 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. Consulte as instruções de implementação "Buckets e políticas de buckets do S3" para obter mais informações.

- * Caso de uso do provedor de serviços:* se o sistema StorageGRID estiver sendo usado por um provedor de serviços, o armazenamento de objetos da grade pode ser segregado pelas diferentes entidades que alugam o armazenamento. Por exemplo, pode haver contas de inquilino para a empresa A, empresa B, empresa C e assim por diante.

### Como criar uma conta de locatário

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

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

Além disso, os administradores de grade podem ativar a configuração bloqueio de objeto S3 para o sistema StorageGRID se as contas de locatário S3 precisarem cumprir os requisitos regulamentares. Quando o bloqueio de objeto S3 está ativado, todas as contas de locatário do S3 podem criar e gerenciar buckets compatíveis.

#### Configurar locatários do S3

Depois de um "S3 conta de locatário é criada", você pode acessar o Gerenciador do Locatário para executar tarefas como as seguintes:

- Configurar federação de identidade (a menos que a origem de identidade seja compartilhada com a grade)
- Gerenciar grupos e usuários
- Use a federação de grade para clone de conta e replicação entre grade
- Gerenciar S3 chaves de acesso
- Crie e gerencie buckets do S3
- Use os serviços da plataforma S3
- Utilize S3 Select (Selecionar)
- Monitorar o uso do storage

Embora você possa criar e gerenciar buckets do S3 com o Gerenciador do locatário, use um "Cliente S3" ou "S3 Console" para obter e gerenciar objetos.

#### Configurar os locatários Swift

Depois de um "Conta de locatário Swift foi criada", você pode acessar o Gerenciador do Locatário para executar tarefas como as seguintes:

- Configurar federação de identidade (a menos que a origem de identidade seja compartilhada com a grade)
- Gerenciar grupos e usuários
- Monitorar o uso do storage

Os usuários Swift devem ter a permissão de acesso root para acessar o Gerenciador do locatário. No entanto, a permissão de acesso root não permite que os usuários se autentiquem no "Swift REST API" para criar containers e ingerir objetos. Os usuários devem ter a permissão Swift Administrator para se autenticar na API Swift REST.

# Como entrar e sair

## Inicie sessão no Tenant Manager

Você acessa o Gerenciador do Locatário inserindo o URL do locatário na barra de endereços de um "navegador da web suportado".

#### Antes de começar

- Você tem suas credenciais de login.
- Você tem um URL para acessar o Gerenciador do Locatário, conforme fornecido pelo administrador da grade. O URL será parecido com 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
```

O URL sempre inclui um nome de domínio totalmente qualificado (FQDN), o endereço IP de um nó de administração ou o endereço IP virtual de um grupo de HA de nós de administração. Ele também pode incluir um número de porta, o ID da conta de locatário de 20 dígitos ou ambos.

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

**Passos**

1. Inicie um "navegador da web suportado".
2. Na barra de endereços do navegador, insira o URL para acessar o Gerenciador de locatários.
3. Se for solicitado um alerta de segurança, instale o certificado usando o assistente de instalação do navegador.
4. Inicie sessão no Gestor do Locatário.

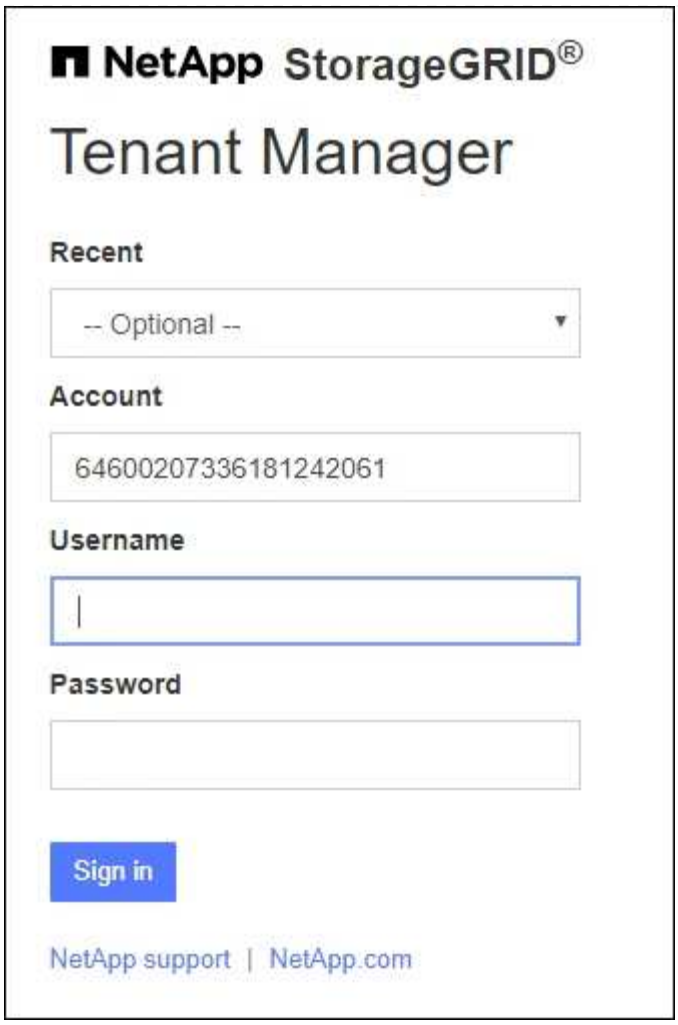
   A tela de login exibida depende do URL digitado e se o SSO (logon único) foi configurado para o StorageGRID.

**Não está a utilizar SSO**

Se o StorageGRID não estiver usando SSO, uma das seguintes telas será exibida:

- A página de login do Gerenciador de Grade. Selecione o link **Logon** do locatário.


- A página de início de sessão do Tenant Manager. O campo **Account** pode já estar concluído, como mostrado abaixo.




i. Se o ID da conta de 20 dígitos do locatário 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. Introduza o seu nome de utilizador e palavra-passe.

iii. Selecione **entrar**.

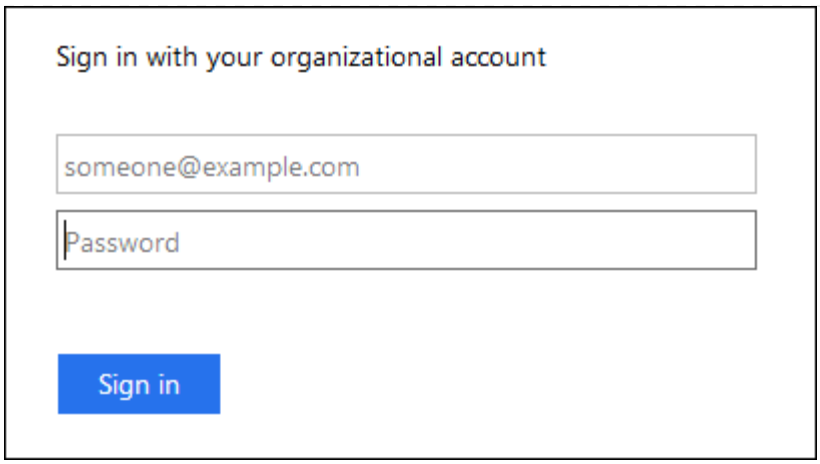
É apresentado o painel do Tenant Manager.

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

**Usando SSO**

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

◦ Página SSO da sua organização. Por exemplo:




Insira suas credenciais SSO padrão e selecione **entrar**.

- A página de login SSO do Tenant Manager.


i. Se o ID da conta de 20 dígitos do locatário 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 **entrar**.

iii. Inicie sessão com as suas credenciais SSO padrão na página de início de sessão SSO da sua organização.

É apresentado o painel do Tenant Manager.

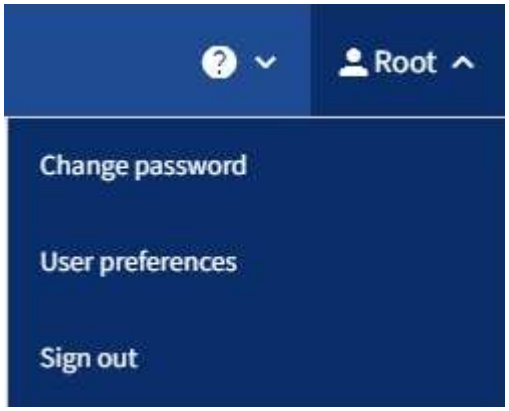
## Sair do Tenant Manager

Quando terminar de trabalhar com o Gestor de Locatário, tem de terminar sessão para

garantir que os utilizadores não autorizados não possam aceder ao sistema StorageGRID. Fechar seu navegador pode não sair do sistema, com base nas configurações de cookies do navegador.

**Passos**

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




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

   - Se o SSO não estiver em uso:

     Você está desconetado do Admin Node. É apresentada a página de início de sessão do Gestor do Locatário.

     Se você tiver feito login em mais de um nó de administrador, será necessário sair de cada nó.

   - Se o SSO estiver ativado:

     Você está desconetado de todos os nós de administrador que estava acessando. É apresentada a página de início de sessão do StorageGRID. O nome da conta de locatário que você acabou de acessar é listado como padrão na lista suspensa **Recent Accounts** (Contas recentes) e o **Account ID** do locatário é mostrado.

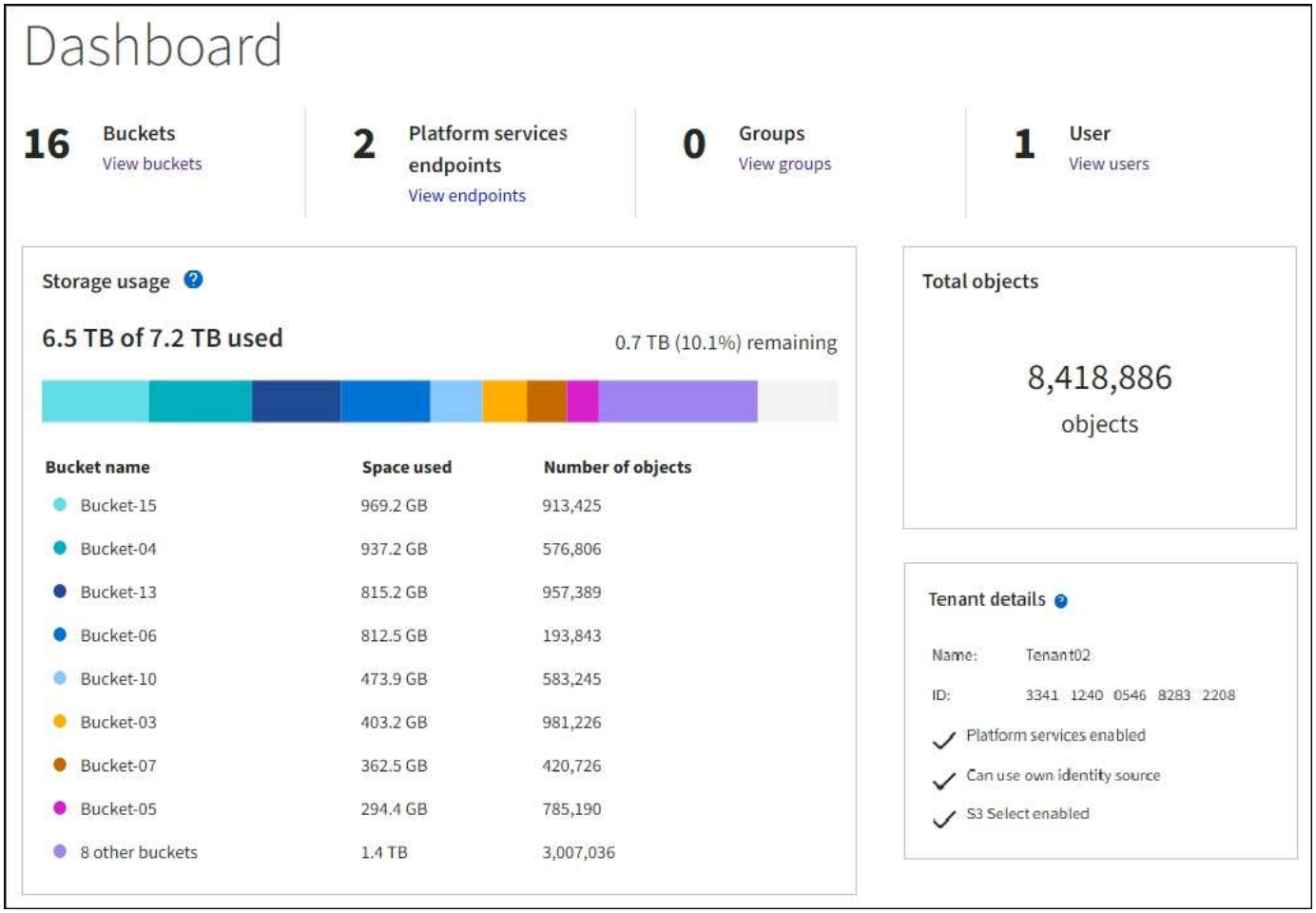
     Se o SSO estiver ativado e você também estiver conetado ao Gerenciador de Grade, você também deverá sair do Gerenciador de Grade para sair do SSO.

# Entenda o painel do Tenant Manager

O painel do Tenant Manager fornece uma visão geral da configuração de uma conta de locatário e da quantidade de espaço usada por objetos nos buckets do locatário (S3) ou contentores (Swift). Se o locatário tiver uma cota, o painel mostrará quanto da cota é usada e quanto resta. Se houver algum erro relacionado à conta do locatário, os erros serão exibidos no painel.

Os valores espaço utilizado são estimativas. Essas estimativas são afetadas pelo timing de inests, conetividade de rede e status de nó.

Quando os objetos tiverem sido carregados, o painel se parece com o seguinte exemplo:




## Resumo da conta do locatário

A parte superior do painel contém as seguintes informações:

- O número de buckets ou contêineres configurados, grupos e usuários
- O número de endpoints de serviços de plataforma, se algum tiver sido configurado

Pode selecionar as ligações para ver os detalhes.

O lado direito do painel de instrumentos contém as seguintes informações:

- O número total de objetos para o locatário.

  Para uma conta do S3, se nenhum objeto tiver sido ingerido e você tiver as "Permissão de acesso à raiz"diretrizes , Introdução aparecerão em vez do número total de objetos.

- Detalhes do locatário, incluindo o nome e a ID da conta do locatário e se o locatário pode usar "serviços de plataforma", "sua própria fonte de identidade", "federação de grade"ou "S3 Selecione" (somente as permissões habilitadas são listadas).

## Uso de storage e cota

O painel uso do armazenamento contém as seguintes informações:

- A quantidade de dados de objeto para o locatário.

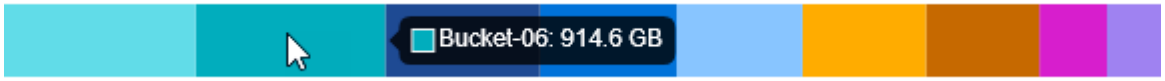
  Esse valor indica a quantidade total de dados de objeto carregados e não representa o espaço usado para armazenar cópias desses objetos e seus metadados.

- Se uma cota for definida, a quantidade total de espaço disponível para os dados do objeto 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, o StorageGRID verifica a cota quando um locatário começa a carregar objetos e rejeita novos ingere se o locatário tiver excedido a cota. No entanto, o StorageGRID não leva em conta o tamanho do upload atual ao determinar se a cota foi excedida. Se os objetos forem excluídos, um locatário poderá ser temporariamente impedido de carregar novos objetos até que o uso da cota seja recalculado. Os cálculos de uso de cotas podem levar 10 minutos ou mais.

- Um gráfico de barras que representa os tamanhos relativos dos maiores baldes ou contentores.

  Você pode colocar o cursor sobre qualquer um dos segmentos do gráfico para visualizar o espaço total consumido por esse intervalo ou contentor.




- Para corresponder ao gráfico de barras, uma lista dos maiores buckets ou contentores, incluindo a quantidade total de dados do objeto e o número de objetos para cada bucket ou contentor.

| 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 locatário tiver mais de nove buckets ou contêineres, todos os outros buckets ou contêineres serão combinados em uma única entrada na parte inferior da lista.

Para alterar as unidades para os valores de armazenamento exibidos no Gerenciador do locatário, selecione a lista suspensa usuário no canto superior direito do Gerenciador do locatário e selecione **Preferências do usuário**.

### Alertas de uso de cota

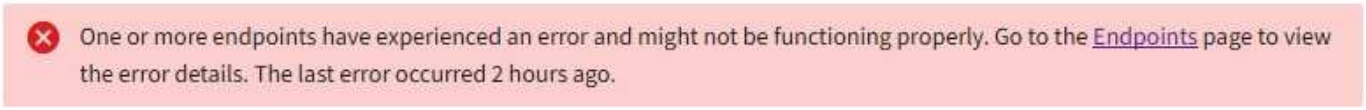
Se os alertas de uso de cota tiverem sido ativados no Gerenciador de Grade, eles aparecerão no Gerenciador de Locatário quando a cota for baixa ou excedida, da seguinte forma:

Se 90% ou mais da cota de um locatário tiver sido usada, o alerta **uso de cota de locatário alto** será acionado. Execute as ações recomendadas para o alerta.


Se você exceder sua cota, não poderá carregar novos objetos.


### Erros de endpoint

Se você usou o Gerenciador de Grade para configurar um ou mais endpoints para uso com serviços de plataforma, o painel do Gerenciador do locatário exibirá um alerta se algum erro de endpoint tiver ocorrido nos últimos sete dias.




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

# API de gerenciamento do locatário

## Entenda a API de gerenciamento do locatário

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

A API de gerenciamento do locatário:

- Usa a plataforma de API Swagger de código aberto. O Swagger fornece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores interajam com a API. A interface do usuário Swagger fornece detalhes completos e documentação para cada operação da API.
- Utiliza "controle de versão para dar suporte a atualizações sem interrupções".

Para acessar a documentação do Swagger para a API de gerenciamento do locatário:

1. Inicie sessão no Gestor do Locatário.
2. Na parte superior do Gerenciador do Locatário, selecione o ícone de ajuda e selecione **Documentação da API**.

### Operações da API

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

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

  A API de gerenciamento do locatário suporta o esquema de autenticação de token do portador. Para um login de locatário, 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 êxito, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("autorização: Token portador").

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

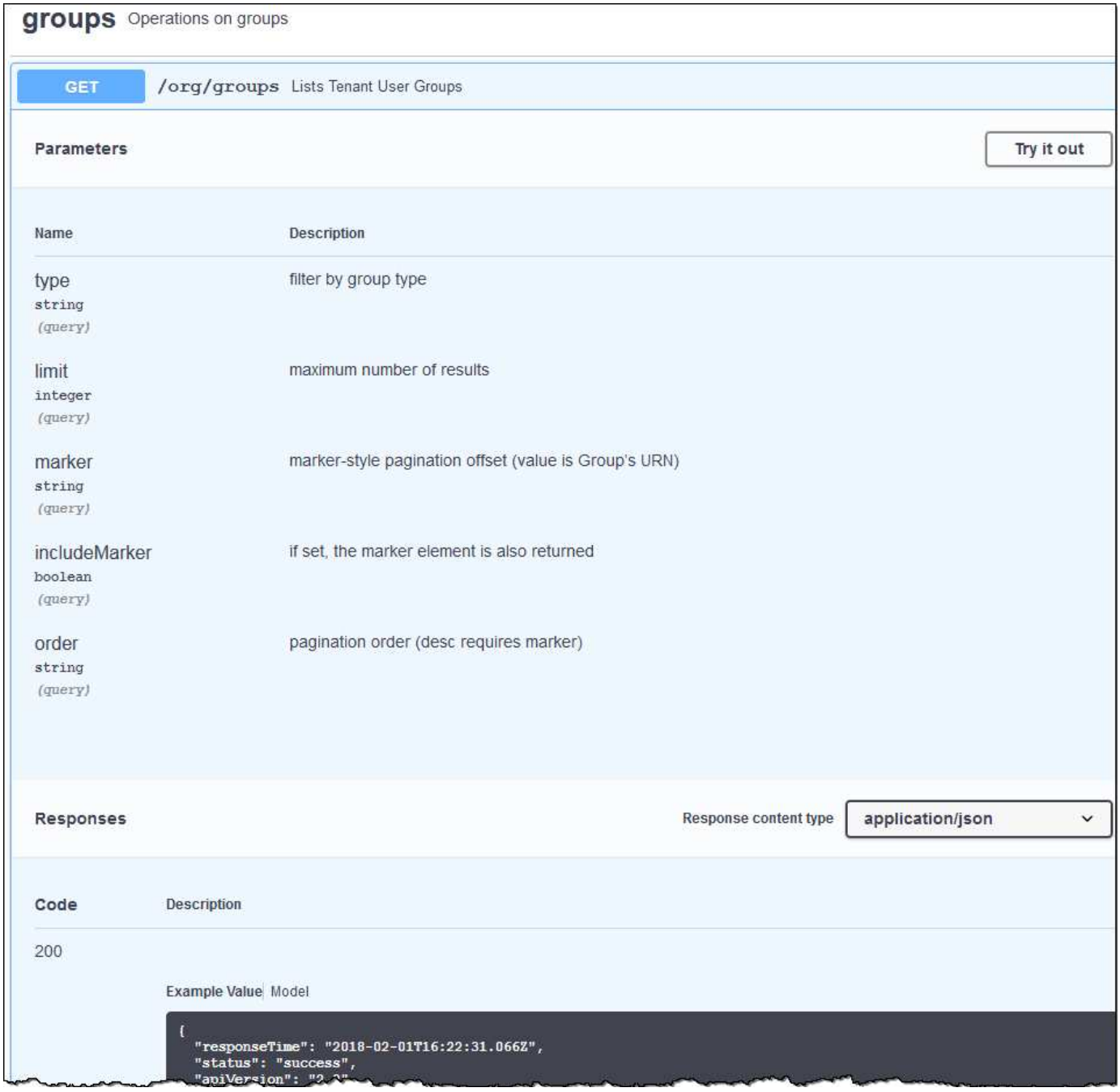
  > Se o logon único (SSO) estiver ativado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Consulte "Instruções para usar a API Grid Management".

- **Config**: Operações relacionadas à versão do produto e versões da API de Gerenciamento do Tenant. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **Containers**: Operações em baldes S3 ou contentores Swift.
- **Disabled-features**: Operações para visualizar recursos que podem ter sido desativados.
- **Endpoints**: Operações para gerenciar um endpoint. Os endpoints permitem que um bucket do S3 use um serviço externo para replicação, notificações ou integração de pesquisa do StorageGRID CloudMirror.
- * Grid-federação-conexões*: Operações em conexões de federação de grade e replicação entre grade.
- **Groups**: 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 federado e de usuário.
- **ilm**: Operações nas configurações de gerenciamento do ciclo de vida da informação (ILM).
- **Regions**: Operações para determinar quais regiões foram configuradas para o sistema StorageGRID.
- **S3**: Operações para gerenciar S3 chaves de acesso para usuários arrendatários.
- **S3-object-lock**: Operações em configurações globais de bloqueio de objetos S3D, usadas para suportar a conformidade regulamentar.
- **Usuários**: Operações para visualizar e gerenciar usuários de inquilinos.

### Detalhes da operação

Quando você expande cada operação da API, você pode ver sua ação HTTP, URL do endpoint, uma lista de todos os parâmetros necessários ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as

possíveis respostas.




### Emitir solicitações de API

> Todas as operações de API que você executa usando a página da Web do API Docs são operações ativas. 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 grupo ou ID de usuário. Em seguida, obtenha esses valores. Talvez você precise emitir uma solicitação de API diferente primeiro para obter as informações de que precisa.

3. Determine se você precisa modificar o corpo de solicitação de exemplo. Em caso afirmativo, você pode selecionar **modelo** para aprender os requisitos para cada campo.
4. Selecione **Experimente**.
5. Forneça quaisquer parâmetros necessários ou modifique o corpo do pedido conforme necessário.
6. Selecione **Executar**.
7. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

## Controle de versão da API de gerenciamento de locatário

A API de gerenciamento do locatário usa o controle de versão para oferecer suporte a atualizações sem interrupções.

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

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

A versão principal da API é quebrada quando alterações são feitas que são *não compatíveis* com versões mais antigas. A versão menor da API é quebrada quando alterações são feitas que *são compatíveis* com versões mais antigas. As alterações compatíveis incluem a adição de novos endpoints ou novas propriedades.

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

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

Quando você instala o software StorageGRID pela primeira vez, apenas a versão mais recente da API é ativada. No entanto, quando você atualiza para uma nova versão de recurso do StorageGRID, você continua tendo acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID.

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

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Deprecated: True"
- O corpo de resposta JSON inclui "obsoleto": True
- Um aviso obsoleto é adicionado ao nms.log. Por exemplo:

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

#### Determine quais versões de API são suportadas na versão atual

Use a `GET /versions` solicitação de API para retornar uma lista das principais versões da API suportada. Esta 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
```

## Proteger contra falsificação de solicitação entre locais (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra StorageGRID usando tokens CSRF para melhorar a autenticação que usa cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes de API podem optar por ativá-lo quando fizerem login.

Um invasor que pode acionar uma solicitação para um site diferente (como um POST de formulário HTTP) pode fazer com que certas solicitações sejam feitas usando os cookies do usuário conetado.

O 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 DO corpo DO POST.

Para ativar a funcionalidade, defina o `csrfToken` parâmetro para `true` durante a autenticação. A predefinição 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 `GridCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Grade, e o `AccountCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Tenant.

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

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

Para configurar a proteção CSRF, use o "API de gerenciamento de grade" ou "API de gerenciamento do locatário".

> As solicitações que têm um conjunto de cookies de token CSRF também irão aplicar o cabeçalho "Content-Type: Application/json" para qualquer solicitação que espera um corpo de solicitação JSON como uma proteção adicional contra ataques CSRF.

# Use conexões de federação de grade

## Clonar grupos de locatários e usuários

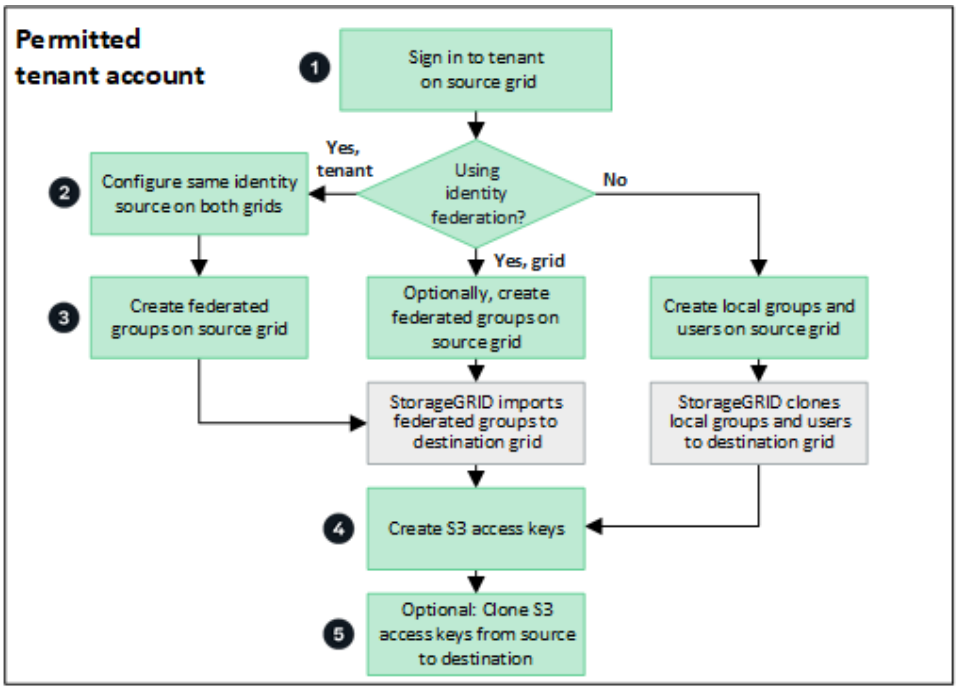
Se um locatário foi criado ou editado para usar uma conexão de federação de grade, esse locatário é replicado de um sistema StorageGRID (o locatário de origem) para outro sistema StorageGRID (o locatário de réplica). Depois que o locatário tiver sido replicado, todos os grupos e usuários adicionados ao locatário de origem serão clonados para o locatário de réplica.

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

A clonagem de informações de conta de locatário é necessária para "replicação entre grade"objetos bucket. Ter os mesmos grupos de inquilinos e usuários em ambas as grades garante que você possa acessar os buckets e objetos correspondentes em qualquer grade.

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

Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, revise o diagrama do fluxo de trabalho para ver as etapas que você executará para clonar grupos, usuários e chaves de acesso S3.




Estas são as etapas principais no fluxo de trabalho:

**Inicie sessão no inquilino**

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

**Opcionalmente, configure a federação de identidade**

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

**Crie grupos e usuários**

Ao criar grupos e usuários, sempre comece a partir da grade de origem do locatário. Quando você adiciona um novo grupo, o StorageGRID o clona automaticamente à grade de destino.

- Se a federação de identidade estiver configurada para todo o sistema StorageGRID ou para sua conta de locatário, "criar novos grupos de inquilinos"importando grupos federados da origem da identidade.
- Se você não estiver usando a federação de identidade "crie novos grupos locais"e, em seguida"crie usuários locais", .

**Crie S3 chaves de acesso**

Você pode "crie suas próprias chaves de acesso" ou fazer "crie chaves de acesso de outro usuário" na grade de origem ou na grade de destino para acessar buckets nessa grade.

5 **Opcionalmente, clonar 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 use a API do Gerenciador do locatário para cloná-las manualmente na grade de destino. Para obter instruções, "Clonar chaves de acesso S3 usando a API"consulte .

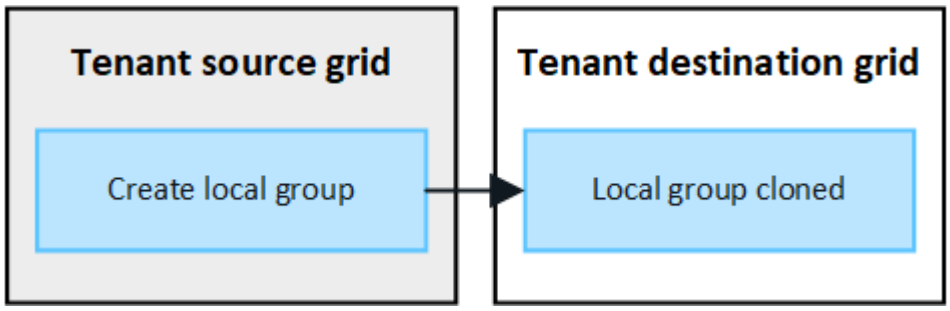
### Como grupos, usuários e chaves de acesso S3 são clonadas?

Revise 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

Depois que uma conta de locatário é criada e replicada na grade de destino, o StorageGRID clonará automaticamente todos os grupos locais adicionados à grade de origem do locatário à grade de destino do locatário.

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

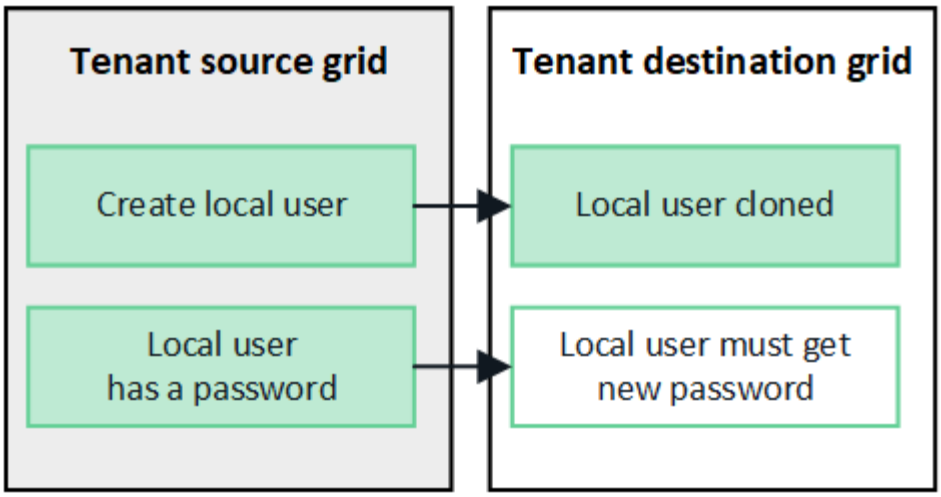



Os usuários selecionados quando você cria um grupo local na grade de origem não são incluídos quando o grupo é clonado para a grade de destino. Por esse motivo, não selecione usuários quando você criar o grupo. Em vez disso, selecione o grupo quando você criar os usuários.

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

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

Por motivos de segurança, as senhas de usuário local não são clonadas para a grade de destino. Se um usuário local precisar acessar o Gerenciador do Locatário na grade de destino, o usuário raiz da conta do locatário deve adicionar uma senha para esse usuário na grade de destino. Para obter instruções, "Gerenciar usuários locais"consulte .

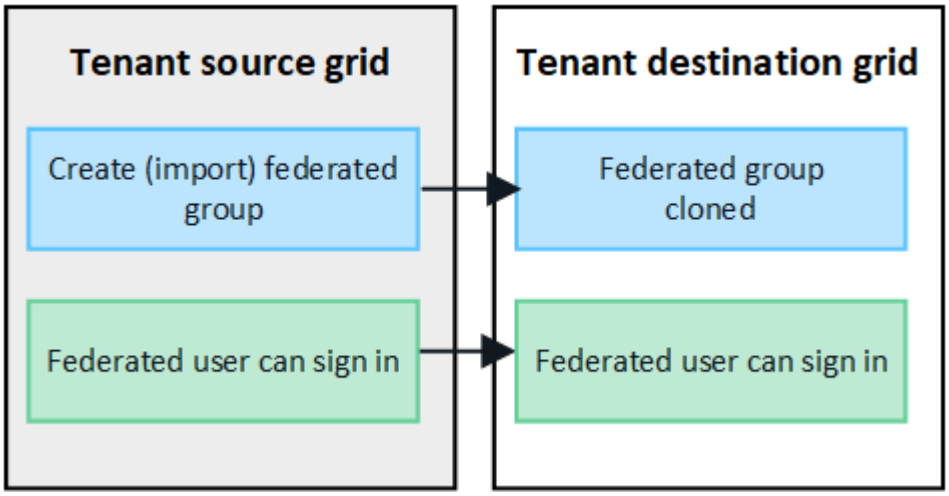



**Os grupos federados criados na grade de origem são clonados**

Supondo que os requisitos para usar o clone de conta com "logon único" e "federação de identidade" tenham sido atendidos, os grupos federados que você criar (importar) para o locatário na grade de origem são 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.

Depois que os grupos federados forem criados para o locatário de origem e clonados para o locatário de destino, os usuários federados poderão fazer login no locatário em qualquer grade.

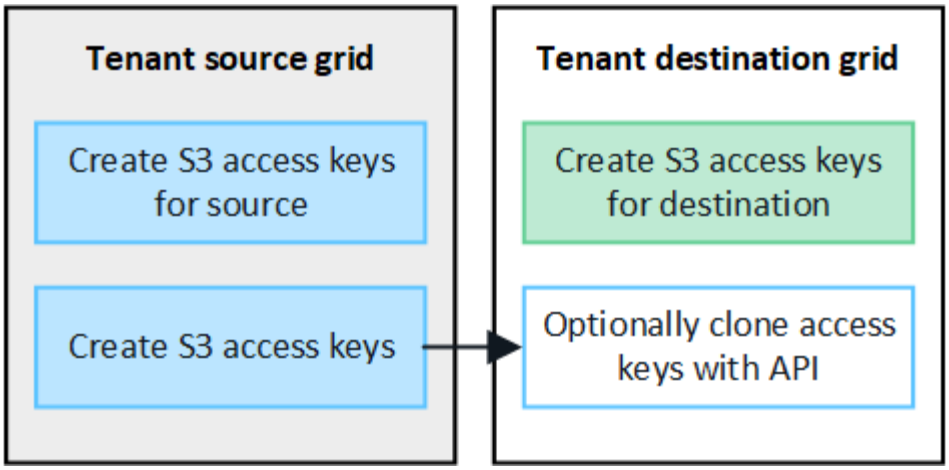



**S3 teclas de acesso podem ser clonadas manualmente**

O StorageGRID não clonar automaticamente as chaves de acesso S3 porque a segurança é melhorada por ter chaves diferentes em cada grade.

Para gerenciar chaves de acesso nas duas grades, você pode fazer um dos seguintes procedimentos:

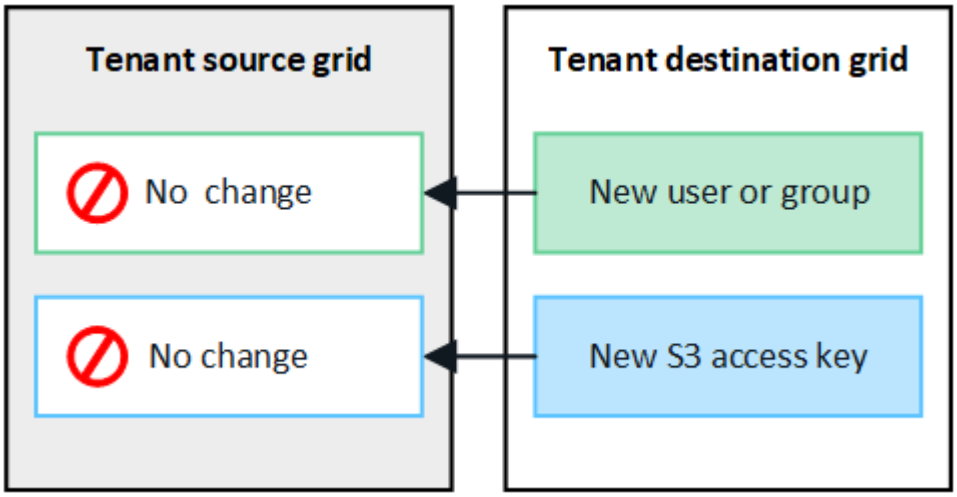
- Se você não precisa usar as mesmas teclas para cada grade, você pode "crie suas próprias chaves de acesso" ou "crie chaves de acesso de outro usuário" em cada grade.
- Se você precisar usar as mesmas chaves em ambas as grades, você pode criar chaves na grade de origem e usar a API do Gerenciador do locatário para manualmente "clone as chaves" para a grade de destino.




Quando você clonar chaves de acesso S3 para um usuário federado, tanto o usuário quanto as chaves de acesso S3 são clonadas para o locatário de destino.

**Os grupos e usuários adicionados à grade de destino não são clonados**

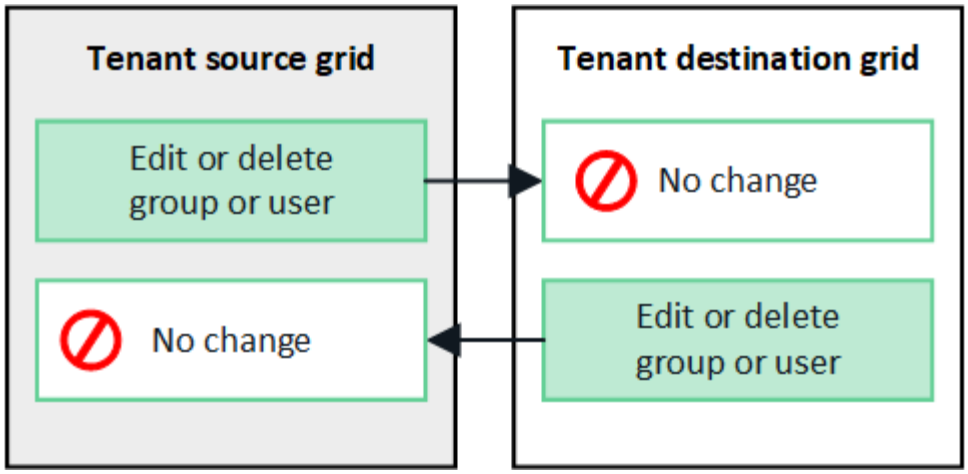
A clonagem ocorre somente da grade de origem do locatário para a grade de destino do locatário. Se você criar ou importar grupos e usuários na grade de destino do locatário, o StorageGRID não clonará esses itens de volta à grade de origem do locatário.




**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 grade, suas alterações não serão clonadas para a outra grade.




## Clonar chaves de acesso S3 usando a API

Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, você poderá usar a API de Gerenciamento do locatário para clonar manualmente as chaves de acesso S3 do locatário na grade de origem para o locatário na grade de destino.

**Antes de começar**

- A conta de locatário tem a permissão **Use Grid Federation Connection**.
- A conexão de federação de grade tem um **status de conexão** de **conectado**.
- Você está conetado ao Gerenciador do Locatário na grade de origem do locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie suas próprias credenciais S3 ou permissão de acesso root".
- Se você estiver clonando chaves de acesso para um usuário local, o usuário já existe em ambas as grades.

> Quando você clonar chaves de acesso S3 para um usuário federado, tanto o usuário quanto as chaves de acesso S3 são adicionadas 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 grades.

**Passos**

1. Usando o Gerenciador do Tenant na grade de origem e "crie suas próprias chaves de acesso"baixe o `.csv` arquivo.
2. Na parte superior do Gerenciador do Locatário, selecione o ícone de ajuda e selecione **Documentação da API**.
3. Na seção **S3**, selecione o seguinte ponto final:

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


4. Selecione **Experimente**.
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-hora ISO 8601 (por exemplo, `2024-02-28T22:46:33-08:00` ). Se a chave não expirar, digite **null** como o valor da entrada **expira** (ou remova a linha **expira** 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 a grade de destino.

### Clonar chaves de acesso de outro usuário

Você pode clonar as chaves de acesso de outro usuário se ele precisar acessar os mesmos buckets em ambas as grades.

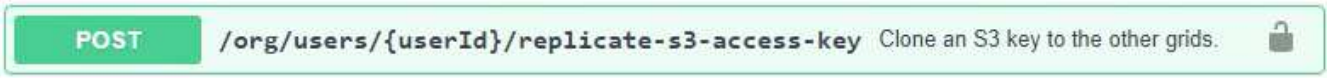
**Passos**

1. Usando o Gerenciador do Tenant na grade de origem e "Crie as chaves de acesso S3 do outro usuário"baixe o `.csv` arquivo.
2. Na parte superior do Gerenciador do Locatário, selecione o ícone de ajuda e selecione **Documentação da API**.
3. Obtenha a ID do utilizador. Você precisará desse valor para clonar as chaves de acesso do outro usuário.
   a. Na seção **usuários**, selecione o seguinte ponto final:

      `GET /org/users`

   b. Selecione **Experimente**.
   c. Especifique quaisquer parâmetros que você deseja usar ao procurar usuários.
   d. Selecione **Executar**.
   e. Encontre o usuário cujas chaves você deseja clonar e copie o número no campo **id**.
4. Na seção **S3**, selecione o seguinte ponto final:

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




5. Selecione **Experimente**.
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 ao redor da string.

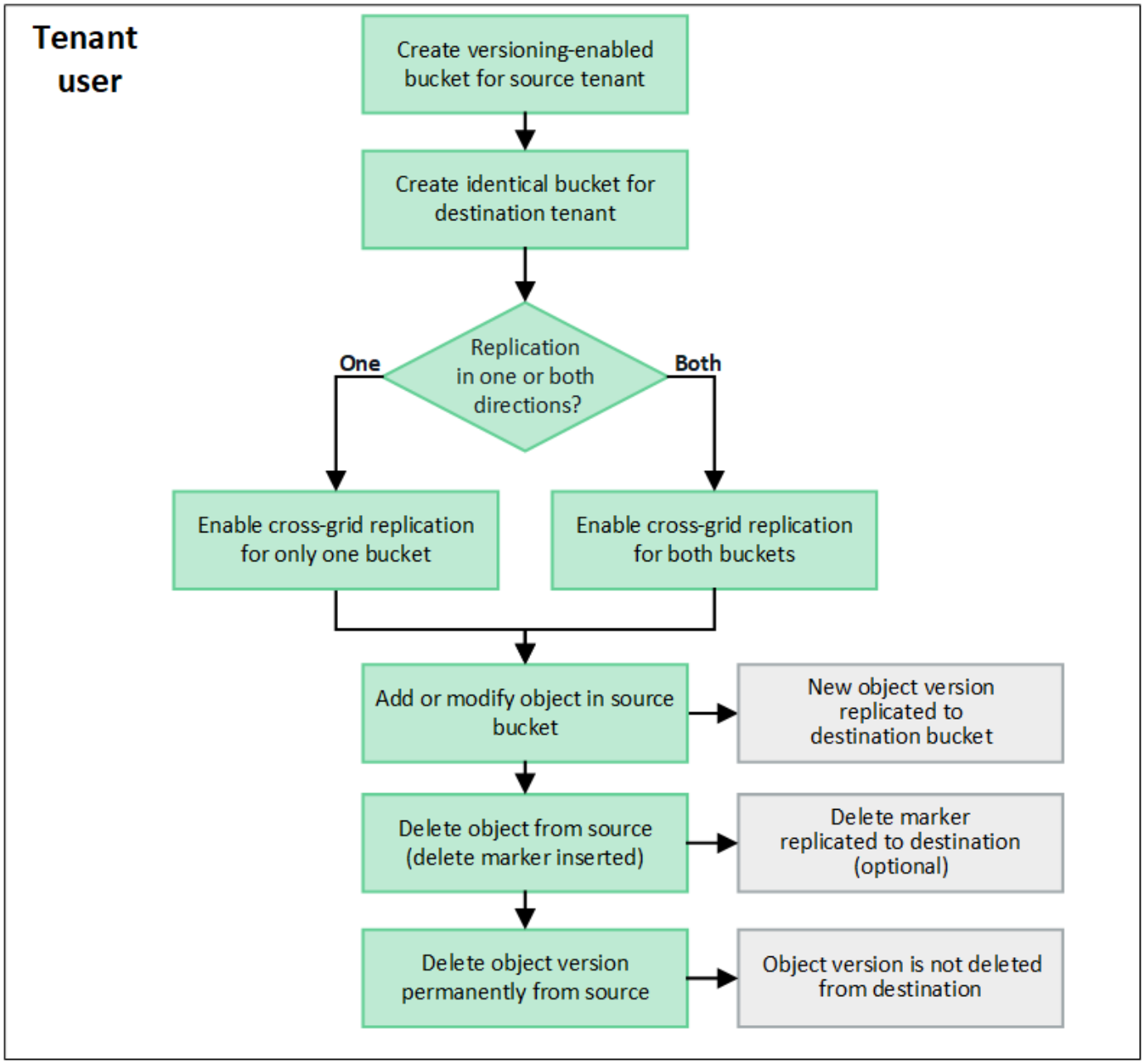
8. Se a chave expirar, substitua a entrada de exemplo para **Expires** pela data e hora de expiração como uma string no formato de data-hora ISO 8601 (por exemplo, `2023-02-28T22:46:33-08:00` ). Se a chave não expirar, digite **null** como o valor da entrada **expira** (ou remova a linha **expira** e 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 a grade de destino.

## Gerenciar a replicação entre grades

Se a sua conta de locatário tiver sido atribuída a permissão **usar conexão de federação de grade** quando ela foi criada, você poderá usar a replicação entre grade para replicar automaticamente objetos entre buckets na grade de origem do locatário e buckets na grade de destino do locatário. A replicação entre grades pode ocorrer em uma ou ambas as direções.

### Fluxo de trabalho para replicação entre grades

O diagrama do fluxo de trabalho resume as etapas que você executará para configurar a replicação entre grades entre intervalos em duas grades. Estas etapas são descritas em mais detalhes abaixo.




### Configurar a replicação entre redes

Antes de usar a replicação entre grade, você deve fazer login nas contas de locatário correspondentes em cada grade e criar buckets idênticos. Em seguida, é possível habilitar a replicação entre grade em um ou em ambos os buckets.

#### Antes de começar

- Você revisou os requisitos para replicação entre grade. "O que é replicação entre grades"Consulte .
- Você está usando um "navegador da web suportado".
- A conta de locatário tem a permissão **usar conexão de federação de grade** e contas de locatário idênticas existem em ambas as grades. "Gerenciar os locatários permitidos para conexão de federação de grade"Consulte .
- O usuário de locatário que você fará login como já existe em ambas as grades e pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

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

#### Crie dois baldes idênticos

Como primeira etapa, faça login nas contas de locatário correspondentes em cada grade e crie buckets idênticos.

**Passos**

1. A partir de qualquer grade na conexão de federação de grade, crie um novo intervalo:
   a. Faça login na conta de locatário usando as credenciais de um usuário de locatário que existe em ambas as grades.

      Se você não conseguir entrar na grade de destino do locatário como um usuário local, confirme se o usuário raiz da conta de locatário definiu uma senha para sua conta de usuário.

   b. Siga as instruções "Crie um bucket do S3"para .
   c. Na guia **Manage Object settings** (Gerenciar configurações de objeto), selecione **Enable Object versioning** (Ativar controle de versão de objeto).
   d. Se o bloqueio de objeto S3 estiver ativado para o seu sistema StorageGRID, não ative o bloqueio de objeto S3 para o bucket.
   e. Selecione **criar bucket**.
   f. Selecione **Finish**.
2. Repita essas etapas para criar um intervalo idêntico para a mesma conta de locatário na outra grade na conexão de federação de grade.

   Conforme necessário, cada balde pode usar uma região diferente.

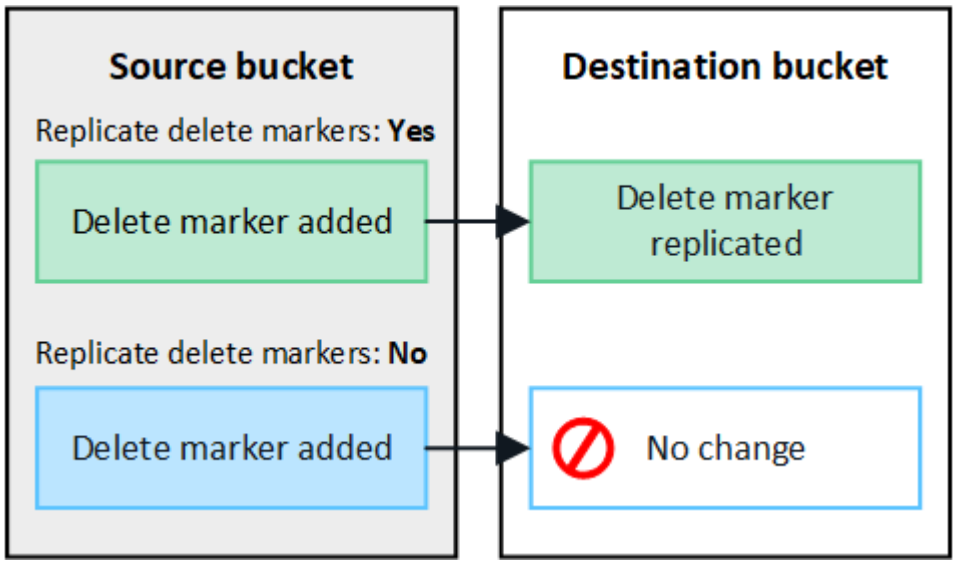
#### Ative a replicação entre redes

Você deve executar estas etapas antes de adicionar quaisquer objetos a qualquer bucket.

**Passos**

1. A partir de uma grade cujos objetos você deseja replicar, habilite "replicação entre grade em uma direção":
   a. Faça login na conta do locatário do bucket.
   b. Selecione **View 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 reveja a lista de requisitos.
   f. Se todos os requisitos tiverem sido atendidos, selecione a conexão de federação de grade que deseja usar.
   g. Opcionalmente, altere a configuração de **Replicate DELETE markers** para determinar o que acontece na grade de destino se um cliente S3 emitir uma solicitação de exclusão para a grade de origem que não inclui um ID de versão:

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




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

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

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

   Depois de alguns momentos, uma mensagem de sucesso aparece. Os objetos adicionados a esse bucket serão replicados automaticamente para a outra grade. **A replicação entre grades** é mostrada como um recurso habilitado na página de detalhes do bucket.

2. Opcionalmente, vá para o balde correspondente na outra grade e "ative a replicação entre grades em ambas as direções".

### Teste a replicação entre grades

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 controle de versão ainda está habilitado).

**Antes de começar**

- Você está usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

**Passos**

1. Faça login na conta do locatário do bucket.
2. Selecione **View 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 é exibida, que você e o administrador da grade podem usar para resolver o problema. Para obter detalhes, "Solucionar erros de federação de grade"consulte .

6. Se a replicação entre grades estiver configurada para ocorrer em ambas as direções, vá para o intervalo correspondente na outra grade e selecione **conexão de teste** para verificar se a replicação entre grades está funcionando na outra direção.

### Desative a replicação entre redes

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

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

- A desativação da replicação entre grades não remove nenhum objeto que já tenha sido copiado entre grades. Por exemplo, os objetos no `my-bucket` na Grade 1 que foram copiados `my-bucket` no Grid 2 não serão 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 grade foi ativada para cada um dos buckets (ou seja, se a replicação ocorrer em ambas as direções), você pode desativar a replicação entre grade para um ou ambos os buckets. Por exemplo, você pode querer desativar a replicação de objetos `my-bucket` de na Grade 1 para na Grade `my-bucket` 2, enquanto continua a replicar objetos `my-bucket` de na Grade 2 para na Grade `my-bucket` 1.
- Você deve desativar a replicação entre grade antes de remover a permissão de um locatário para usar a conexão de federação de grade. "Gerenciar locatários permitidos"Consulte .
- Se você desabilitar a replicação entre grade para um bucket que contém objetos, não será possível reativar a replicação entre grade a menos que você exclua todos os objetos dos buckets de origem e destino.

  Não é possível reativar a replicação a menos que ambos os buckets estejam vazios.

**Antes de começar**

- Você está usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

**Passos**

1. A partir da grade cujos objetos você não deseja mais replicar, pare a replicação entre grade para o bucket:
   a. Faça login na conta do locatário do bucket.
   b. Selecione **View 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 tiver certeza de que deseja desativar a replicação entre grades para esse intervalo, digite **Yes** na caixa de texto e selecione **Disable**.

      Depois de alguns momentos, uma mensagem de sucesso aparece. Novos objetos adicionados a esse bucket não podem mais ser replicados automaticamente para a outra grade. **A replicação entre grades** não é mais mostrada como um recurso habilitado na página Buckets.
2. Se a replicação entre grade foi configurada para ocorrer em ambas as direções, vá para o intervalo correspondente na outra grade e pare a replicação entre grade na outra direção.

## Exibir conexões de federação de grade

Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, você poderá visualizar as conexões permitidas.

**Antes de começar**

- A conta de locatário tem a permissão **Use Grid Federation Connection**.
- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

**Passos**

1. Selecione **STORAGE (S3)** > **conexões de federação de grade**.

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

| Coluna | Descrição |
|---|---|
| Nome da ligação | As conexões de federação de grade que este locatário tem permissão para usar. |
| Buckets com replicação entre grade | Para cada conexão de federação de grade, os buckets do locatário que têm replicação entre grade habilitada. Os objetos adicionados a esses buckets serão replicados para a outra grade na conexão. |
| Último erro | Para cada conexão de federação de grade, o erro mais recente ocorre, se houver, quando os dados estavam sendo replicados para a outra grade. Apague o último erroConsulte . |

2. Opcionalmente, selecione um nome de bucket para "veja os detalhes do balde".

### limpe o último erro

Um erro pode aparecer na coluna **último erro** por um destes motivos:

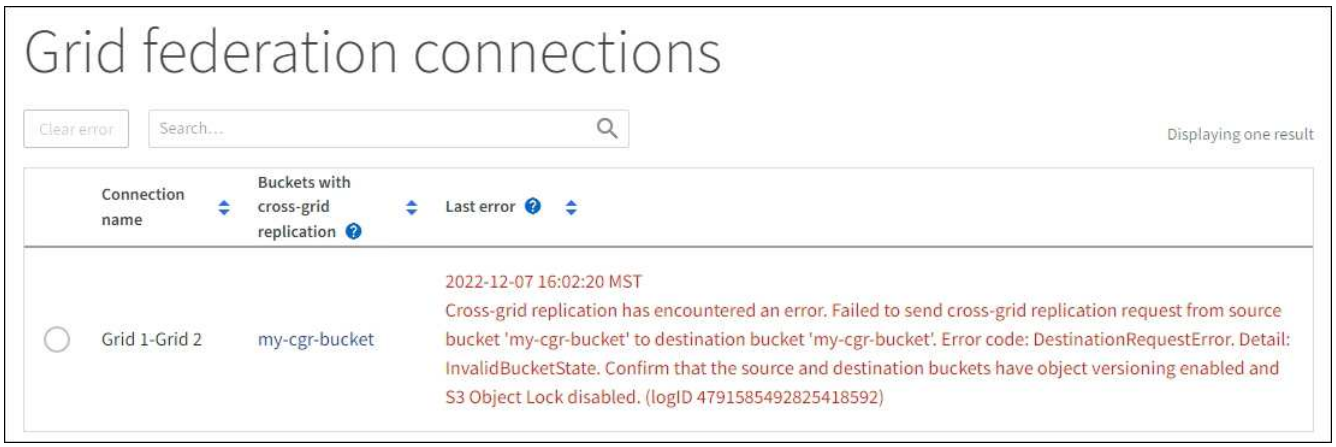
- A versão do objeto fonte não foi encontrada.
- O balde de origem não foi encontrado.
- O intervalo de destino foi eliminado.
- O intervalo de destino foi recriado por uma conta diferente.
- O bucket de destino tem controle de versão suspenso.
- O intervalo de destino foi recriado pela mesma conta, mas agora não foi versionado.

> Esta coluna mostra apenas o último erro de replicação entre grelha a ocorrer; os erros anteriores que possam ter ocorrido não serão apresentados.

**Passos**

1. Se uma mensagem for exibida na coluna **último erro**, exiba o texto da mensagem.

   Por exemplo, esse erro indica que o intervalo de destino para replicação entre grades estava em um estado inválido, possivelmente porque o controle de versão foi suspenso ou o bloqueio de objeto S3 foi ativado.




2. Execute quaisquer ações recomendadas. Por exemplo, se o controle de versão foi suspenso no bucket de destino para replicação entre grades, reative o controle de versão desse bucket.
3. Selecione a ligação na tabela.
4. Selecione **Clear error**.
5. Selecione **Sim** para limpar a mensagem e atualizar o estado do sistema.
6. Aguarde 5-6 minutos e, em seguida, insira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.

   > Para garantir que a mensagem de erro seja limpa, aguarde pelo menos 5 minutos após o carimbo de data/hora na mensagem antes de inserir um novo objeto.

7. Para determinar se algum objeto não pôde ser replicado devido ao erro de bucket, "Identificar e tentar novamente operações de replicação com falha"consulte .

# Gerenciar grupos e usuários

## Use a federação de identidade

O uso da federação de identidade torna a configuração de grupos de locatários e usuários mais rápida e permite que os usuários do locatário façam login na conta do locatário usando credenciais familiares.

### Configure a federação de identidade para o Gerenciador do Locatário

Você pode configurar a federação de identidade para o Gerenciador do locatário se quiser que grupos de locatários e usuários sejam gerenciados em outro sistema, como o ative Directory, o Azure ative Directory (Azure AD), o OpenLDAP ou o Oracle Directory Server.

#### Antes de começar

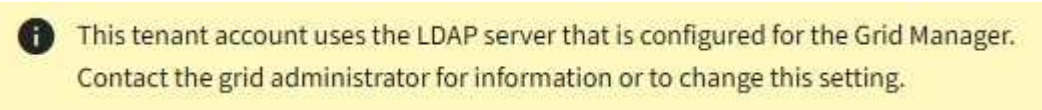
- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Você está usando o ative Directory, o Azure AD, o OpenLDAP ou o Oracle Directory Server como provedor de identidade.

  Se pretender utilizar um serviço LDAP v3 que não esteja listado, contacte o suporte técnico.

- Se você pretende usar o OpenLDAP, você deve configurar o servidor OpenLDAP. Diretrizes para configurar o servidor OpenLDAPConsulte .
- Se você pretende usar TLS (Transport Layer Security) para comunicações com o servidor LDAP, o provedor de identidade deve estar usando TLS 1,2 ou 1,3. "Cifras suportadas para conexões TLS de saída"Consulte .

#### Sobre esta tarefa

Se você pode configurar um serviço de federação de identidade para seu locatário depende de como sua conta de locatário foi configurada. Seu locatário pode compartilhar o serviço de federação de identidade configurado para o Gerenciador de Grade. Se você vir essa mensagem ao acessar a página Federação de identidade, não será possível configurar uma origem de identidade federada separada para esse locatário.

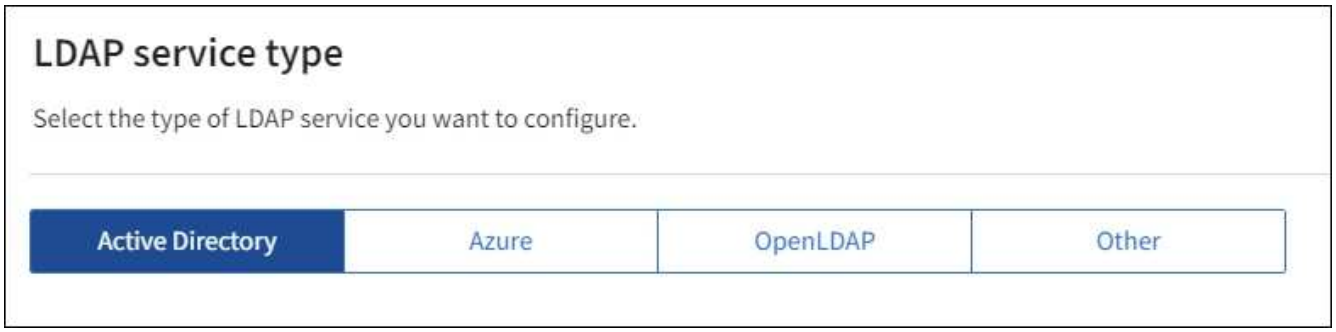



#### Introduza a configuração

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

#### Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **federação de identidade**.
2. Selecione **Ativar federação de identidade**.
3. Na secção tipo de serviço LDAP, selecione o tipo de serviço LDAP que pretende configurar.




Selecione **Other** para configurar valores para um servidor LDAP que use o Oracle Directory Server.

4. Se você selecionou **Other**, preencha os campos na seção atributos LDAP. Caso contrário, vá para a próxima etapa.
   - **Nome exclusivo do usuário**: O nome do atributo que contém o identificador exclusivo de um usuário LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `uid` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `uid`.
   - **UUID de usuário**: O nome do atributo que contém o identificador exclusivo permanente de um usuário LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.
   - **Group Unique Name**: O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `cn` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `cn`.
   - **Group UUID**: O nome do atributo que contém o identificador exclusivo permanente de um grupo LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.
5. Para todos os tipos de serviço LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias na secção Configurar servidor LDAP.
   - **Nome de host**: O nome de domínio totalmente qualificado (FQDN) ou endereço IP do servidor LDAP.
   - **Port**: A porta usada para se conetar 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 distinto (DN) para o usuário que se conetará ao servidor LDAP.

     No ative Directory, você também pode especificar o Nome de logon de nível inferior ou o Nome principal do usuário.

     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`
- **Ative Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, E `userPrincipalName`
- **Azure**: `accountEnabled` E. `userPrincipalName`

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

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

◦ **Group base DN**: O caminho completo do nome distinto (DN) para uma subárvore LDAP que você deseja pesquisar grupos. No exemplo do ative Directory (abaixo), todos os grupos cujo Nome distinto é relativo ao DN base (DC-StorageGRID,DC-com) podem ser usados como grupos federados.

> Os valores **Group unique name** devem ser exclusivos dentro do **Group base DN** a que pertencem.

◦ **DN da base do usuário**: O caminho completo do nome distinto (DN) de uma subárvore LDAP que você deseja pesquisar por usuários.

> Os valores **Nome exclusivo do usuário** devem ser exclusivos dentro do **DN da base de usuários** a que pertencem.

◦ **Bind username format** (opcional): O padrão de username padrão StorageGRID deve ser usado se o padrão não puder ser determinado automaticamente.

É recomendado fornecer **Bind username format** porque pode permitir que os usuários façam login se o StorageGRID não conseguir vincular-se à conta de serviço.

Introduza um destes padrões:

- **Padrão UserPrincipalName (ative Directory e Azure)**: `[USERNAME]@*example*.com`
- * Padrão de nome de logon de nível inferior (ative Directory e Azure)*: `*example*\[USERNAME]`
- * Padrão de nome distinto *: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

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

6. Na seção Transport Layer Security (TLS), selecione uma configuração de segurança.
◦ **Use STARTTLS**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada para ative Directory, OpenLDAP ou outro, mas esta opção não é suportada para o Azure.
◦ **Use LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar essa opção para o Azure.
◦ **Não use TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido. Esta opção não é suportada para o Azure.

> O uso da opção **não usar TLS** não é suportado se o servidor do ative Directory forçar a assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

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

     Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

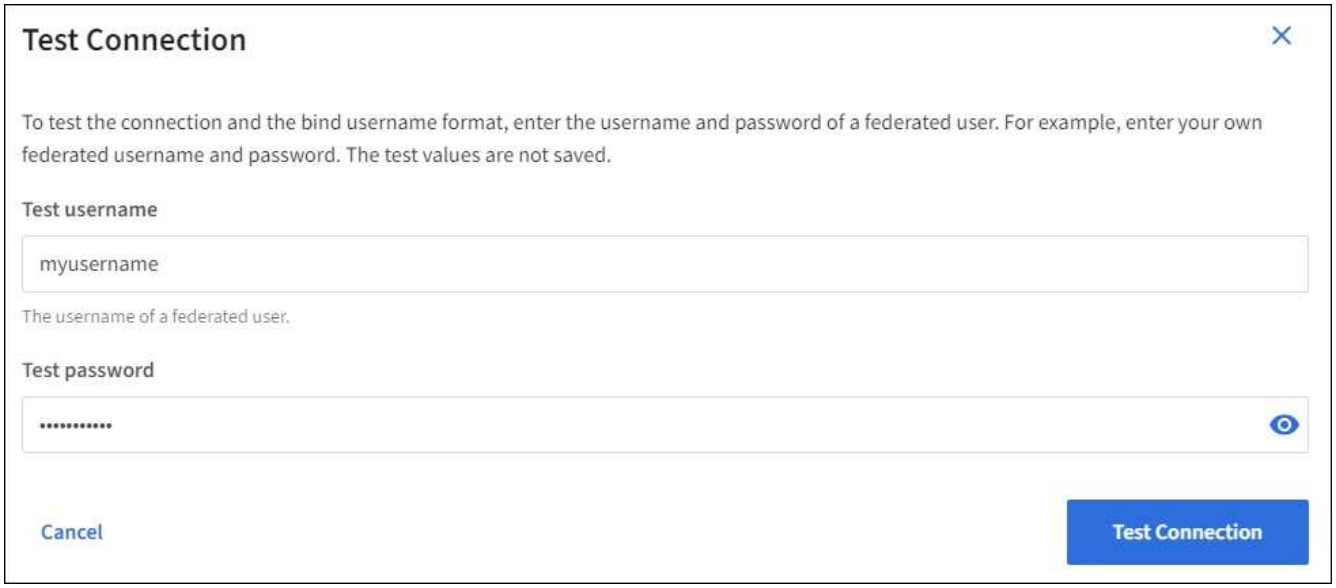
#### Teste a conexão e salve a configuração

Depois de introduzir todos os valores, tem de testar a ligação antes de poder guardar a configuração. O StorageGRID verifica as configurações de conexão para o servidor LDAP e o formato de nome de usuário de vinculação, se você tiver fornecido uma.

**Passos**

1. Selecione **Test Connection**.
2. Se você não forneceu um formato de nome de usuário do BIND:
   - É apresentada uma mensagem "Test Connection successful" (testar ligação bem-sucedida) se as definições de ligação forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - É apresentada uma mensagem "não foi possível estabelecer ligação de teste" se as definições da ligação forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.
3. Se você tiver fornecido um formato de nome de usuário do BIND, 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 carateres especiais no nome de usuário, como em ou /.




   - É apresentada uma mensagem "Test Connection successful" (testar ligação bem-sucedida) se as definições de ligação forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - Uma mensagem de erro é exibida se as configurações de conexão, o formato de nome de usuário de ligação ou o nome de usuário de teste e a senha forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

### Forçar a sincronização com a fonte de identidade

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

**Passos**

1. Vá para a página de federação de identidade.
2. Selecione **servidor de sincronização** na parte superior da página.

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

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

### Desativar a federação de identidade

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

**Sobre esta tarefa**

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

- Os utilizadores federados não poderão iniciar sessão.
- Os usuários federados que estiverem conetados no momento manterão o acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.
- A sincronização entre o sistema StorageGRID e a origem da identidade não ocorrerá e os alertas ou alarmes não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Ativar federação de identidade** será desativada se o logon único (SSO) estiver definido como **ativado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade. "Desative o logon único"Consulte .

**Passos**

1. Vá para a página de federação de identidade.
2. Desmarque a caixa de seleção **Ativar federação de identidade**.

### Diretrizes para configurar o servidor OpenLDAP

Se você quiser usar um servidor OpenLDAP para federação de identidade, você deve configurar configurações específicas no servidor OpenLDAP.

Para fontes de identidade que não são ActiveDirectory ou Azure, o StorageGRID não bloqueará automaticamente o acesso S3 aos usuários que estão desativados externamente. Para bloquear o acesso S3, exclua quaisquer chaves S3 para o usuário ou remova o usuário de todos os grupos.

#### Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as instruções para a manutenção da associação de grupo reverso no "Documentação do OpenLDAP: Guia do administrador da versão 2,4".

#### Indexação

Você deve configurar os seguintes atributos 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 do Nome de usuário sejam indexados para um desempenho ideal.

Consulte as informações sobre a manutenção da associação de grupo reverso no "Documentação do OpenLDAP: Guia do administrador da versão 2,4".

## Gerenciar grupos de locatários

### Crie grupos para um locatário do S3

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

#### Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Se você pretende importar um grupo federado, o "federação de identidade configurada", e o grupo federado já existe na origem de identidade configurada.
- Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, você revisou o fluxo de trabalho e as considerações para "clonar grupos de locatários e usuários", e você estará conetado à grade de origem do locatário.

#### Acesse o assistente criar grupo

Como primeira etapa, acesse o assistente criar grupo.

#### Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Se sua conta de locatário tiver a permissão **Use Grid Federation Connection**, confirme se um banner azul aparece, indicando que novos grupos criados nessa grade serão clonados para o mesmo locatário na outra grade na conexão. Se este banner não aparecer, você pode estar conetado à grade 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 **local group** para criar um grupo local ou selecione a guia **Federated group** para importar um grupo da origem de identidade configurada anteriormente.

   Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, os usuários pertencentes a grupos locais não poderão fazer login no Gerenciador de locatários, embora possam usar aplicativos clientes para gerenciar os recursos do locatário, com base nas permissões de grupo.

2. Introduza o nome do grupo.
   - **Local group**: Insira um nome de exibição e um nome exclusivo. Pode editar o nome de apresentação mais tarde.

     Se sua conta de locatário tiver a permissão **Use Grid Federation Connection**, ocorrerá um erro de clonagem se o mesmo **nome exclusivo** já existir para o locatário na grade de destino.

   - **Federated group**: Insira o nome exclusivo. Para o ative 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 **continuar**.

#### 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-escrita** (padrão): Os usuários podem fazer login no Gerenciador do locatário e gerenciar a configuração do locatário.

- **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar nenhuma operação no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. Os usuários locais só de leitura podem alterar suas próprias senhas.

> Se um usuário pertencer a vários grupos e qualquer grupo 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.

   "Permissões de gerenciamento do locatário"Consulte .

3. Selecione **continuar**.

#### Defina a política de grupo S3

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

**Passos**

1. Selecione a política que pretende utilizar para este grupo.

| Política de grupo | Descrição |
|---|---|
| Sem acesso S3 | Padrão. Os usuários deste grupo não têm acesso a recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar essa opção, somente o usuário root terá acesso aos recursos do S3 por padrão. |
| Acesso somente leitura | Os usuários deste grupo têm acesso somente leitura a recursos do S3. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo somente leitura aparece na caixa de texto. Não é possível editar esta cadeia de carateres. |
| Acesso total | Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo de acesso total aparece na caixa de texto. Não é possível editar esta cadeia de carateres. |
| Mitigação de ransomware | Esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários deste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que têm o controle de versão de objeto habilitado.<br><br>Os usuários do Gerenciador de locatários que têm a permissão **Gerenciar todos os buckets** podem substituir essa política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação multifator (MFA), onde disponível. |

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

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

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

3. Se estiver criando um grupo local, selecione **continuar**. Se você estiver criando um grupo federado, selecione **criar grupo** e **concluir**.

#### Adicionar utilizadores (apenas grupos locais)

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

> Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, os usuários selecionados ao criar um grupo local na grade de origem não serão incluídos quando o grupo for clonado para a grade de destino. Por esse motivo, não selecione usuários quando você criar o grupo. Em vez disso, selecione o grupo quando você criar os usuários.

**Passos**

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

   O grupo criado aparece na lista de grupos.

   Se sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver na grade de origem do locatário, o novo grupo será clonado para a grade de destino do locatário. **Success** aparece como **status de clonagem** na seção Visão geral da página de detalhes do grupo.

### Crie grupos para um locatário Swift

Você pode gerenciar permissões de acesso para uma conta de locatário Swift importando grupos federados ou criando grupos locais. Pelo menos um grupo deve ter a permissão Swift Administrator, que é necessária para gerenciar os contentores e objetos para uma conta Swift.

> O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Se você pretende importar um grupo federado, o "federação de identidade configurada", e o grupo federado já existe na origem de identidade configurada.

#### Acesse o assistente criar grupo

**Passos**

Como primeira etapa, acesse o assistente criar grupo.

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Selecione **criar grupo**.

#### Escolha um tipo de grupo

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

**Passos**

1. Selecione a guia **local group** para criar um grupo local ou selecione a guia **Federated group** para importar um grupo da origem de identidade configurada anteriormente.

   Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, os usuários pertencentes a grupos locais não poderão fazer login no Gerenciador de locatários, embora possam usar aplicativos clientes para gerenciar os recursos do locatário, com base nas permissões de grupo.

2. Introduza o nome do grupo.
   - **Local group**: Insira um nome de exibição e um nome exclusivo. Pode editar o nome de apresentação mais tarde.
   - **Federated group**: Insira o nome exclusivo. Para o ative 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 **continuar**.

#### 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-escrita** (padrão): Os usuários podem fazer login no Gerenciador do locatário e gerenciar a configuração do locatário.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar nenhuma operação no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. Os usuários locais só de leitura podem alterar suas próprias senhas.

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

2. Marque a caixa de seleção **Root Access** se os usuários do grupo precisarem fazer login na API de Gerenciamento de Locatário ou Gerenciamento de Locatário.
3. Selecione **continuar**.

#### Defina a política de grupo Swift

Os usuários Swift precisam de permissão de administrador para se autenticar na API REST do Swift para criar contentores e ingerir objetos.

1. Marque a caixa de seleção **Swift administrator** se os usuários do grupo precisarem usar a Swift REST API para gerenciar contentores e objetos.
2. Se estiver criando um grupo local, selecione **continuar**. Se você estiver criando um grupo federado, selecione **criar grupo** e **concluir**.

#### Adicionar utilizadores (apenas grupos locais)

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

**Passos**

1. Opcionalmente, selecione um ou mais usuários locais para este grupo.

   Se ainda não tiver criado utilizadores locais, pode adicionar este grupo ao utilizador na página utilizadores. "Gerenciar usuários locais"Consulte .

2. Selecione **criar grupo** e **concluir**.

   O grupo criado aparece na lista de grupos.

### Permissões de gerenciamento do locatário

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

Para fazer login no Gerenciador do Locatário ou usar a API de Gerenciamento do Locatário, os usuários devem pertencer a um grupo que tenha pelo menos uma permissão. Todos os usuários que podem entrar podem executar as seguintes tarefas:

- Visualizar o painel de instrumentos
- Alterar sua própria senha (para usuários locais)

Para todas as permissões, a configuração do modo de acesso do grupo determina se os usuários podem alterar configurações e executar operações ou se eles podem exibir somente as configurações e recursos relacionados.

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

Pode atribuir as seguintes permissões a um grupo. Observe que S3 locatários e locatários Swift têm permissões de grupo diferentes.

| Permissão | Descrição | Detalhes |
| --- | --- | --- |
| Acesso à raiz | Fornece acesso total ao Gerenciador do Locatário e à API de Gerenciamento do Locatário. | Os usuários Swift devem ter permissão de acesso root para entrar na conta do locatário. |
| Administrador | Apenas inquilinos Swift. Fornece acesso total aos contentores e objetos Swift para essa conta de locatário | Os usuários Swift devem ter a permissão Swift Administrator para executar qualquer operação com a SWIFT REST API. |
| Gerencie suas próprias credenciais S3 | Permite que os usuários criem e removam suas próprias chaves de acesso S3. | Os utilizadores que não têm esta permissão não veem a opção de menu **STORAGE (S3)** > **My S3 Access Keys**. |
| Veja todos os baldes | **S3 locatários**: Permite que os usuários visualizem todos os buckets e configurações de bucket.<br><br>**Swift tenants**: Permite que os usuários do Swift visualizem todos os contentores e configurações de contentores usando a API de Gerenciamento do locatário. | Os usuários que não têm a permissão Exibir todos os buckets ou Gerenciar todos os buckets não veem a opção de menu **Buckets**.<br><br>Essa permissão é substituída pela permissão Gerenciar todos os buckets. Não afeta as políticas de grupo ou bucket S3 usadas por clientes S3 ou console S3.<br><br>Você só pode atribuir essa permissão aos grupos Swift a partir da API de Gerenciamento de Tenant. Não é possível atribuir essa permissão a grupos Swift usando o Gerenciador de Locações. |
| Gerenciar todos os buckets | **S3 inquilinos**: Permite que os usuários usem o Gerenciador do locatário e a API de gerenciamento do locatário para criar e excluir buckets do S3 e gerenciar as configurações de todos os buckets do S3 na conta do locatário, independentemente das políticas de bucket ou grupo do S3.<br><br>**Swift tenants**: Permite que usuários Swift controlem a consistência para contentores Swift usando a API de Gerenciamento de inquilinos. | Os usuários que não têm a permissão Exibir todos os buckets ou Gerenciar todos os buckets não veem a opção de menu **Buckets**.<br><br>Esta permissão substitui a permissão Exibir todos os buckets. Não afeta as políticas de grupo ou bucket S3 usadas por clientes S3 ou console S3.<br><br>Você só pode atribuir essa permissão aos grupos Swift a partir da API de Gerenciamento de Tenant. Não é possível atribuir essa permissão a grupos Swift usando o Gerenciador de Locações. |

| Permissão | Descrição | Detalhes |
| --- | --- | --- |
| Gerenciar endpoints | Permite que os usuários usem o Gerenciador do Locatário ou a API de Gerenciamento do Locatário para criar ou editar endpoints de serviço da plataforma, que são usados como o destino dos serviços da plataforma StorageGRID. | Os usuários que não têm essa permissão não veem a opção de menu **endpoints de serviços da plataforma**. |
| Use a guia Console do S3 | Quando combinada com a permissão Exibir todos os buckets ou Gerenciar todos os buckets, permite que os usuários visualizem e gerenciem objetos na guia Console do S3 na página de detalhes de um bucket. | |

### Gerenciar grupos

Gerencie seus grupos de locatários conforme necessário para exibir, editar ou duplicar um grupo e muito mais.

#### Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

##### Ver ou editar grupo

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

#### Passos

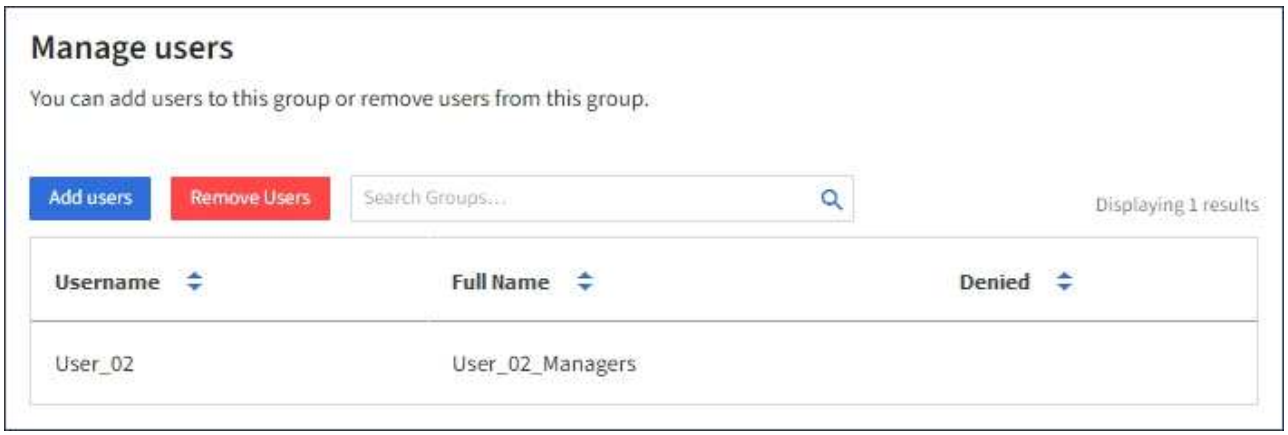
1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Revise as informações fornecidas na página grupos, que lista informações básicas para todos os grupos locais e federados dessa conta de locatário.

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

   - Uma mensagem de banner indica que, se você editar ou remover um grupo, suas alterações não serão sincronizadas com a outra grade.
   - Conforme necessário, uma mensagem de banner indica se os grupos não foram clonados ao locatário na grade de destino. Você pode tente novamente um clone de grupo que falhou.
3. Se quiser alterar o nome do grupo:
   a. Selecione a caixa de verificação para o grupo.
   b. Selecione **ações** > **Editar nome do grupo**.
   c. Introduza o novo nome.
   d. Selecione **Salvar alterações.**
4. Se você quiser ver mais detalhes ou fazer edições adicionais, faça um dos seguintes procedimentos:
   - Selecione o nome do grupo.

- Marque a caixa de seleção para o grupo e selecione **ações** > **Exibir detalhes do grupo**.

5. Revise a seção Visão geral, que mostra as seguintes informações para cada grupo:
   - Nome do visor
   - Nome único
   - Tipo
   - Modo de acesso
   - Permissões
   - S3 Política
   - Número de usuários neste grupo
   - Campos adicionais se a conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver visualizando o grupo na grade de origem do locatário:
     - Status da clonagem, **sucesso** ou **falha**
     - Um banner azul indicando que, se você editar ou excluir esse grupo, suas alterações não serão sincronizadas com a outra grade.
6. Edite as definições do grupo conforme necessário. "Crie grupos para um locatário do S3"Consulte e "Crie grupos para um locatário Swift" para obter detalhes sobre o que introduzir.
   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 quaisquer alterações e selecione **Salvar alterações**.
      - Se você estiver editando um grupo S3, opcionalmente, selecione uma política de grupo S3 diferente ou insira a string JSON para uma política personalizada, conforme necessário.
      - Se você estiver editando um grupo Swift, opcionalmente selecione ou desmarque a caixa de seleção **Administrador Swift**.
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 deseja remover e selecione **Remover usuários**.

   Uma mensagem de sucesso aparece no canto superior direito.

9. Confirme se selecionou **Guardar alterações** para cada secção alterada.

#### Grupo duplicado

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

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

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Marque a caixa de seleção do grupo que deseja duplicar.
3. Selecione **ações** > **grupo duplicado**.
4. "Crie grupos para um locatário do S3"Consulte ou "Crie grupos para um locatário Swift" para obter detalhes sobre o que introduzir.
5. Selecione **criar grupo**.

#### Repetir o clone do grupo

Para tentar novamente um clone que falhou:

1. Selecione cada grupo que indica *(Falha na clonagem)* abaixo do nome do grupo.
2. Selecione **ações** > **Clone groups**.
3. Veja o status da operação de clone na página de detalhes de cada grupo que você está clonando.

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

#### Exclua um ou mais grupos

Pode eliminar um ou mais grupos. Quaisquer usuários que pertençam apenas a um grupo que seja excluído não poderão mais entrar no Gerenciador do locatário ou usar a conta do locatário.

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

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
2. Selecione a caixa de verificação para cada grupo que pretende eliminar.
3. Selecione **ações** > **Excluir grupo** ou **ações** > **Excluir grupos**.

   É apresentada uma caixa de diálogo de confirmação.

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

## Gerenciar usuários locais

Você pode criar usuários locais e atribuí-los a grupos locais para determinar quais recursos esses usuários podem acessar. O Gerenciador do Tenant inclui um usuário local predefinido, chamado "root". Embora você possa adicionar e remover usuários locais, você não pode remover o usuário raiz.

> Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, os usuários locais não poderão fazer login no Gerenciador do Locatário ou na API de Gerenciamento do Locatário, embora possam usar aplicativos cliente para acessar os recursos do locatário, com base nas permissões de grupo.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".
- Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, você revisou o fluxo de trabalho e as considerações para "clonar grupos de locatários e usuários", e você estará conetado à grade de origem do locatário.

### Crie um usuário local

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

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

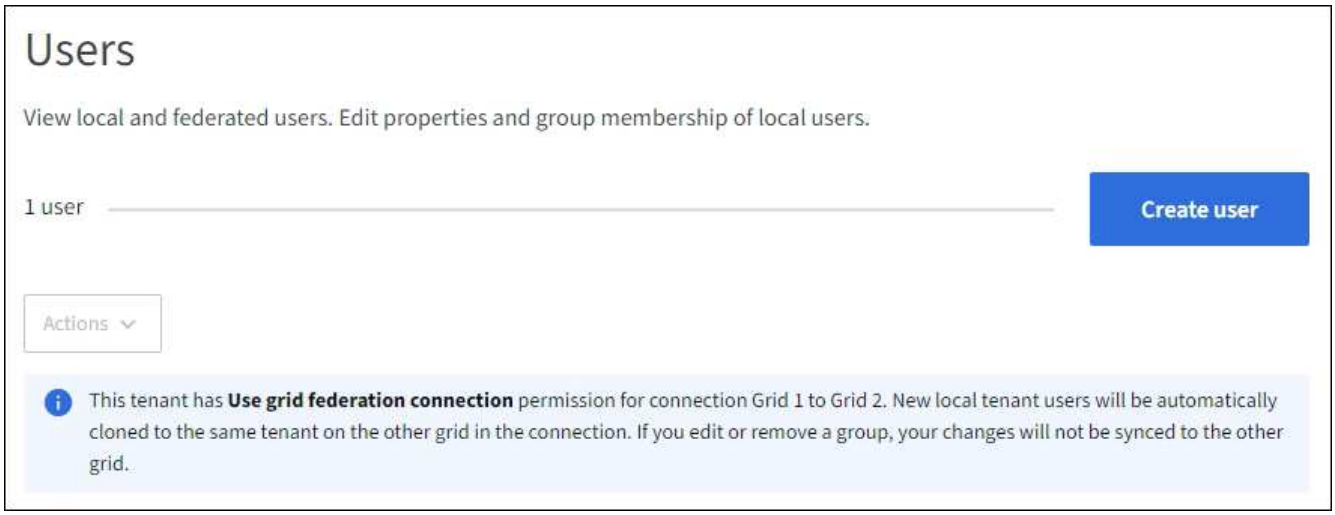
Os usuários Swift que não pertencem a nenhum grupo não têm permissões de gerenciamento ou acesso ao contentor Swift.

#### Acesse o assistente criar usuário

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.

   Se sua conta de locatário tiver a permissão **usar conexão de federação de grade**, um banner azul indica que essa é a grade de origem do locatário. Todos os usuários locais que você criar nesta grade serão clonados para a outra grade na conexão.




2. Selecione **criar usuário**.

#### Introduza as credenciais

**Passos**

1. Para a etapa **Insira as credenciais do usuário**, preencha os campos a seguir.

| 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 utilizador | O nome que este usuário usará para entrar. Os nomes de usuário devem ser exclusivos e não podem ser alterados.<br><br>**Nota**: Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, ocorrerá um erro de clonagem se o mesmo **Username** já existir para o locatário na grade de destino. |
| Senha e confirmar senha | A senha que o usuário usará inicialmente ao fazer login. |
| Negar acesso | Selecione **Sim** para impedir que esse usuário faça login na conta de locatário, mesmo que ele ainda possa pertencer a um ou mais grupos.<br><br>Por exemplo, selecione **Sim** para suspender temporariamente a capacidade de um usuário fazer login. |

2. Selecione **continuar**.

#### Atribuir a grupos

**Passos**

1. Atribua o usuário a um ou mais grupos locais para determinar quais tarefas podem ser executadas.

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

Os usuários que não pertencem a nenhum grupo não terão permissões de gerenciamento. As permissões são cumulativas. Os usuários terão todas as permissões para todos os grupos aos quais pertencem. "Permissões de gerenciamento do locatário"Consulte .

2. Selecione **criar usuário**.

   Se sua conta de locatário tiver a permissão **Use Grid Federation Connection** e você estiver na grade de origem do locatário, o novo usuário local será clonado para a grade de destino do locatário. **Success** aparece como **status de clonagem** na seção Visão geral da página de detalhes do usuário.

3. Selecione **Finish** para retornar à página usuários.

### Ver ou editar utilizador local

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Revise as informações fornecidas na página usuários, que lista informações básicas para todos os usuários locais e federados dessa conta de locatário.

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

   - Uma mensagem de banner indica que, se você editar ou remover um usuário, suas alterações não serão sincronizadas com a outra grade.
   - Conforme necessário, uma mensagem de banner indica se os usuários não foram clonados para o locatário na grade de destino. Você pode tente novamente um clone de usuário que falhou.
3. Se pretender alterar o nome completo do utilizador:
   a. Selecione a caixa de verificação para o utilizador.
   b. Selecione **ações** > **Editar nome completo**.
   c. Introduza o novo nome.
   d. Selecione **Salvar alterações.**
4. Se você quiser ver mais detalhes ou fazer edições adicionais, faça um dos seguintes procedimentos:
   - Selecione o nome de utilizador.
   - Marque a caixa de seleção para o usuário e selecione **ações** > **Exibir detalhes do usuário**.
5. Revise a seção Visão geral, que mostra as seguintes informações para cada usuário:
   - Nome completo
   - Nome de utilizador
   - Tipo de utilizador
   - Acesso negado
   - Modo de acesso
   - Associação ao grupo
   - Campos adicionais se a conta de locatário tiver a permissão **usar conexão de federação de grade** e você estiver visualizando o usuário na grade de origem do locatário:
     - Status da clonagem, **sucesso** ou **falha**
     - Um banner azul indicando que, se você editar este usuário, suas alterações não serão

sincronizadas com a outra grade.

6. Edite as definições do utilizador conforme necessário. Consulte Criar utilizador local para obter detalhes sobre o que introduzir.
   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 guia **Senha**, altere a senha do usuário e selecione **Salvar alterações**.
   c. Na guia **Access**, 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 **teclas de acesso**, selecione **criar chave** e siga as instruções para "Criando as chaves de acesso S3 de outro usuário".
   e. Na guia **grupos**, selecione **Editar grupos** para adicionar o usuário aos grupos ou remover o usuário dos grupos. Em seguida, selecione **Salvar alterações**.
7. Confirme se selecionou **Guardar alterações** para cada secção alterada.

### Duplicar utilizador local

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

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

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Selecione a caixa de verificação para o utilizador que pretende duplicar.
3. Selecione **ações** > **usuário duplicado**.
4. Consulte Criar utilizador local para obter detalhes sobre o que introduzir.
5. Selecione **criar usuário**.

### Repetir o clone do usuário

Para tentar novamente um clone que falhou:

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

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

### Exclua 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 sua conta de locatário tiver a permissão **usar conexão de federação de grade** e você excluir um usuário local, o StorageGRID não excluirá o usuário correspondente na outra grade. Se você precisar manter essas informações em sincronia, você deve excluir o mesmo usuário de ambas as grades.

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

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO** > **usuários**.
2. Selecione a caixa de verificação para cada utilizador que pretende eliminar.
3. Selecione **ações** > **Excluir usuário** ou **ações** > **Excluir usuários**.

   É apresentada uma caixa de diálogo de confirmação.

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

# Gerenciar S3 chaves de acesso

## Gerenciar chaves de acesso S3: Visão geral

Cada usuário de uma conta de locatário do S3 deve ter 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:

- Os usuários que têm a permissão **Gerenciar suas próprias credenciais S3** podem criar ou remover suas próprias chaves de acesso S3.
- Os usuários que têm a permissão **Root Access** podem gerenciar as chaves de acesso para a conta raiz do S3 e todos os outros usuários. As chaves de acesso root fornecem acesso total a todos os buckets e objetos para o locatário, a menos que explicitamente desabilitado por uma política de bucket.

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

## Crie suas próprias chaves de acesso S3

Se você estiver usando um locatário do S3 e tiver a permissão apropriada, você poderá criar suas próprias chaves de acesso do S3. Você precisa ter uma chave de acesso para acessar seus buckets e objetos.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie suas próprias credenciais 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 locatário. Depois de criar uma nova chave de acesso, atualize a aplicação com a sua nova ID de chave de

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

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

- Defina um tempo de expiração para que suas chaves limitem seu acesso a um determinado período de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco se o ID da chave de acesso e a chave de acesso secreta forem acidentalmente expostos. As chaves expiradas são removidas automaticamente.
- Se o risco de segurança em seu ambiente for baixo e você não precisar criar periodicamente novas chaves, você não precisa definir um tempo de expiração para suas chaves. Se você decidir mais tarde criar novas chaves, 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 a sua conta no Gerenciador do Locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

**Passos**

1. Selecione **ARMAZENAMENTO (S3)** > **as minhas chaves de acesso**.

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

2. Selecione **criar chave**.
3. Execute um dos seguintes procedimentos:
   - Selecione **não defina um tempo de expiração** para criar uma chave que não expirará. (Predefinição)
   - Selecione **defina um tempo de expiração** e defina a data e a hora de expiração.

     > A data de validade pode ser um máximo de cinco anos a partir da data atual. O tempo de expiração pode ser um mínimo de um minuto a partir do tempo atual.

4. Selecione **criar chave de acesso**.

   A caixa de diálogo Download Access Key (Transferir chave de acesso) é exibida, listando o ID da 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 **Transferir .csv** para guardar um ficheiro de folha de cálculo que contenha a ID da chave de acesso e a chave de acesso secreta.

   > Não feche esta caixa de diálogo até que você tenha copiado ou baixado essas informações. Não é possível copiar ou transferir chaves depois de a caixa de diálogo ter sido fechada.

6. Selecione **Finish**.

   A nova chave está listada na página Minhas chaves de acesso.

7. Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, opcionalmente use a API de Gerenciamento do locatário para clonar manualmente as chaves de acesso S3 do locatário na grade

de origem para o locatário na grade de destino. "Clonar chaves de acesso S3 usando a API"Consulte .

## Veja as suas teclas de acesso S3

Se você estiver usando um locatário do S3 e tiver o "permissão apropriada", você poderá exibir uma lista das chaves de acesso do S3. Você pode classificar a lista por tempo de expiração, para que você possa determinar quais chaves expirarão em breve. Conforme necessário, você pode "crie novas chaves" ou "eliminar chaves"não está 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 a sua conta no Gerenciador do Locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire 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 conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem as credenciais Gerenciar suas próprias credenciais S3 "permissão".

**Passos**

1. Selecione **ARMAZENAMENTO (S3)** > **as minhas chaves de acesso**.
2. Na página Minhas chaves de acesso, classifique todas as chaves de acesso existentes por **tempo 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, você pode começar a usar as novas chaves sem perder temporariamente o acesso aos objetos na conta.

   As chaves expiradas são removidas automaticamente.

## Elimine as suas próprias chaves de acesso S3

Se você estiver usando um locatário do S3 e tiver a permissão apropriada, você poderá excluir suas próprias chaves de acesso do S3. Depois que uma chave de acesso for excluída, ela não poderá mais ser usada para acessar os objetos e buckets na conta do locatário.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você tem o "Gerencie sua própria permissão de credenciais 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 a sua conta no Gerenciador do Locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

**Passos**

1. Selecione **ARMAZENAMENTO (S3)** > **as minhas chaves de acesso**.
2. Na página Minhas chaves de acesso, marque a caixa de seleção para cada chave de acesso que deseja remover.
3. Selecione **Delete key**.
4. Na caixa de diálogo de confirmação, selecione **Delete key**.

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

## Crie as chaves de acesso S3 de outro usuário

Se você estiver usando um locatário do S3 e tiver a permissão apropriada, poderá criar chaves de acesso do S3 para outros usuários, como aplicativos que precisam de acesso a buckets e objetos.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz".

**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 sua conta de locatário. Depois de criar uma nova chave de acesso, atualize a aplicação com a nova ID da chave de acesso e chave de acesso secreta. Para 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 chave antes que a antiga expire e, em seguida, exclua a antiga.

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

- Defina um tempo de expiração para as teclas para limitar o acesso do usuário a um determinado período de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco se o ID da chave de acesso e a chave de acesso secreta forem acidentalmente expostos. As chaves expiradas são removidas automaticamente.
- Se o risco de segurança em seu ambiente for baixo e você não precisar criar periodicamente novas chaves, você não precisa definir um tempo de expiração para as chaves. Se você decidir mais tarde criar novas chaves, 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 Gerenciador do locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire 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 S3 você deseja gerenciar.

   É apresentada a página de detalhes do utilizador.

3. Selecione **teclas de acesso** e, em seguida, selecione **criar chave**.
4. Execute um dos seguintes procedimentos:
   - Selecione **não defina um tempo de expiração** para criar uma chave que não expire. (Predefinição)
   - Selecione **defina um tempo de expiração** e defina a data e a hora de expiração.

   > A data de validade pode ser um máximo de cinco anos a partir da data atual. O tempo de expiração pode ser um mínimo de um minuto a partir do tempo atual.

5. Selecione **criar chave de acesso**.

   A caixa de diálogo Download Access Key (Transferir 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 **Transferir .csv** para guardar um ficheiro de folha de cálculo que contenha a ID da chave de acesso e a chave de acesso secreta.

   > Não feche esta caixa de diálogo até que você tenha copiado ou baixado essas informações. Não é possível copiar ou transferir chaves depois de a caixa de diálogo ter sido fechada.

7. Selecione **Finish**.

   A nova chave está listada na guia teclas de acesso da página de detalhes do usuário.

8. Se a sua conta de locatário tiver a permissão **Use Grid Federation Connection**, opcionalmente use a API de Gerenciamento do locatário para clonar manualmente as chaves de acesso S3 do locatário na grade de origem para o locatário na grade de destino. "Clonar chaves de acesso S3 usando a API"Consulte .

## Veja as S3 chaves de acesso de outro usuário

Se você estiver usando um locatário do S3 e tiver permissões apropriadas, poderá 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. Conforme necessário, você pode criar novas chaves e excluir chaves que não estão mais em uso.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

> 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 Gerenciador do locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire 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 teclas de acesso S3 você deseja exibir.
3. Na página Detalhes do usuário, selecione **teclas 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 pode começar a usar as novas chaves sem perder temporariamente o acesso aos objetos na conta.

   As chaves expiradas são removidas automaticamente.

**Informações relacionadas**

"Crie as chaves de acesso S3 de outro usuário"

"Eliminar as S3 chaves de acesso de outro utilizador"

## Exclua as S3 chaves de acesso de outro usuário

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

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

> 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 Gerenciador do locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire 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 S3 você deseja gerenciar.
3. Na página Detalhes do usuário, selecione **teclas de acesso** e, em seguida, marque a caixa de seleção para cada chave de acesso que deseja excluir.
4. Selecione **ações** > **Excluir tecla 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 do S3

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

### Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o acesso raiz ou Gerenciar todos os buckets "permissão". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

> As permissões para definir ou modificar as propriedades de bloqueio de objetos S3D de buckets ou objetos podem ser concedidas pelo "política de bucket ou política de grupo".

- Se você planeja habilitar o bloqueio de objeto S3 para um bucket, um administrador de grade ativou a configuração global de bloqueio de objeto S3 para o sistema StorageGRID e revisou os requisitos para buckets e objetos do bloqueio de objeto S3. "Use o bloqueio de objetos S3D para reter objetos"Consulte .

### Acesse o assistente

#### Passos

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

### Introduza os detalhes

#### Passos

1. Introduza os detalhes do balde.

| Campo | Descrição |
|---|---|
| Nome do intervalo | Um nome para o bucket que está em conformidade com estas regras:<br>• Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário).<br>• Deve ser compatível com DNS.<br>• Deve conter pelo menos 3 e não mais de 63 carateres.<br>• 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 usar períodos em solicitações de estilo hospedadas virtuais. Os períodos causarão problemas com a verificação do certificado curinga do servidor.<br>Para obter mais informações, consulte "Documentação da Amazon Web Services (AWS) sobre regras de nomenclatura de bucket" .<br>**Nota**: Não é possível alterar o nome do bucket depois de criar o bucket. |
| Região | A região do balde.<br>O administrador do StorageGRID gerencia as regiões disponíveis. A região de um bucket pode afetar a política de proteção de dados aplicada a objetos. Por padrão, todos os buckets são criados na `us-east-1` região.<br>**Nota**: Não é possível alterar a região depois de criar o intervalo. |

2. Selecione **continuar**.

### Gerenciar configurações de objeto

**Passos**

1. Opcionalmente, habilite o controle de versão de objetos para o bucket.

   Ative o controle de versão de objetos se você quiser armazenar todas as versões de cada objeto neste intervalo. Em seguida, você pode recuperar versões anteriores de um objeto, conforme necessário. Você deve habilitar o controle de versão de objetos se o bucket for usado para replicação entre grades.

2. Se a configuração global S3 Object Lock estiver ativada, ative opcionalmente o S3 Object Lock para o bucket armazenar objetos usando um modelo WORM (write-once-read-many).

   Ative o bloqueio de objetos S3D para um bucket somente se você precisar manter objetos por um período de tempo fixo, por exemplo, para atender a certos requisitos regulatórios. S3 Object Lock é uma configuração permanente que ajuda a evitar que objetos sejam excluídos ou substituídos por um período fixo de tempo ou indefinidamente.

   > Depois que a configuração S3 Object Lock estiver ativada para um bucket, ele não poderá ser desativado. Qualquer pessoa com as permissões corretas pode adicionar objetos a esse intervalo que não podem ser alterados. Você pode não ser capaz de excluir esses objetos ou o próprio bucket.

   Se você ativar o bloqueio de objeto S3 para um bucket, o controle de versão do bucket será ativado automaticamente.

3. Se você selecionou **Enable Object Lock** (Ativar bloqueio de objetos S3), opcionalmente, ative **Default retension** (retenção padrão) para este intervalo.

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

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

| Modo de retenção predefinido | Descrição |
|---|---|
| Conformidade | • O objeto não pode ser excluído até que sua data de retenção seja alcançada.<br>• O retent-until-date do objeto pode ser aumentado, mas não pode ser diminuído.<br>• A data de retenção do objeto não pode ser removida até que essa data seja atingida. |

| Modo de retenção predefinido | Descrição |
| --- | --- |
| Governança | • Os usuários com `s3:BypassGovernanceRetention` permissão podem usar o `x-amz-bypass-governance-retention: true` cabeçalho de solicitação para ignorar as configurações de retenção.<br>• Esses usuários podem excluir uma versão de objeto antes de sua data de retenção ser alcançada.<br>• Esses usuários podem aumentar, diminuir ou remover a data de retenção até um objeto. |

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

   O **período de retenção padrão** indica quanto tempo novos objetos adicionados a esse intervalo devem ser retidos, a partir do momento em que são ingeridos. Especifique um valor entre 1 e 36.500 dias ou entre 1 e 100 anos, inclusive.

4. Selecione **criar bucket**.

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

5. Opcionalmente, selecione **ir para a página de detalhes do bucket** "veja os detalhes do balde"e execute configurações adicionais.

## Veja os detalhes do balde

Você pode visualizar os buckets em sua conta de locatário.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Acesso root, Gerenciar todos os buckets ou permissão Ver todos os buckets". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket.

**Passos**

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

   A página baldes é exibida.

2. Reveja as informações de resumo de cada balde.

   Conforme necessário, você pode classificar as informações por qualquer coluna, ou pode encaminhar e voltar a página através da lista.

   Os valores contagem de objetos e espaço utilizados apresentados são estimativas. Essas estimativas são afetadas pelo timing de inests, conetividade de rede e status de nó. Se os buckets tiverem o controle de versão habilitado, as versões de objetos excluídos serão incluídas na contagem de objetos.

| Coluna | Descrição |
| --- | --- |
| Nome | O nome exclusivo do bucket, que não pode ser alterado. |
| Recursos ativados | A lista de recursos que estão ativados para o bucket. |
| S3 bloqueio de objetos | Se o bloqueio de objeto S3 está ativado para o balde.<br><br>Esta coluna só aparece se o bloqueio de objeto S3 estiver ativado para a grade. Esta coluna também mostra informações para quaisquer buckets em conformidade com o legado. |
| Região | A região do balde, que não pode ser alterada. |
| Contagem de objetos | O número de objetos neste intervalo. Quando objetos são adicionados ou excluídos, esse valor pode não ser atualizado imediatamente. Se os buckets tiverem o controle de versão ativado, versões de objetos não atuais serão incluídas neste valor. |
| Espaço utilizado | O tamanho lógico de todos os objetos no intervalo. O tamanho lógico não inclui o espaço real necessário para cópias replicadas ou codificadas para apagamento ou metadados de objetos. |
| Data de criação | A data e a hora em que o intervalo foi criado. |

3. Para ver detalhes de um intervalo específico, selecione o nome do intervalo na tabela.

   É apresentada a página de detalhes do balde. Nesta página, você pode executar as seguintes tarefas se tiver as permissões necessárias:

   - Configurar e gerenciar opções de bucket:
     - "Tags de política ILM"
     - "Gerenciar a consistência do balde"
     - "Últimas atualizações de tempo de acesso"
     - "Controle de versão de objetos"
     - "S3 bloqueio de objetos"
     - "Retenção padrão do balde"
   - Configure o acesso ao balde, como por exemplo "Compartilhamento de recursos entre origens (CORS)"
   - "Gerenciar serviços de plataforma" (Se permitido para o locatário), incluindo replicação do CloudMirror, notificações de eventos e integração de pesquisa
   - Habilite e "gerenciar a replicação entre grades"(se permitido para o locatário) a replicar objetos ingeridos nesse bucket para outro sistema StorageGRID
   - Aceda "S3 Console"ao para gerir os objetos no balde
   - "Exclua todos os objetos em um bucket"

- "Eliminar um balde" isso já está vazio

## Aplique uma etiqueta de política ILM a um bucket

Escolha uma etiqueta de política ILM para aplicar a um bucket com base nos requisitos de armazenamento de objetos.

A política ILM controla onde os dados do objeto são armazenados e se eles são excluídos após um determinado período de tempo. O administrador da grade cria políticas ILM e as atribui a tags de política ILM ao usar várias políticas ativas.

> Evite reatribuir frequentemente a etiqueta de política de um bucket. Caso contrário, podem ocorrer problemas de desempenho.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Acesso root, Gerenciar todos os buckets ou permissão Ver todos os buckets". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket.

**Passos**

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

   A página baldes é exibida. Conforme necessário, você pode classificar as informações por qualquer coluna, ou pode encaminhar e voltar a página através da lista.

2. Selecione o nome do intervalo ao qual deseja atribuir uma etiqueta de política ILM.

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

   > Os valores contagem de objetos e espaço utilizados apresentados são estimativas. Essas estimativas são afetadas pelo timing de inests, conetividade de rede e status de nó. Se os buckets tiverem o controle de versão habilitado, as versões de objetos excluídos serão incluídas na contagem de objetos.

3. Na guia Opções de balde, expanda o acordeão da etiqueta de política ILM. Esse acordeão só aparece se o administrador da grade 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 etiqueta de política ILM para um bucket acionará a reavaliação ILM de todos os objetos no bucket. Se a nova política reter objetos por um tempo limitado, os objetos mais antigos serão excluídos.

5. Selecione o botão de opção para a etiqueta que pretende atribuir ao balde.
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 de política ILM.

Certifique-se de que as aplicações do S3 não anulam acidentalmente ou excluem a nova etiqueta de bucket. Se essa tag for omitida ao aplicar um novo TagSet ao bucket, os objetos no bucket reverterão para serem avaliados em relação à política padrão do ILM.

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

A alteração da etiqueta de política atribuída a um bucket tem um impactos temporário no desempenho enquanto os objetos estão sendo reavaliados usando a nova política ILM.

## Gerenciar a consistência do balde

Valores de consistência podem ser usados para especificar a disponibilidade de alterações de configuração de bucket, bem como para fornecer um equilíbrio entre a disponibilidade dos objetos dentro de um bucket e a consistência desses objetos em diferentes nós de storage e locais. Você pode alterar os valores de consistência para serem diferentes dos valores padrão para que os aplicativos clientes possam atender às suas necessidades operacionais.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

**Diretrizes de consistência do balde**

A consistência do bucket é usada para determinar a consistência dos aplicativos clientes que afetam objetos dentro desse bucket do S3. Em geral, você deve usar a consistência **Read-after-novo-write** para seus buckets.

**altere a consistência do balde**

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

Quando você altera a consistência de um balde, apenas os objetos que são ingeridos após a alteração têm a garantia de atender à configuração revisada.

**Passos**

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

   É apresentada a página de detalhes do balde.

3. Na guia **Opções de balde**, selecione o acordeão **.

4. Selecione uma consistência para as operações realizadas nos objetos neste intervalo.
   - **Todos**: Fornece 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 de clientes em todos os sites.
   - * Strong-site*: Garante consistência de leitura-após-gravação para todas as solicitações de clientes dentro de um site.
   - **Read-after-novo-write** (padrão): Fornece consistência de leitura-após-gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
   - **Disponível**: Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.
5. Selecione **Salvar alterações**.

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

Os buckets têm várias configurações que afetam o comportamento dos buckets e dos objetos dentro desses buckets.

As seguintes configurações de bucket usam a consistência **strong** por padrão. Se dois ou mais nós de storage não estiverem disponíveis em nenhum local, ou se um site não estiver disponível, quaisquer alterações nessas configurações poderão não estar disponíveis.

- "Eliminação do balde vazio em segundo plano"
- "Último tempo de acesso"
- "Ciclo de vida do balde"
- "Política de balde"
- "Identificação do balde"
- "Controle de versão do bucket"
- "S3 bloqueio de objetos"
- "Criptografia do bucket"

> O valor de consistência para controle de versão de bucket, bloqueio de objeto S3 e criptografia de bucket não pode ser definido para um valor que não é fortemente consistente.

As seguintes configurações de bucket não usam consistência forte e têm maior disponibilidade para alterações. As alterações a essas configurações podem levar algum tempo antes de ter um efeito.

- "Configuração de serviços de plataforma: Integração de notificação, replicação ou pesquisa"
- "Configuração CORS"
- Altere a consistência do balde

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

## Ative ou desative as atualizações da última hora de acesso

Quando os administradores de grade criam as regras de gerenciamento do ciclo de vida das informações (ILM) para um sistema StorageGRID, opcionalmente, eles podem especificar que o último tempo de acesso de um objeto seja usado para determinar se deseja mover esse objeto para um local de armazenamento diferente. Se você estiver usando um locatário do S3, poderá aproveitar essas regras habilitando as atualizações da última hora de acesso para os objetos em um bucket do S3.

Estas instruções aplicam-se apenas a sistemas StorageGRID que incluam pelo menos uma regra ILM que utilize a opção **último tempo de acesso** como um filtro avançado ou como um tempo de referência. Você pode ignorar essas instruções se o seu sistema StorageGRID não incluir essa regra. "Use o último tempo de acesso nas regras do ILM"Consulte para obter detalhes.

### Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

### Sobre esta tarefa

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

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

- Os objetos recuperados no mês passado devem permanecer nos nós de storage locais.
- Os objetos que não foram recuperados no mês passado devem ser movidos para um local externo.

Por padrão, as atualizações para a última hora de acesso são desativadas. Se o seu sistema StorageGRID incluir uma regra ILM que use a opção **último tempo de acesso** e você quiser que essa opção se aplique a objetos neste intervalo, você deverá habilitar as atualizações para o último tempo de acesso para os buckets do S3 especificados nessa regra.

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

Um impactos no desempenho ocorre com as últimas atualizações de tempo de acesso porque o StorageGRID deve executar essas etapas adicionais sempre que os objetos são recuperados:

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

ILM

A tabela resume o comportamento aplicado a todos os objetos no intervalo quando o último tempo de acesso é desativado ou ativado.

| Tipo de solicitação | Comportamento se a última hora de acesso estiver desativada (predefinição) | | Comportamento se a última hora de acesso estiver ativada | |
|---|---|---|---|---|
| | Último tempo de acesso atualizado? | Objeto adicionado à fila de avaliação ILM? | Último tempo de acesso atualizado? | Objeto adicionado à fila de avaliação ILM? |
| 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 copiar um objeto de um bucket para outro | • Não, para a cópia de origem<br>• Sim, para a cópia de destino | • Não, 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 | • Sim, para a cópia de origem<br>• Sim, para a cópia de destino |
| Pedido para concluir um carregamento multipart | Sim, para o objeto montado | Sim, para o objeto montado | Sim, para o objeto montado | Sim, para o objeto montado |

**Passos**

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

   É apresentada a página de detalhes do balde.

3. Na guia **Opções do balde**, selecione o acordeão **atualizações do último tempo de acesso**.
4. Ative ou desative as atualizações da última hora de acesso.
5. Selecione **Salvar alterações**.

## Alterar o controle de versão de objetos para um bucket

Se você estiver usando um locatário S3, poderá alterar o estado de controle de versão para buckets do S3.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Todos os nós de storage estão disponíveis.

**Sobre esta tarefa**

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

- Desativado: O controle de versão nunca foi habilitado
- Habilitado: O controle de versão está habilitado
- Suspenso: O controle de versão foi ativado anteriormente e está suspenso

Para obter mais informações, consulte o seguinte:

- "Controle de versão de objetos"
- "Regras e políticas do ILM para objetos com versão S3 (exemplo 4)"
- "Como os objetos são excluídos"

**Passos**

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

   É apresentada a página de detalhes do balde.

3. Na guia **Opções de balde**, selecione o acordeão **versão de objeto**.
4. Selecione um estado de controle de versão para os objetos neste intervalo.

   O controle de versão do objeto deve permanecer habilitado para um bucket usado para replicação entre grades. Se o bloqueio de objeto S3 ou a conformidade legada estiver ativada, as opções **versão de objeto** serão desativadas.

| Opção | Descrição |
| --- | --- |
| Habilite o controle de versão | Ative o controle de versão de objetos se você quiser armazenar todas as versões de cada objeto neste intervalo. Em seguida, você pode 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. |
| Suspenda o controle de versão | Suspenda o controle de versão do objeto se você não quiser mais criar novas versões de objeto. Você ainda pode recuperar quaisquer versões de objetos existentes. |

5. Selecione **Salvar alterações**.

## Use o bloqueio de objetos S3D para reter objetos

Você pode usar o bloqueio de objetos S3 se os buckets e os objetos precisarem cumprir os requisitos regulamentares para retenção.

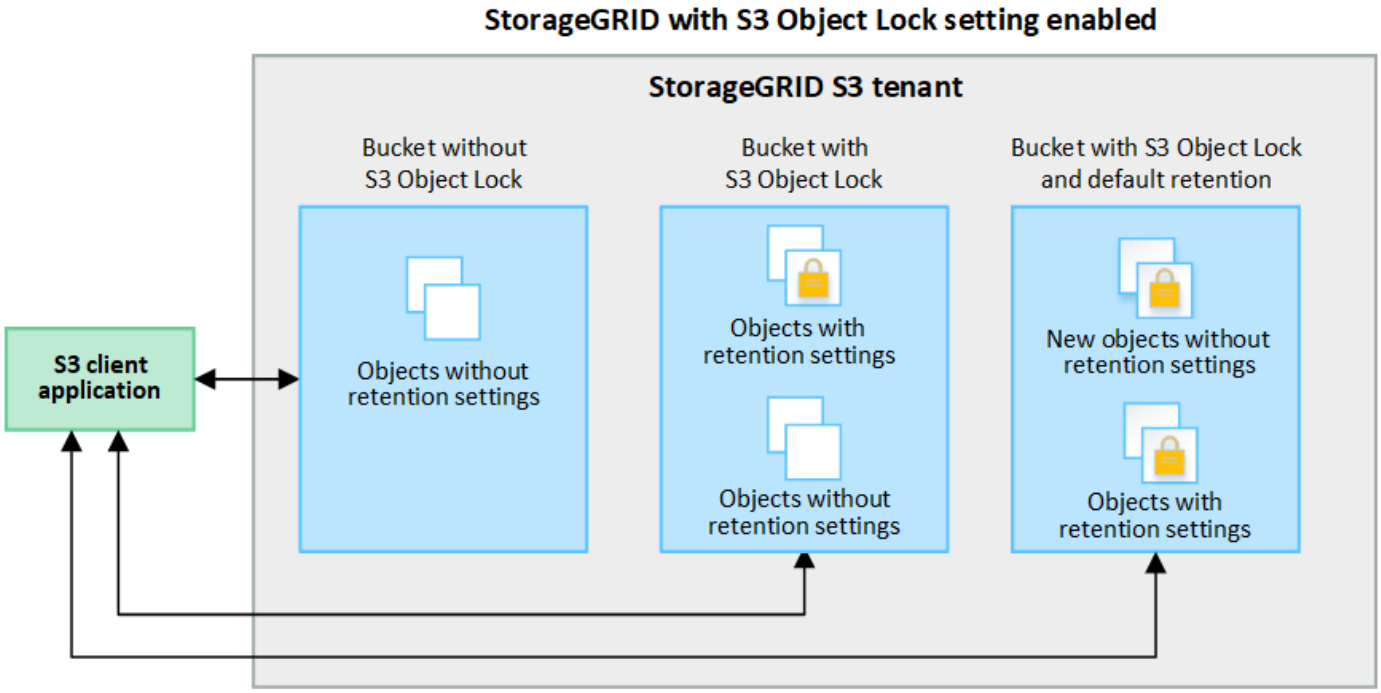
### O que é S3 Object Lock?

O recurso bloqueio de objetos do StorageGRID S3 é uma solução de proteção de objetos equivalente ao bloqueio de objetos do S3 no Amazon Simple Storage Service (Amazon S3).

Como mostrado na figura, quando a configuração global de bloqueio de objeto S3D está ativada para um sistema StorageGRID, uma conta de locatário S3D pode criar buckets com ou sem bloqueio de objeto S3D ativado. Se um bucket tiver o bloqueio de objetos S3 ativado, o controle de versão do bucket é necessário e é ativado automaticamente.

Se um bucket tiver o bloqueio de objeto S3 ativado, os aplicativos cliente S3 podem, opcionalmente, especificar configurações de retenção para qualquer versão de objeto salva nesse bucket.

Além disso, um bucket com o bloqueio de objetos S3 ativado pode, opcionalmente, ter um modo de retenção e um período de retenção padrão. As configurações padrão se aplicam somente a objetos que são adicionados ao bucket sem suas próprias configurações de retenção.




#### Modos de retenção

O recurso bloqueio de objetos do StorageGRID S3 suporta 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 data de retenção seja alcançada.
  - O retent-until-date do objeto pode ser aumentado, mas não pode ser diminuído.
  - A data de retenção do objeto não pode ser removida até que essa data seja atingida.

- No modo de governança:
  - Os usuários com permissão especial podem usar um cabeçalho de desvio em solicitações para modificar determinadas configurações de retenção.
  - Esses usuários podem excluir uma versão de objeto antes de sua data de retenção ser alcançada.
  - Esses usuários podem aumentar, diminuir ou remover a data de retenção até um objeto.

#### Configurações de retenção para versões de objetos

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

- **Modo de retenção**: Conformidade ou governança.
- **Retent-until-date**: Se a data de retent-until de uma versão de objeto estiver no futuro, o objeto pode ser recuperado, mas não pode ser excluído.
- **Retenção legal**: Aplicar uma retenção legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar colocar uma retenção legal em um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até que seja explicitamente removida. As obrigações legais são independentes da retenção até à data.

  > ⓘ Se um objeto estiver sob uma retenção legal, ninguém poderá excluir o objeto, independentemente de seu modo de retenção.

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

#### Configuração de retenção padrão para buckets

Se um bucket for criado com o bloqueio de objetos S3 ativado, os usuários podem especificar opcionalmente as seguintes configurações padrão para o bucket:

- **Modo de retenção padrão**: Conformidade ou governança.
- **Período de retenção padrão**: Quanto tempo as novas versões de objetos adicionadas a este intervalo devem ser mantidas, a partir do dia em que são adicionadas.

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

"Crie um bucket do S3"Consulte e "Atualização S3 retenção padrão bloqueio Objeto".

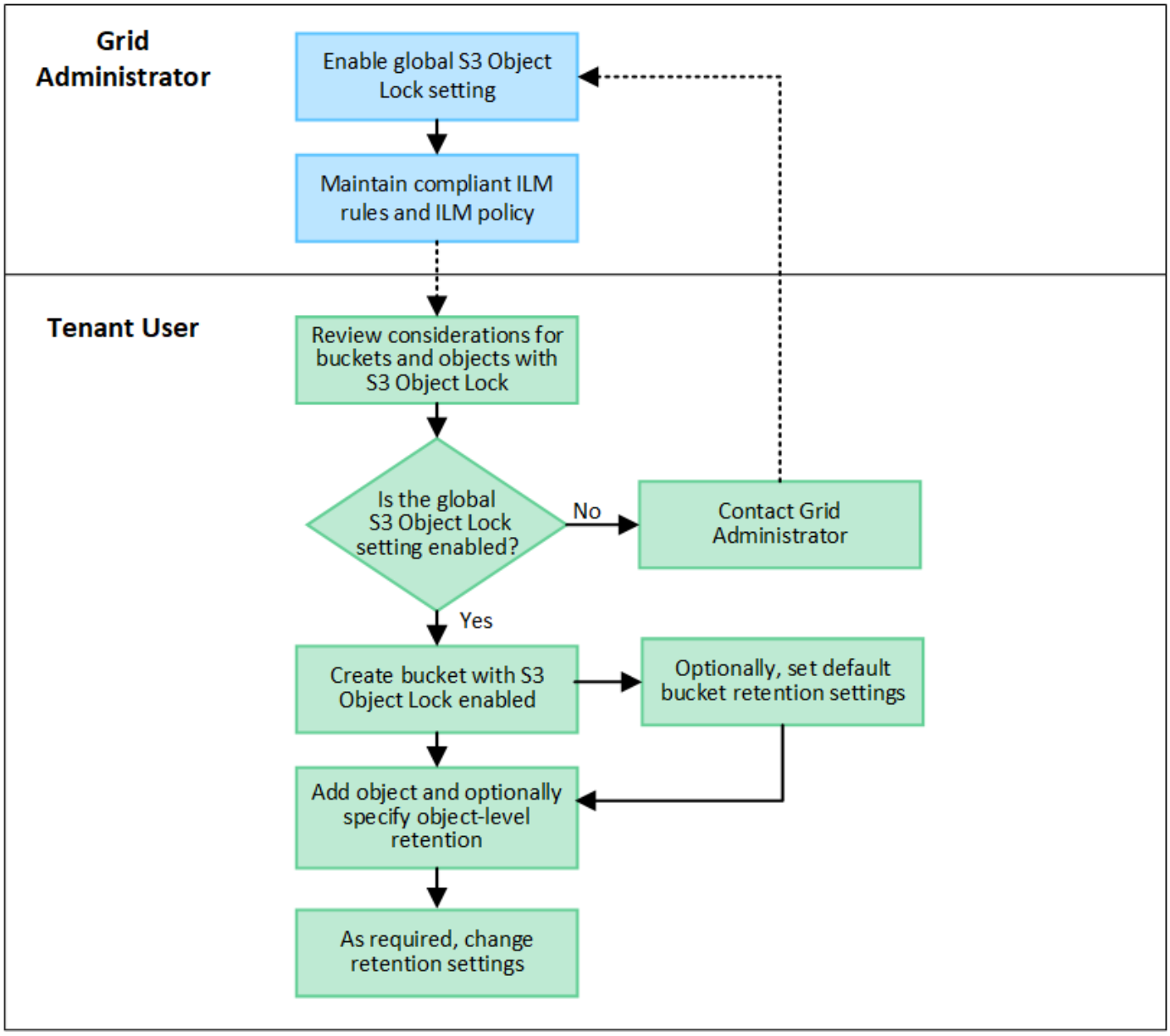
### S3 fluxo de trabalho Object Lock

O diagrama de fluxo de trabalho mostra as etapas de alto nível para usar o recurso bloqueio de objetos S3 no StorageGRID.

Antes de criar buckets com o bloqueio de objeto S3 ativado, o administrador de grade deve ativar a configuração global de bloqueio de objeto S3 para todo o sistema StorageGRID. O administrador da grade também deve garantir que a política de gerenciamento do ciclo de vida das informações (ILM) seja "compatível"; ela deve atender aos requisitos dos buckets com o bloqueio de objetos S3 ativado. Para obter detalhes, contacte o administrador da grelha ou consulte as instruções "Gerencie objetos com o S3 Object

Lock"para .

Depois que a configuração global S3 Object Lock for ativada, você poderá criar buckets com o S3 Object Lock ativado e, opcionalmente, especificar as configurações de retenção padrão para cada bucket. Além disso, você pode usar o aplicativo cliente S3 para especificar opcionalmente as configurações de retenção para cada versão do objeto.




**Requisitos para buckets com bloqueio de objeto S3 ativado**

- Se a configuração global de bloqueio de objeto S3 estiver ativada para o sistema StorageGRID, você poderá usar o Gerenciador de locatário, a API de gerenciamento de locatário ou a API REST S3 para criar buckets com o bloqueio de objeto S3 ativado.
- Se você planeja usar o bloqueio de objetos S3D, você deve ativar o bloqueio de objetos S3D ao criar o bucket. Não é possível ativar o bloqueio de objetos S3 para um bucket existente.
- Quando o bloqueio de objeto S3 está ativado para um bucket, o StorageGRID ativa automaticamente o controle de versão desse bucket. Não é possível desativar o bloqueio de objetos S3 ou suspender o controle de versão para o bucket.

- Opcionalmente, você pode especificar um modo de retenção padrão e um período de retenção para cada bucket usando o Gerenciador de locatários, a API de gerenciamento do locatário ou a API REST do S3. 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 manter-até-data para cada versão do objeto quando ele é carregado.
- A configuração do ciclo de vida do bucket é compatível com buckets com o S3 Object Lock ativado.
- A replicação do CloudMirror não é compatível com buckets com o S3 Object Lock ativado.

**Requisitos para objetos em buckets com o bloqueio de objetos S3 ativado**

- Para proteger uma versão de objeto, você pode especificar configurações de retenção padrão para o bucket ou especificar configurações de retenção para cada versão do objeto. As configurações de retenção no nível do objeto podem ser especificadas usando o aplicativo cliente S3 ou a API REST S3.
- As configurações de retenção se aplicam a versões de objetos individuais. Uma versão de objeto pode ter uma configuração de retenção de data e de retenção legal, uma mas não a outra, ou nenhuma. Especificar uma configuração reter-até-data ou retenção 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 dos objetos em buckets com o bloqueio de objetos S3 ativado**

Cada objeto que é salvo em um bucket com o S3 Object Lock ativado passa por estes estágios:

1. * Ingestão de objetos*

   Quando uma versão de objeto é adicionada ao bucket que tem o bloqueio de objeto S3 ativado, as configurações de retenção são aplicadas da seguinte forma:

   - Se as configurações de retenção forem especificadas para o objeto, as configurações de nível do objeto serão aplicadas. Todas as configurações padrão do bucket são ignoradas.
   - Se não forem especificadas configurações de retenção para o objeto, as configurações padrão de bucket serão aplicadas, se existirem.
   - Se nenhuma configuração de retenção for especificada para o objeto ou o bucket, o objeto não será protegido pelo bloqueio de objeto S3.

   Se as configurações de retenção forem aplicadas, o objeto e quaisquer metadados definidos pelo usuário do S3 serão protegidos.

2. * Retenção e exclusão de objetos*

   Várias cópias de cada objeto protegido são armazenadas pelo StorageGRID durante o período de retenção especificado. O número exato e o tipo de cópias de objetos e os locais de storage são determinados pelas regras em conformidade nas políticas ativas de ILM. Se um objeto protegido pode ser excluído antes de sua data de retenção ser alcançada depende de seu modo de retenção.

   - Se um objeto estiver sob uma retenção legal, ninguém poderá excluir o objeto, independentemente de seu modo de retenção.

**Ainda posso gerenciar buckets em conformidade com o legado?**

O recurso bloqueio de objetos S3 substitui o recurso de conformidade que estava disponível nas versões anteriores do StorageGRID. Se você criou buckets compatíveis usando uma versão anterior do StorageGRID,

poderá continuar gerenciando as configurações desses buckets. No entanto, não será mais possível criar novos buckets compatíveis. Para obter instruções, "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"consulte .

## Atualização S3 retenção padrão bloqueio Objeto

Se você ativou o bloqueio de objeto S3 quando criou o bucket, poderá editar o bucket para alterar as configurações de retenção padrão. Você pode ativar (ou desativar) a retenção padrão e definir um modo de retenção e um período de retenção padrão.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- O bloqueio de objetos S3D é ativado globalmente para o seu sistema StorageGRID e você ativou o bloqueio de objetos S3D quando criou o bucket. "Use o bloqueio de objetos S3D para reter objetos"Consulte .

**Passos**

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

   É apresentada a página de detalhes do balde.

3. Na guia **Opções de balde**, selecione o acordeão **S3 Object Lock**.
4. Opcionalmente, ative ou desative **retenção padrão** para este bucket.

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

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

| Modo de retenção predefinido | Descrição |
| --- | --- |
| Conformidade | • O objeto não pode ser excluído até que sua data de retenção seja alcançada.<br>• O retent-until-date do objeto pode ser aumentado, mas não pode ser diminuído.<br>• A data de retenção do objeto não pode ser removida até que essa data seja atingida. |

| Modo de retenção predefinido | Descrição |
| --- | --- |
| Governança | • Os usuários com `s3:BypassGovernanceRetention` permissão podem usar o `x-amz-bypass-governance-retention: true` cabeçalho de solicitação para ignorar as configurações de retenção.<br>• Esses usuários podem excluir uma versão de objeto antes de sua data de retenção ser alcançada.<br>• Esses usuários podem aumentar, diminuir ou remover a data de retenção até um objeto. |

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

   O **período de retenção padrão** indica quanto tempo novos objetos adicionados a esse intervalo devem ser retidos, a partir do momento em que são ingeridos. Especifique um valor entre 1 e 36.500 dias ou entre 1 e 100 anos, inclusive.

7. Selecione **Salvar alterações**.

## Configurar o compartilhamento de recursos entre origens (CORS)

Você pode configurar o compartilhamento de recursos entre origens (CORS) para um bucket do S3 se quiser que esse bucket e objetos nesse bucket estejam acessíveis a aplicativos da Web em outros domínios.

### Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

### Sobre esta tarefa

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

### Ativar CORS para um balde

### Passos

1. Use um editor de texto para criar o XML necessário.

   Este exemplo mostra o XML usado para ativar o CORS para um bucket S3. Esse XML permite que qualquer domínio envie SOLICITAÇÕES GET para o bucket, mas só permite que o `http://www.example.com` domínio envie SOLICITAÇÕES POST e EXCLUA. 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 do CORS, "Documentação do Amazon Web Services (AWS): Guia do desenvolvedor do Amazon Simple Storage Service" consulte .

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

   É apresentada a página de detalhes do balde.

4. Na guia **Bucket Access**, selecione o acordeão **Cross-Origin Resource Sharing (CORS)**.
5. Marque a caixa de seleção **Enable CORS** (Ativar CORS*).
6. Cole o XML de configuração do CORS na caixa de texto.
7. Selecione **Salvar alterações**.

#### Modificar a definição CORS

**Passos**

1. Atualize o XML de configuração do CORS na caixa de texto ou selecione **Limpar** para recomeçar.
2. Selecione **Salvar alterações**.

#### Desativar a definição CORS

**Passos**

1. Desmarque a caixa de seleção **Enable CORS** (Ativar CORS*).
2. Selecione **Salvar alterações**.

## Excluir objetos no bucket

Você pode usar o Gerenciador do locatário para excluir os objetos em um ou mais buckets.

### Considerações e requisitos

Antes de executar estas etapas, observe o seguinte:

- Quando você exclui os objetos em um bucket, o StorageGRID remove permanentemente todos os objetos e todas as versões de objetos em cada bucket selecionado de todos os nós e sites do seu sistema StorageGRID. O StorageGRID também remove quaisquer metadados de objetos relacionados. Você não será capaz de recuperar essas informações.
- A exclusão de todos os objetos em um bucket pode levar minutos, dias ou até semanas, com base no número de objetos, cópias de objetos e operações simultâneas.
- Se um bucket tiver "S3 bloqueio de objetos ativado", ele poderá permanecer no estado **Deletando objetos: Somente leitura** por *anos*.

Um bucket que usa o bloqueio de objeto S3 permanecerá no estado **excluindo objetos: Somente leitura** até que a data de retenção seja alcançada para todos os objetos e quaisquer retenções legais sejam removidas.

- Enquanto os objetos estão sendo excluídos, o estado do bucket é **excluindo objetos: Somente leitura**. Neste estado, não é possível adicionar novos objetos ao intervalo.
- Quando todos os objetos tiverem sido excluídos, o bucket permanece no estado somente leitura. Você pode fazer um dos seguintes procedimentos:
  - Retorne o bucket ao modo de gravação e reutilize-o para novos objetos
  - Elimine o balde
  - Mantenha o intervalo no modo somente leitura para reservar seu nome para uso futuro
- Se um bucket tiver o controle de versão de objetos ativado, excluir marcadores criados no StorageGRID 11,8 ou posterior poderá ser removido usando o recurso Excluir objetos em operações de bucket.
- Se um bucket tiver o controle de versão de objeto ativado, a operação excluir objetos não removerá marcadores de exclusão criados no StorageGRID 11,7 ou anterior. Consulte informações sobre como excluir objetos em um bucket no "Como objetos com versão S3 são excluídos".
- Se utilizar "replicação entre grade"o , tenha em atenção o seguinte:
  - Usar essa opção não exclui nenhum objeto do bucket na outra grade.
  - Se você selecionar essa opção para o intervalo de origem, o alerta **Falha na replicação entre grades** será acionado se você adicionar objetos ao intervalo de destino na outra grade. Se você não puder garantir que ninguém adicionará objetos ao bucket na outra grade, "desative a replicação entre redes" para esse bucket antes de excluir todos os objetos do bucket.

### Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Permissão de acesso à raiz". Essa permissão substitui as configurações de permissões em políticas de grupo ou bucket.

### Passos

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

   A página baldes é exibida e mostra todos os baldes S3 existentes.

2. Use o menu **ações** ou a página de detalhes de um intervalo específico.

**Menu ações**

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

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

**Página de detalhes**

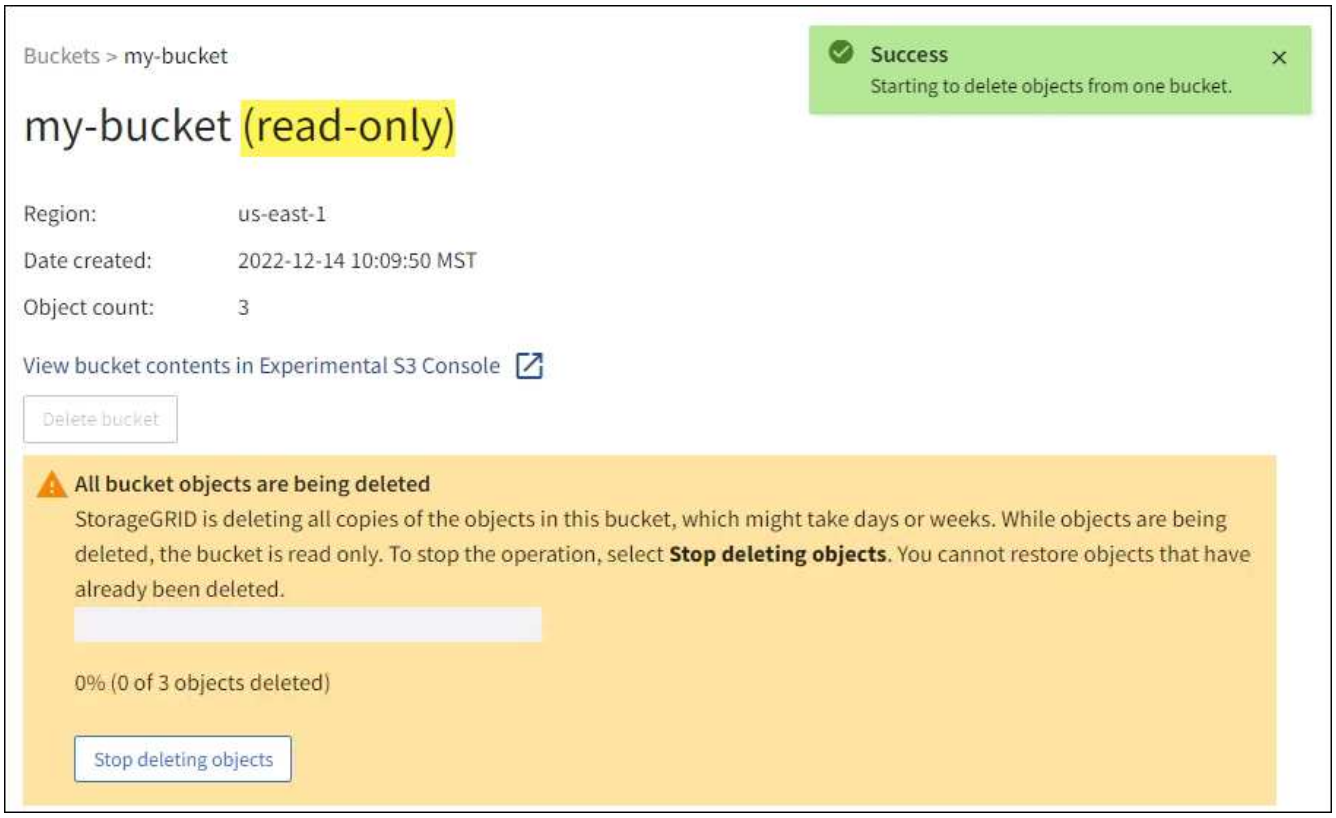
a. Selecione um nome de bucket para exibir seus detalhes.

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

3. Quando a caixa de diálogo de confirmação for exibida, revise os detalhes, digite **Sim** e selecione **OK**.
4. Aguarde o início da operação de eliminação.

   Após alguns minutos:

   - É apresentado um banner de estado amarelo na página de detalhes do balde. A barra de progresso representa a porcentagem de objetos que foram excluídos.
   - **(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.

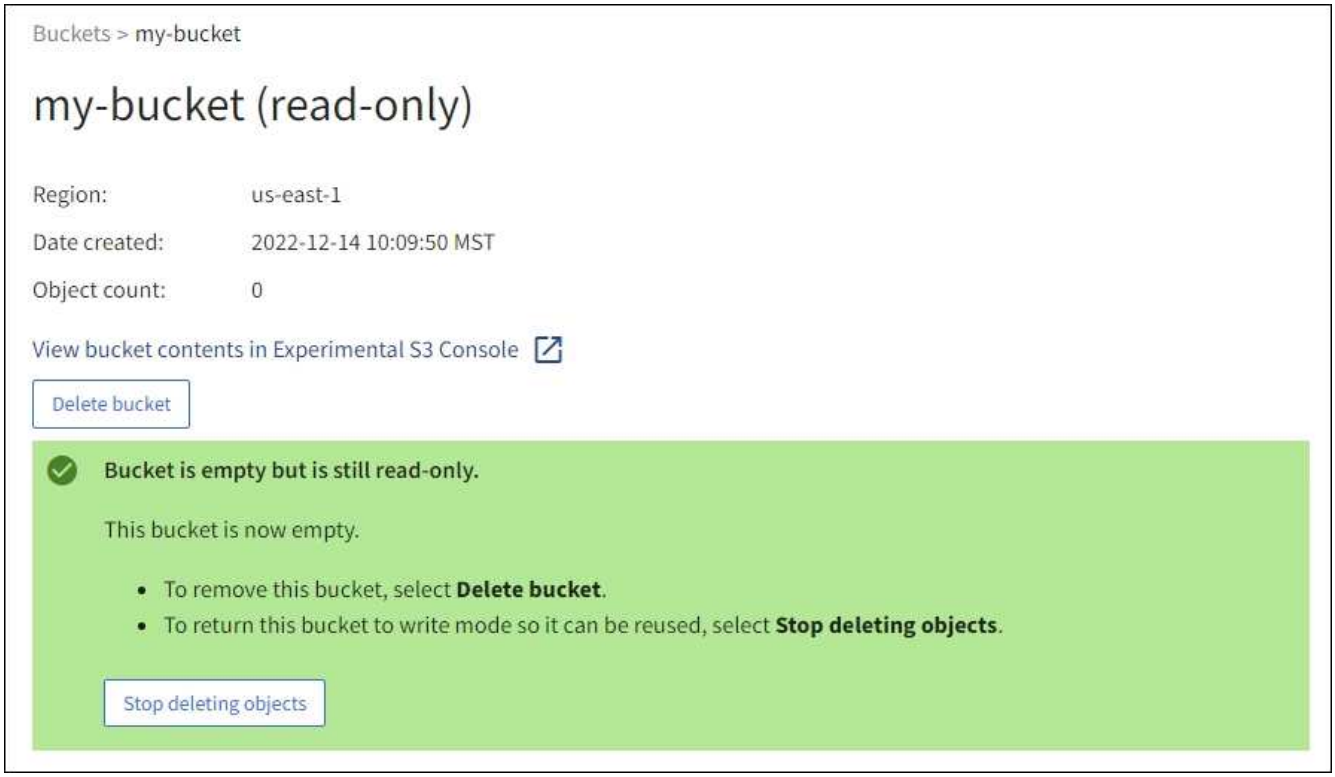



5. Conforme necessário enquanto a operação estiver em execução, selecione **Parar de excluir objetos** para interromper o processo. Em seguida, opcionalmente, selecione **Excluir objetos no bucket** para retomar o processo.

   Quando você seleciona **Parar de excluir objetos**, o bucket é retornado ao modo de gravação; no entanto, você não pode acessar ou restaurar quaisquer objetos que tenham sido excluídos.

6. Aguarde até que a operação seja concluída.

Quando o intervalo está vazio, o banner de status é atualizado, mas o intervalo permanece somente leitura.




7. Execute um dos seguintes procedimentos:
   - Saia da página para manter o balde no modo só de leitura. Por exemplo, você pode manter um bucket vazio no modo somente leitura para reservar o nome do bucket para uso futuro.
   - Elimine o balde. Você pode selecionar **Excluir bucket** para excluir um único bucket ou retornar a página Buckets e selecionar **Actions** > **Delete** buckets para remover mais de um bucket.

     Se você não conseguir excluir um bucket versionado depois que todos os objetos foram excluídos, os marcadores de exclusão podem permanecer. Para eliminar o intervalo, tem de remover todos os marcadores de eliminação 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.

## Eliminar o balde S3

Você pode usar o Gerenciador do Locatário para excluir um ou mais buckets do S3 vazios.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Os intervalos que você deseja excluir estão vazios. Se os intervalos que você deseja excluir estiverem *não* vazios, "eliminar objetos do intervalo".

**Sobre esta tarefa**

Estas instruções descrevem como excluir um bucket do S3 usando o Gerenciador do locatário. Também é possível excluir buckets do S3 usando o "API de gerenciamento do locatário" 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 com versão S3 são excluídos, "Como os objetos são excluídos"consulte .

**Passos**

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

   A página baldes é exibida e mostra todos os baldes S3 existentes.

2. Use o menu **ações** ou a página de detalhes de um intervalo específico.

   **Menu ações**

   a. Selecione a caixa de verificação para cada intervalo que pretende eliminar.

   b. Selecione **ações** > **Excluir buckets**.

   **Página de detalhes**

   a. Selecione um nome de bucket para exibir seus detalhes.

   b. Selecione **Eliminar balde**.

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

   O StorageGRID confirma que cada bucket está vazio e, em seguida, exclui cada bucket. Esta operação pode demorar alguns minutos.

   Se um balde não estiver vazio, é apresentada uma mensagem de erro. Você deve "exclua todos os objetos e quaisquer marcadores de exclusão no bucket" antes de poder excluir o bucket.

## Use o Console S3

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

S3 Console permite que você:

- Carregar, transferir, mudar o nome, copiar, mover e eliminar objetos
- Exibir, reverter, baixar e excluir versões de objetos
- Pesquisar objetos por prefixo
- Gerenciar tags de objeto
- Exibir metadados de objetos
- Exibir, criar, renomear, copiar, mover e excluir pastas

O console S3 oferece uma experiência de usuário aprimorada para os casos mais comuns. Ele não foi projetado para substituir as operações CLI ou API em todas as situações.

Se o uso do Console S3 resulta em operações demoradas demais (por exemplo, minutos ou horas), considere:

- Reduzindo o número de objetos selecionados
- Usando métodos não gráficos (API ou CLI) para acessar seus dados

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Se você quiser gerenciar objetos, você pertence a um grupo de usuários que tem a permissão de acesso root. Como alternativa, você pertence a um grupo de usuários que tem a permissão usar a guia Console S3 e a permissão Exibir todos os buckets ou Gerenciar todos os buckets. "Permissões de gerenciamento do locatário"Consulte .
- Uma política de grupo S3 ou balde foi configurada para o utilizador. "Use políticas de acesso de grupo e bucket"Consulte .
- Você sabe o ID da chave de acesso do usuário e a chave de acesso secreta. Opcionalmente, você tem um `.csv` arquivo contendo essas informações. Consulte "instruções para criar chaves de acesso".

**Passos**

1. Selecione **STORAGE** > **Buckets** > ***bucket name***.
2. Selecione a guia Console do S3.
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 o seu `.csv` ficheiro.
4. Selecione **entrar**.
5. É apresentada a tabela de objetos de balde. Você pode gerenciar objetos conforme necessário.

**Informações adicionais**

- **Busca por prefixo**: O recurso de pesquisa de prefixo procura apenas objetos que começam com uma palavra específica relativa à pasta atual. A pesquisa não inclui objetos que contenham a palavra em outro lugar. Esta regra também se aplica a objetos dentro de pastas. Por exemplo, uma pesquisa `folder1/folder2/somefile-` retornaria objetos que estão dentro da `folder1/folder2/` pasta e começaria com a palavra `somefile-`.
- * Arrastar e soltar*: Você pode arrastar e soltar arquivos do gerenciador de arquivos do computador para o console S3. No entanto, não é possível carregar pastas.
- **Operações em pastas**: Quando você move, copia ou renomeia uma pasta, todos os objetos na pasta são atualizados um de cada vez, o que pode levar tempo.
- **Exclusão permanente quando o controle de versão do bucket está desativado**: Quando você substitui ou exclui um objeto em um bucket com o controle de versão desativado, a operação é permanente. "Alterar o controle de versão de objetos para um bucket"Consulte .

# Gerenciar os serviços da plataforma S3

# Gerenciar serviços de plataforma: Visão geral

Os serviços de plataforma StorageGRID ajudam você a implementar uma estratégia de nuvem híbrida permitindo que você envie notificações de eventos e cópias de objetos S3 e metadados de objetos para destinos externos.

Se o uso de serviços de plataforma for permitido para sua conta de locatário, você poderá configurar os seguintes serviços para qualquer bucket do S3:

**Replicação do CloudMirror**

"Serviço de replicação do StorageGRID CloudMirror"Use para espelhar objetos específicos de um bucket do StorageGRID para um destino externo especificado.

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

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

**Notificações**

Use "notificações de eventos por bucket" para enviar notificações sobre ações específicas executadas em objetos para um Amazon Simple Notification Service (Amazon SNS) externo especificado.

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.

> ⓘ Embora a notificação de evento possa ser configurada em um bucket com o bloqueio de objeto S3 ativado, os metadados do bloqueio de objeto S3 (incluindo o status reter até a data e retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

**Serviço de integração de pesquisa**

Use o "serviço de integração de pesquisa" para enviar metadados de objetos S3 para um índice Elasticsearch especificado, onde os metadados podem ser pesquisados ou analisados usando o serviço externo.

Por exemplo, você pode configurar seus buckets para enviar metadados de objeto S3 para um serviço Elasticsearch remoto. Você pode usar o Elasticsearch para realizar pesquisas entre buckets e realizar análises sofisticadas de padrões presentes nos metadados do objeto.

> ⓘ Embora a integração do Elasticsearch possa ser configurada em um bucket com o bloqueio de objeto S3 ativado, os metadados do bloqueio de objeto S3 (incluindo o status reter até a data e retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

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

Qualquer combinação de serviços de plataforma pode ser configurada para um único bucket do S3. Por exemplo, você pode configurar o serviço CloudMirror e as notificações em um bucket do StorageGRID S3 para que você possa espelhar objetos específicos para o Amazon Simple Storage Service, enquanto envia uma notificação sobre cada objeto a um aplicativo de monitoramento de terceiros para ajudá-lo a controlar

suas despesas da AWS.

> O uso de serviços de plataforma deve ser habilitado para cada conta de locatário por um administrador do StorageGRID usando o Gerenciador de Grade ou a API de Gerenciamento de Grade.

### Como os serviços de plataforma são configurados

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

Depois de criar um endpoint externo, você pode habilitar um serviço de plataforma para um bucket adicionando a configuração XML ao bucket. A configuração XML identifica os objetos nos quais o bucket deve agir, a ação que o bucket deve realizar e o ponto final que o bucket deve usar para o serviço.

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

- Se você quiser que todos os objetos cujas chaves comecem por `/images` ser replicados em um bucket do Amazon S3, adicione uma configuração de replicação ao bucket de origem.
- Se você também quiser enviar notificações quando esses objetos estiverem armazenados no bucket, adicione uma configuração de notificações.
- Finalmente, se você quiser indexar os metadados para esses objetos, adicione a configuração de notificação de metadados usada para implementar a integração de pesquisa.

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

| Serviço de plataforma | S3 API REST | Consulte |
|---|---|---|
| Replicação do CloudMirror | • GetBucketReplication<br>• PutBucketReplication | • "Replicação do CloudMirror"<br>• "Operações em baldes" |
| Notificações | • GetBucketNotificationConfiguration<br>• PutBucketNotificationConfiguration | • "Notificações"<br>• "Operações em baldes" |
| Integração de pesquisa | • OBTER configuração de notificação de metadados do bucket<br>• COLOQUE a configuração de notificação de metadados do bucket | • "Integração de pesquisa"<br>• "Operações personalizadas do StorageGRID" |

### Informações relacionadas

"Considerações para serviços de plataforma"

**Serviço de replicação do CloudMirror**

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

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

> A replicação do CloudMirror tem semelhanças e diferenças importantes com o recurso de replicação entre grades. Para saber mais, "Compare a replicação entre redes e a replicação do CloudMirror"consulte .

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

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

No StorageGRID, é possível replicar os objetos em um único bucket em vários buckets do destino. Para fazer isso, especifique o destino para cada regra no XML de configuração de replicação. Não é possível replicar um objeto para mais de um bucket ao mesmo tempo.

Além disso, você pode configurar a replicação do CloudMirror em buckets com controle de versão ou não versionados e especificar um bucket com controle de versão ou não versionado como destino. Você pode usar qualquer combinação de buckets versionados e não versionados. Por exemplo, você pode especificar um bucket versionado como o destino para um bucket de origem não versionado, ou vice-versa. Você também pode replicar entre buckets não versionados.

O comportamento de exclusão para o serviço de replicação do CloudMirror é o mesmo que o comportamento de exclusão do serviço CRR (Cross Region Replication) fornecido pelo Amazon S3 — excluir um objeto em um bucket de origem nunca exclui um objeto replicado no destino. Se os intervalos de origem e destino forem versionados, o marcador de exclusão será replicado. Se o intervalo de destino não tiver versão, a exclusão de um objeto no intervalo de origem não replica o marcador de exclusão para o intervalo de destino nem exclui o objeto de destino.

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

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

A singularidade e a ordem dos eventos no intervalo de destino não são garantidas. Mais de uma cópia idêntica de um objeto de origem pode ser entregue ao destino como resultado de operações tomadas para

garantir o sucesso da entrega. Em casos raros, quando o mesmo objeto é atualizado simultaneamente de dois ou mais locais diferentes do StorageGRID, a ordenação de operações no intervalo de destino pode não corresponder à ordenação de eventos no intervalo de origem.

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

### Entenda as notificações para buckets

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

Você pode "configurar notificações de eventos"associar XML de configuração de notificação a um bucket de origem. O XML de configuração de notificação segue convenções S3 para configurar notificações de bucket, com o tópico Kafka de destino ou Amazon SNS especificado como a URNA de um endpoint.

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

A singularidade e a ordem das notificações não são garantidas. Mais de uma notificação de um evento pode ser entregue ao destino como resultado de operações tomadas para garantir o sucesso da entrega. E como a entrega é assíncrona, o tempo de ordenação das notificações no destino não é garantido para corresponder à ordenação de eventos no intervalo de origem, particularmente para operações originadas de diferentes sites da StorageGRID. Você pode usar a `sequencer` chave na mensagem de evento para determinar a ordem dos eventos para um determinado objeto, conforme descrito na documentação do Amazon S3.

#### Notificações e mensagens suportadas

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

- Os seguintes tipos de evento são suportados:
  - S3:ObjectCreated:*
  - S3:ObjectCreated:put
  - S3:ObjectCreated:Post
  - S3:ObjectCreated:Copy
  - S3:ObjectCreated:CompleteMultipartUpload
  - S3:ObjectRemoved:*
  - S3:ObjectRemovado: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, como mostrado na tabela:

| Nome da chave | Valor StorageGRID |
| --- | --- |
| EventSource | `sgws:s3` |
| AwsRegion | não incluído |
| x-amz-id-2 | não incluído |
| arn | `urn:sgws:s3:::bucket_name` |

**Compreender o serviço de integração de pesquisa**

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

O serviço de integração de pesquisa é um serviço StorageGRID personalizado que envia automaticamente e assincronamente metadados de objetos S3 para um endpoint de destino sempre que um objeto ou seus metadados são atualizados. Depois, você pode 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 do objeto.

Você pode ativar o serviço de integração de pesquisa para qualquer bucket com versão ou não versionado. A integração de pesquisa é configurada associando o XML de configuração de notificação de metadados ao intervalo que especifica quais objetos agir e o destino para os metadados de objeto.

As notificações são geradas na forma de um documento JSON chamado com o nome do intervalo, nome do objeto e 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 do objeto e metadados do usuário.

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

As notificações são geradas e enfileiradas para entrega sempre que:

- Um objeto é criado.
- Um objeto é excluído, inclusive quando os objetos são excluídos como resultado da operação da política ILM da grade.
- Metadados de objetos ou tags 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 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 intervalo. Para garantir que os metadados de objetos para todos os objetos no bucket sejam enviados para o destino, você deve fazer um dos seguintes procedimentos:

- 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 no intervalo que acionará uma mensagem de notificação de metadados a ser enviada para o destino.

O serviço de integração de pesquisa StorageGRID suporta um cluster Elasticsearch como destino. Tal como acontece com os outros serviços da plataforma, o destino é especificado no endpoint cuja URN é usada no XML de configuração para o serviço. Use o "Ferramenta de Matriz de interoperabilidade do NetApp" para determinar as versões suportadas do Elasticsearch.

**Informações relacionadas**

"Configuração XML para integração de pesquisa"

"Metadados de objetos incluídos nas notificações de metadados"

"JSON gerado pelo serviço de integração de pesquisa"

"Configurar o serviço de integração de pesquisa"

## Considerações para serviços de plataforma

Antes de implementar os serviços da plataforma, revise as recomendações e considerações sobre o uso desses serviços.

Para obter informações sobre o S3, "USE A API REST DO S3"consulte .

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

| Consideração | Detalhes |
| --- | --- |
| Monitoramento de endpoint de destino | Você deve monitorar a disponibilidade de cada endpoint de destino. Se a conetividade com o endpoint de destino for perdida por um longo período de tempo e existir um grande backlog de solicitações, solicitações de cliente adicionais (como SOLICITAÇÕES PUT) para o StorageGRID falharão. Você deve tentar novamente essas solicitações com falha quando o endpoint se tornar acessível. |

| Consideração | Detalhes |
| --- | --- |
| Limitação do ponto de extremidade de destino | O software StorageGRID pode controlar as solicitações recebidas do S3 para um bucket se a taxa na qual as solicitações estão sendo enviadas exceder a taxa na qual o endpoint de destino pode receber as solicitações. O estrangulamento só ocorre quando há um backlog de solicitações aguardando para serem enviadas para o endpoint de destino.<br><br>O único efeito visível é que as solicitações S3 recebidas demorarão mais tempo para serem executadas. Se você começar a detetar desempenho significativamente mais lento, você deve reduzir a taxa de ingestão ou usar um endpoint com maior capacidade. Se o backlog de solicitações continuar a crescer, as operações do cliente S3 (como SOLICITAÇÕES PUT) acabarão falhando.<br><br>As solicitações do CloudMirror são mais propensas a serem afetadas pelo desempenho do endpoint de destino, pois essas solicitações geralmente envolvem mais transferência de dados do que solicitações de integração de pesquisa ou notificação de eventos. |
| Garantias de encomenda | A StorageGRID garante o pedido de operações em um objeto dentro de um site. Desde que todas as operações contra um objeto estejam dentro do mesmo local, o estado final do objeto (para replicação) sempre será igual ao estado no StorageGRID.<br><br>A StorageGRID faz o melhor esforço para solicitar solicitações quando as operações são feitas em sites da StorageGRID. Por exemplo, se você escrever um objeto inicialmente no site A e depois sobrescrever o mesmo objeto no site B, o objeto final replicado pelo CloudMirror para o bucket de destino não será garantido como o objeto mais recente. |
| Exclusões de objetos orientadas por ILM | Para corresponder ao comportamento de exclusão do AWS CRR e do Amazon Simple Notification Service, as solicitações de notificação de eventos e CloudMirror não são enviadas quando um objeto no bucket de origem é excluído devido às regras do StorageGRID ILM. Por exemplo, nenhuma solicitação de notificações do CloudMirror ou evento será enviada se uma regra ILM excluir um objeto após 14 dias.<br><br>Em contraste, as solicitações de integração de pesquisa são enviadas quando os objetos são excluídos por causa do ILM. |

| Consideração | Detalhes |
| --- | --- |
| Usando endpoints Kafka | Para endpoints Kafka, 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 de configuração do endpoint do Kafka.<br><br>A autenticação dos endpoints do Kafka usa os seguintes tipos de autenticação. Esses tipos são diferentes daqueles usados para autenticação de outros endpoints, como o Amazon SNS, e exigem credenciais de nome de usuário e senha.<br><br>• SASL/PLANÍCIE<br>• SASL/SCRAM-SHA-256<br>• SASL/SCRAM-SHA-512<br><br>**Observação:** as configurações de proxy de armazenamento configuradas não se aplicam aos pontos de extremidade dos serviços da plataforma Kafka. |

**Considerações para usar o serviço de replicação do CloudMirror**

| Consideração | Detalhes |
| --- | --- |
| Estado da replicação | O StorageGRID não suporta o `x-amz-replication-status` colhedor. |
| Tamanho do objeto | O tamanho máximo para objetos que podem ser replicados para um bucket de destino pelo serviço de replicação do CloudMirror é 5 TIB, o 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. |
| Controle de versão do bucket e IDs de versão | Se o bucket S3 de origem no StorageGRID tiver o controle de versão ativado, você também deverá habilitar o controle de versão para o bucket de destino.<br><br>Ao usar o controle de versão, observe que o pedido de versões de objetos no intervalo de destino é o melhor esforço e não é garantido pelo serviço CloudMirror, devido às limitações no protocolo S3.<br><br>**Nota**: Os IDs de versão para o bucket de origem no StorageGRID não estão relacionados com os IDs de versão para o bucket de destino. |

| Consideração | Detalhes |
| --- | --- |
| Marcação para versões de objetos | O serviço CloudMirror não replica nenhuma solicitação PutObjectTagging ou DeleteObjectTagging que forneça uma ID de versão, devido a limitações no protocolo S3. Como os IDs de versão para a origem e destino não estão relacionados, não há como garantir que uma atualização de tag para uma ID de versão específica seja replicada.<br><br>Em contraste, 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). Inests normais com tags (não marcando atualizações) também são replicados. |
| Carregamentos e valores multiparte `ETag` | Ao espelhar objetos que foram carregados usando um upload multipart, o serviço CloudMirror não preserva as peças. Como resultado, o `ETag` valor para o objeto espelhado será diferente do valor do objeto `ETag` 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 replicação do CloudMirror e a solicitação incluir os cabeçalhos de solicitação SSE-C, a operação falhará. |
| Balde com bloqueio de objetos S3 ativado | Se o intervalo S3 de destino para replicação do CloudMirror tiver o bloqueio de objetos S3 ativado, a tentativa de configurar a replicação de bucket (PutBucketReplication) falhará com um erro AccessDenied. |

## Configurar endpoints de serviços de plataforma

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

O acesso a serviços de plataforma é ativado por locatário por administrador do StorageGRID. Para criar ou usar um endpoint de serviços de plataforma, você deve ser um usuário de locatário com permissão Gerenciar endpoints ou acesso raiz, em uma grade cuja rede foi configurada para permitir que os nós de storage acessem recursos de endpoint externos. Para um único locatário, você pode configurar um máximo de 500 endpoints de serviços de plataforma. Contacte o administrador do StorageGRID para obter mais informações.

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

Ao criar um endpoint de serviços de plataforma, você especifica as informações que o 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, crie um endpoint de serviços de plataforma que inclua 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, então você deve configurar pelo menos um endpoint para cada serviço de plataforma que você planeja usar. Depois de definir um endpoint de serviços de plataforma, você usa o URN do endpoint como o destino no XML de configuração usado para ativar o serviço.

Você pode usar o mesmo ponto de extremidade que o destino para mais de um intervalo de origem. Por exemplo, você pode configurar vários buckets de origem para enviar metadados de objetos para o mesmo endpoint de integração de pesquisa para que você possa realizar pesquisas em vários buckets. Você também pode configurar um bucket de origem para usar mais de um endpoint como destino, o que permite que você faça coisas como 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.

### Endpoints para replicação do CloudMirror

O StorageGRID é compatível com pontos de extremidade de replicação que representam buckets do S3. Esses buckets podem estar hospedados no Amazon Web Services, na mesma ou em uma implantação remota do StorageGRID ou em outro serviço.

### Endpoints para notificações

O StorageGRID suporta endpoints Amazon SNS e Kafka. Os endpoints do Simple Queue Service (SQS) ou do AWS Lambda não são suportados.

Para endpoints Kafka, 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 de configuração do endpoint do Kafka.

### Endpoints para o serviço de integração de pesquisa

O StorageGRID é compatível com endpoints de integração de pesquisa que representam clusters do Elasticsearch. Esses clusters do Elasticsearch podem estar em um data center local ou hospedados em uma nuvem da AWS ou em outro lugar.

O endpoint de integração de pesquisa refere-se 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 envia metadados de objeto para o endpoint.

#### Informações relacionadas

"Administrar o StorageGRID"

### Especifique URN para endpoint de serviços de plataforma

Ao criar um endpoint de serviços de plataforma, você deve especificar um Nome de recurso exclusivo (URN). Você usará a URN para referenciar o endpoint quando criar um XML de configuração para o serviço da plataforma. A URNA para cada endpoint deve ser única.

O StorageGRID valida endpoints de serviços de plataforma à medida que os cria. Antes de criar um endpoint de serviços de plataforma, confirme se o recurso especificado no endpoint existe e se ele pode ser alcançado.

#### URNA elementos

A URNA para um endpoint de serviços de plataforma deve começar com `arn:aws` ou `urn:mysite`, da seguinte forma:

- 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 a URNA para um endpoint do CloudMirror hospedado no StorageGRID, a URNA pode começar com `urn:sgws`.

O próximo elemento da URNA especifica o tipo de serviço de plataforma, como segue:

| Serviço | Tipo |
|---|---|
| Replicação do CloudMirror | `s3` |
| Notificações | `sns` ou `kafka` |
| Integração de pesquisa | `es` |

Por exemplo, para continuar especificando a URN para um endpoint do CloudMirror hospedado no StorageGRID, você adicionaria `s3` ao GET `urn:sgws:s3`.

O elemento final da URNA identifica o recurso alvo específico no URI de destino.

| Serviço | Recurso específico |
|---|---|
| Replicação do CloudMirror | `bucket-name` |
| Notificações | `sns-topic-name` ou `kafka-topic-name` |
| Integração de pesquisa | `domain-name/index-name/type-name`<br><br>**Observação:** se o cluster Elasticsearch estiver configurado para criar índices automaticamente, você deverá criar o índice manualmente antes de criar o endpoint. |

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

Para entidades da AWS e do GCP, a URN completa é um AWS ARN válido. Por exemplo:

- Replicação do CloudMirror:

```
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 cadeia de carateres literal `domain/` , como mostrado aqui.

#### Urnas para serviços hospedados localmente

Ao usar serviços hospedados localmente em vez de serviços em nuvem, você pode especificar a URNA de qualquer forma que crie uma URNA válida e única, desde que a URNA inclua os elementos necessários na terceira e última posições. Você pode deixar os elementos indicados por opcional em branco, ou você pode especificá-los de qualquer forma que o ajude a identificar o recurso e tornar a URNA única. Por exemplo:

- Replicação do CloudMirror:

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

  Para um endpoint do CloudMirror hospedado no StorageGRID, você pode especificar uma URNA válida que começa 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 ponto final Kafka:

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-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 a URNA do endpoint seja única.

#### Criar endpoint de serviços de plataforma

Você deve criar pelo menos um endpoint do tipo correto antes de habilitar um serviço de

plataforma.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Os serviços de plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".
- O recurso referenciado pelo endpoint de serviços da plataforma foi criado:
  - Replicação do CloudMirror: Bucket do S3
  - Notificação de eventos: Tópico do Amazon Simple Notification Service (Amazon SNS) ou Kafka
  - Notificação de pesquisa: Índice Elasticsearch, se o cluster de destino não estiver configurado para criar índices automaticamente.
- Você tem as informações sobre o recurso de destino:
  - Host e porta para o URI (Uniform Resource Identifier)

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

  - Nome de recurso único (URN)

    "Especifique URN para endpoint de serviços de plataforma"

  - Credenciais de autenticação (se necessário):

**Endpoints 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

**Endpoints de replicação do CloudMirror**

Para replicação do 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 senha de chave privada do cliente opcional.

**Endpoints 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 finais 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 estiver usando um certificado de CA personalizado)

- Se os recursos de segurança do Elasticsearch estiverem ativados, você terá o privilégio de cluster do monitor para teste de conetividade e o privilégio de índice de gravação ou o Privileges de índice de índice e exclusão para atualizações de documentos.

**Passos**

1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**. A página de endpoints dos serviços da plataforma é exibida.
2. Selecione **criar endpoint**.
3. Introduza um nome de apresentação para descrever brevemente o ponto final e a respetiva finalidade.

   O tipo de serviço de plataforma que o endpoint suporta é mostrado ao lado do nome do endpoint quando ele está listado na página Endpoints, para que você não precise incluir essas informações no nome.

4. No campo **URI**, especifique o URI (Unique Resource Identifier) do endpoint.

   Use 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 (a maioria dos endpoints)
- Porta 9092 para URIs HTTPS e HTTP (somente endpoints Kafka)

Por exemplo, o URI para 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 StorageGRID high availability (HA) e `10443` representa a porta definida no ponto de extremidade do balanceador de carga.

> Sempre que possível, você deve se conectar a um grupo de HA de nós de balanceamento de carga para evitar um único ponto 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 do CloudMirror, não inclua o nome do bucket no URI. Você inclui o nome do bucket no campo **URN**.

5. Insira o Nome do recurso exclusivo (URN) para o endpoint.

> Você não pode alterar a URNA DE um endpoint depois que o endpoint foi criado.

6. Selecione **continuar**.
7. Selecione um valor para **tipo de autenticação**.

**Endpoints de integração de pesquisa**

Introduza 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 que têm a segurança desativada. | Sem autenticação. |
| Chave de acesso | Usa credenciais de estilo AWS para autenticar conexões com o destino. | • ID da chave de acesso<br>• Chave de acesso secreto |
| HTTP básico | Usa um nome de usuário e senha para autenticar conexões com o destino. | • Nome de utilizador<br>• Palavra-passe |

**Endpoints de replicação do CloudMirror**

Insira ou carregue as credenciais para um endpoint de replicação do 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 que têm a segurança desativada. | Sem autenticação. |
| Chave de acesso | Usa credenciais de estilo AWS para autenticar conexões com o destino. | • ID da chave de acesso<br>• Chave de acesso secreto |
| CAP (Portal de Acesso C2S) | Usa certificados e chaves para autenticar conexões com o destino. | • URL de credenciais temporárias<br>• Certificado CA do servidor (upload de arquivo PEM)<br>• Certificado de cliente (upload de arquivo PEM)<br>• Chave privada do cliente (upload de arquivo PEM, formato criptografado OpenSSL ou formato de chave privada não criptografado)<br>• Senha de chave privada do cliente (opcional) |

**Endpoints do Amazon SNS**

Insira ou carregue as credenciais de 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 que têm a segurança desativada. | Sem autenticação. |
| Chave de acesso | Usa credenciais de estilo AWS para autenticar conexões com o destino. | • ID da chave de acesso<br>• Chave de acesso secreto |

**Pontos finais Kafka**

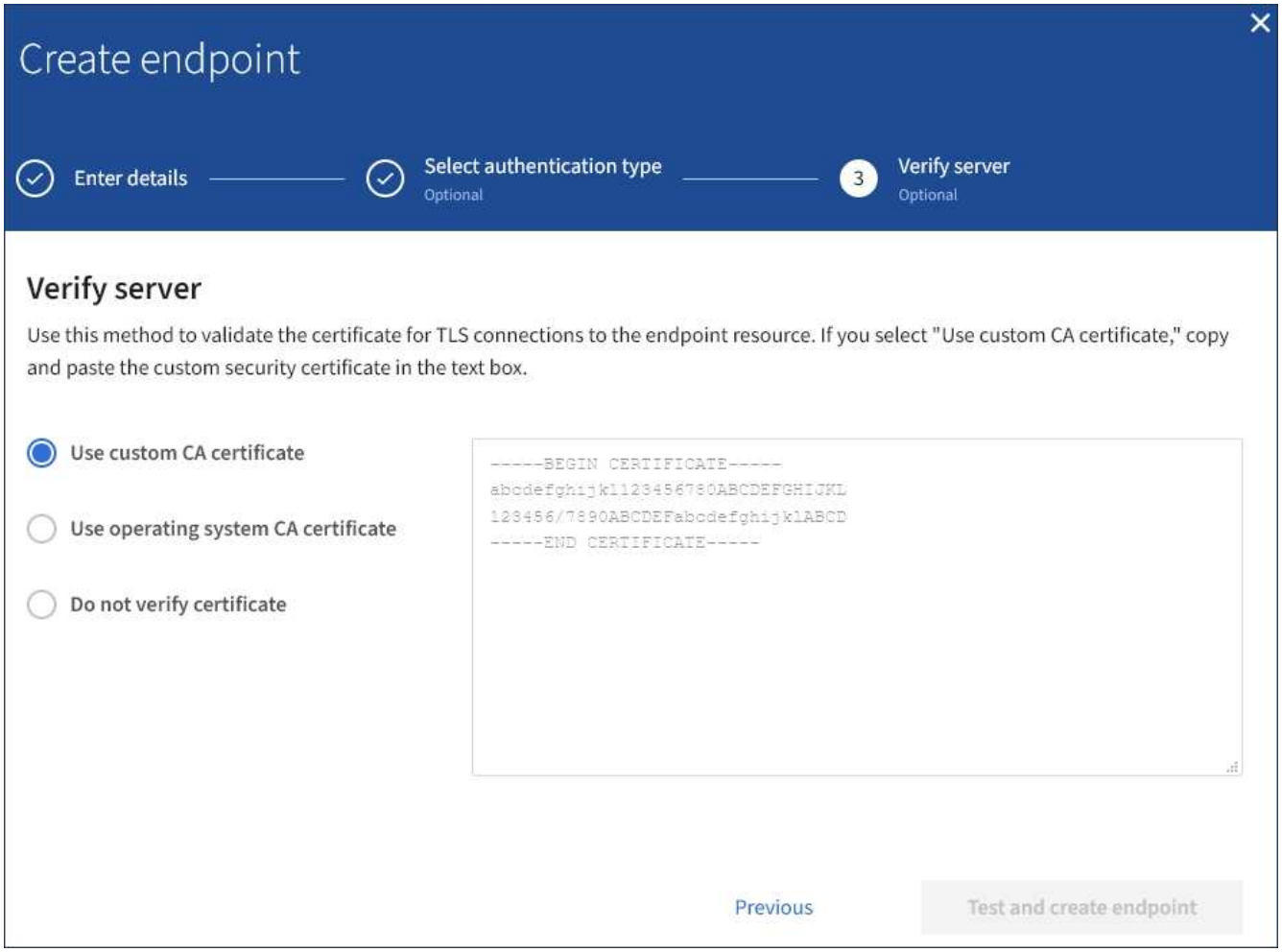
Introduza ou carregue as credenciais para um endpoint Kafka.

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 que têm a segurança desativada. | Sem autenticação. |
| SASL/PLANÍCIE | Usa um nome de usuário e senha com texto simples para autenticar conexões com o destino. | • Nome de utilizador<br>• Palavra-passe |
| SASL/SCRAM-SHA-256 | Usa um nome de usuário e senha usando um protocolo de resposta a desafios e hash SHA-256 para autenticar conexões com o destino. | • Nome de utilizador<br>• Palavra-passe |
| SASL/SCRAM-SHA-512 | Usa um nome de usuário e senha usando um protocolo de resposta a desafios e hash SHA-512 para autenticar conexões com o destino. | • Nome de utilizador<br>• Palavra-passe |

Selecione **usar autenticação de delegação tomada** se o nome de usuário e a senha forem derivados de um token de delegação obtido de um cluster Kafka.

8. Selecione **continuar**.
9. Selecione um botão de opção para **verificar servidor** para escolher como a conexão TLS com o endpoint é verificada.




| Tipo de verificação do certificado | Descrição |
|---|---|
| Use certificado CA personalizado | Use um certificado de segurança personalizado. Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto **certificado CA**. |
| Use o certificado CA do sistema operacional | Use o certificado de CA de grade padrão instalado no sistema operacional para proteger conexões. |
| Não verifique o certificado | O certificado usado para a conexão TLS não é verificado. Esta opção não é segura. |

10. Selecione **testar e criar endpoint**.
    - Uma mensagem de sucesso será exibida se o endpoint puder ser alcançado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada local.
    - Uma mensagem de erro será exibida 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. Em seguida, selecione **testar e criar endpoint**.

> A criação de endpoint falha se os serviços de plataforma não estiverem ativados para sua conta de locatário. Contacte o administrador do StorageGRID.

Depois de configurar um endpoint, você pode usar seu URN para configurar um serviço de plataforma.

**Informações relacionadas**

"Especifique URN para endpoint de serviços de plataforma"

"Configurar a replicação do CloudMirror"

"Configurar notificações de eventos"

"Configurar o serviço de integração de pesquisa"

### Teste a conexão para endpoint de serviços de plataforma

Se a conexão com um serviço de plataforma tiver sido alterada, você pode testar a conexão para que o endpoint valide que o recurso de destino existe e que ele pode ser alcançado usando as credenciais especificadas.

**Antes de começar**

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".

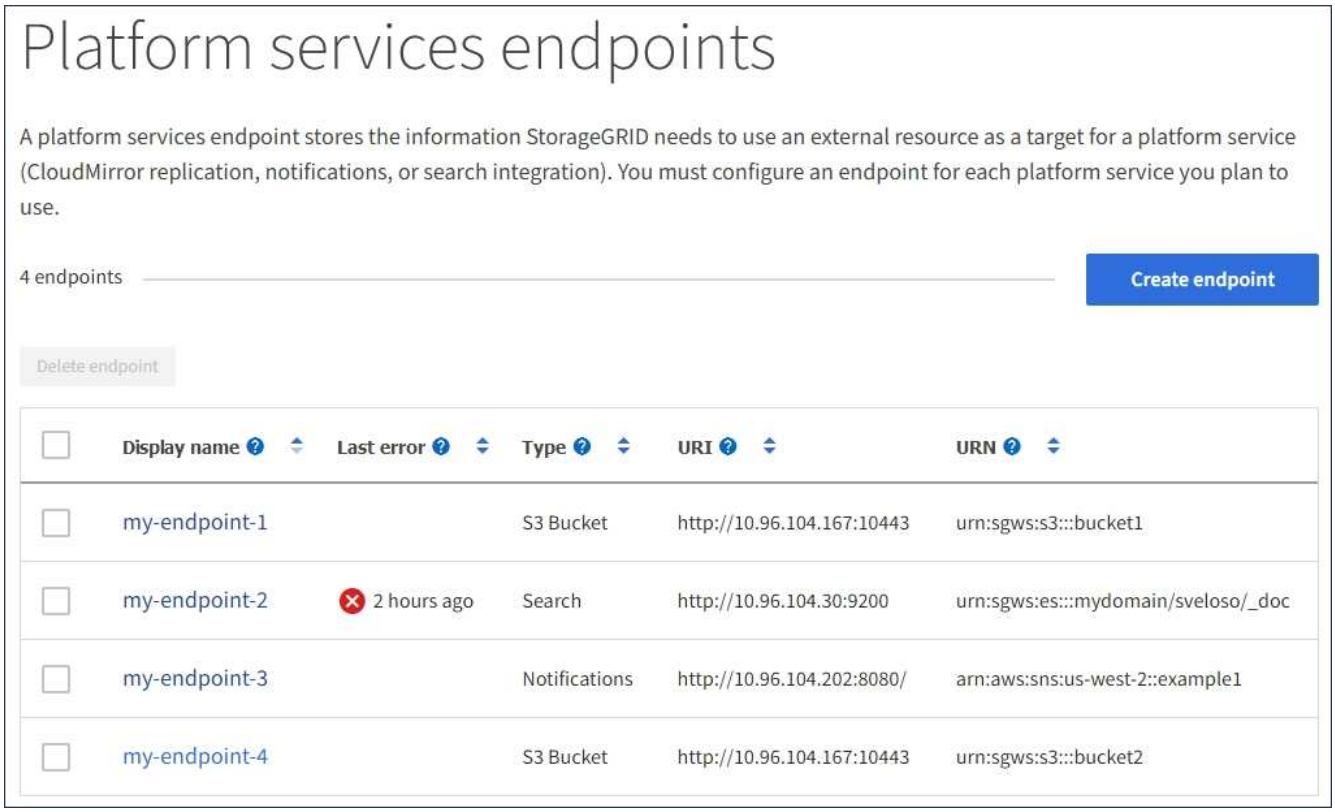
**Sobre esta tarefa**

O StorageGRID não valida se as credenciais têm as permissões corretas.

**Passos**

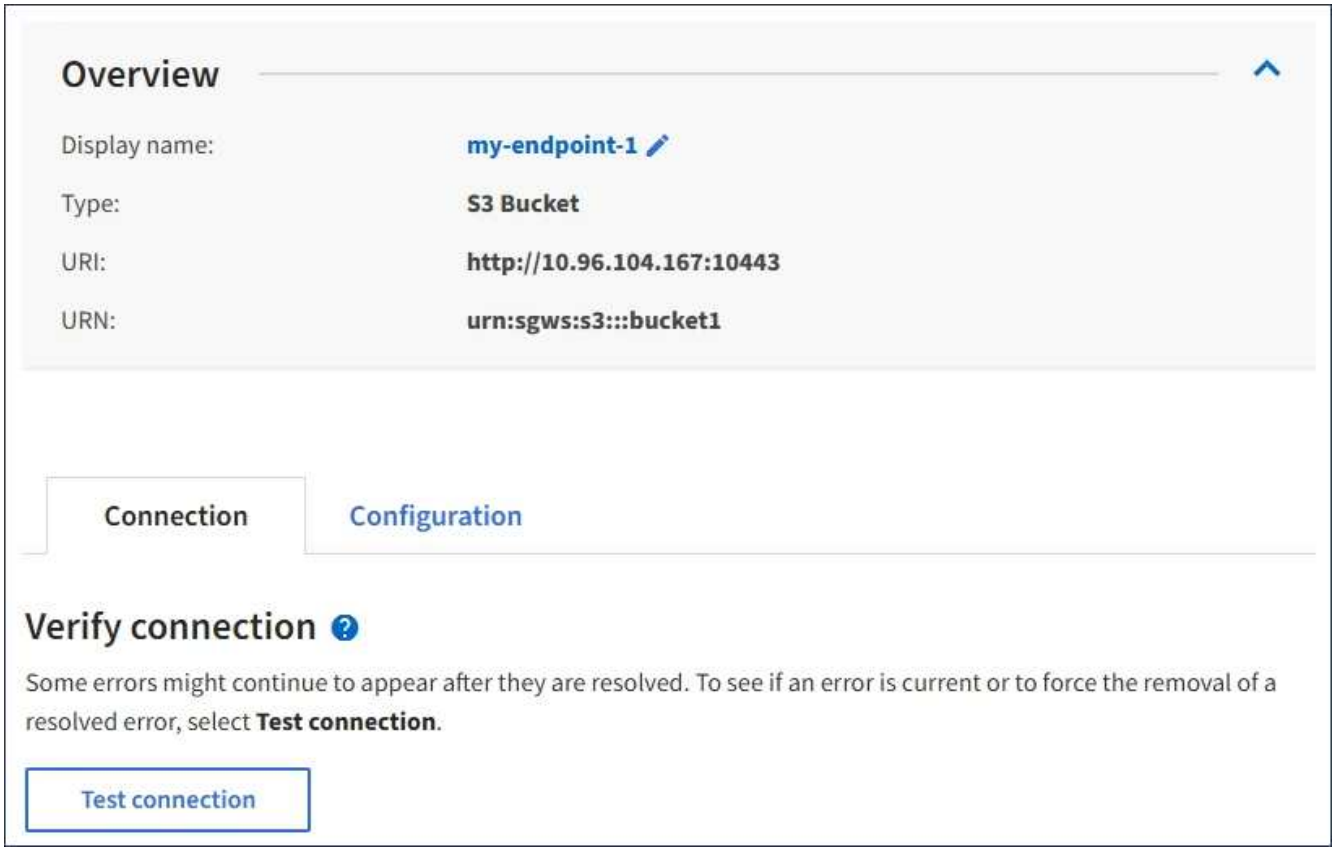
1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**.

   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.




2. Selecione o ponto final cuja ligação pretende testar.

   A página de detalhes do ponto final é exibida.




3. Selecione **Test Connection**.

- Uma mensagem de sucesso será exibida se o endpoint puder ser alcançado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada local.
- Uma mensagem de erro será 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 endpoint de serviços de plataforma

Você pode editar a configuração de um endpoint de serviços de plataforma para alterar seu nome, URI ou outros detalhes. Por exemplo, talvez seja necessário atualizar credenciais expiradas ou alterar o URI para apontar para um índice de backup do Elasticsearch para failover. Não é possível alterar a URN para um endpoint de serviços de plataforma.

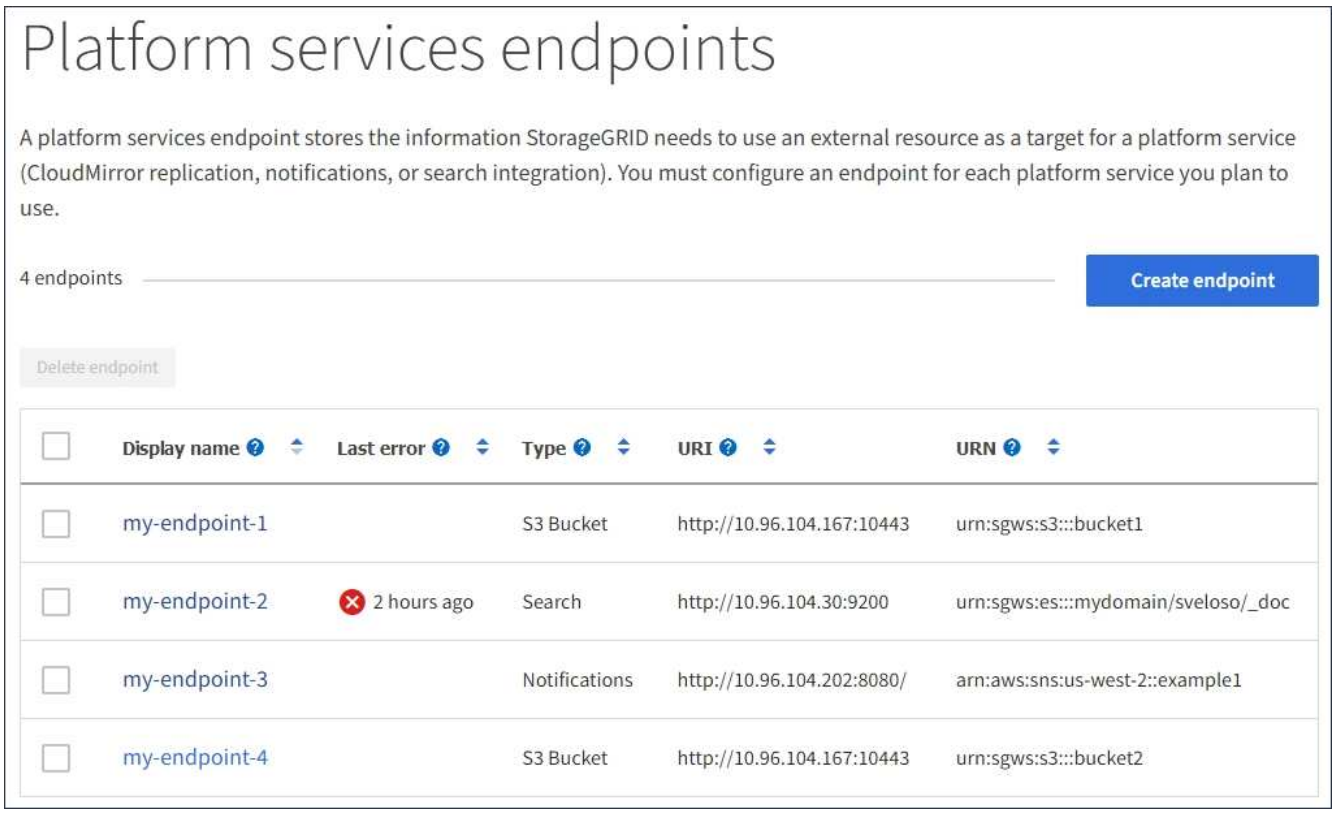
#### Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".

#### Passos

1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**.

   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.




2. Selecione o ponto de extremidade que pretende editar.

   A página de detalhes do ponto final é exibida.

3. Selecione **Configuração**.
4. Conforme necessário, altere a configuração do endpoint.

   Você não pode alterar a URNA DE um endpoint depois que o endpoint foi criado.

   a. Para alterar o nome de exibição do endpoint, selecione o ícone de edição .
   b. Conforme necessário, altere o URI.
   c. Conforme necessário, altere o tipo de autenticação.
      - Para autenticação da chave de acesso, altere a chave conforme necessário selecionando **Editar chave S3** e colando uma nova ID de chave de acesso e chave de acesso secreta. Se você precisar cancelar suas alterações, selecione **Reverter S3 key edit**.
      - Para autenticação CAP (C2S Access Portal), altere a URL de credenciais temporárias ou a senha de chave privada do cliente opcional e carregue novos arquivos de certificado e chave conforme necessário.

        A chave privada do cliente deve estar no formato encriptado OpenSSL ou no formato de chave privada não encriptada.

   d. Conforme necessário, altere o método para verificar o servidor.
5. Selecione **Teste e salve as alterações**.
   - Uma mensagem de sucesso será exibida se o endpoint puder ser alcançado usando as credenciais especificadas. A conexão com o endpoint é verificada a partir de um nó em cada local.
   - Uma mensagem de erro será exibida se a validação do endpoint falhar. Modifique o ponto final para corrigir o erro e selecione **testar e salvar alterações**.

### Excluir endpoint de serviços de plataforma

Você pode excluir um endpoint se não quiser mais usar o serviço de plataforma associado.

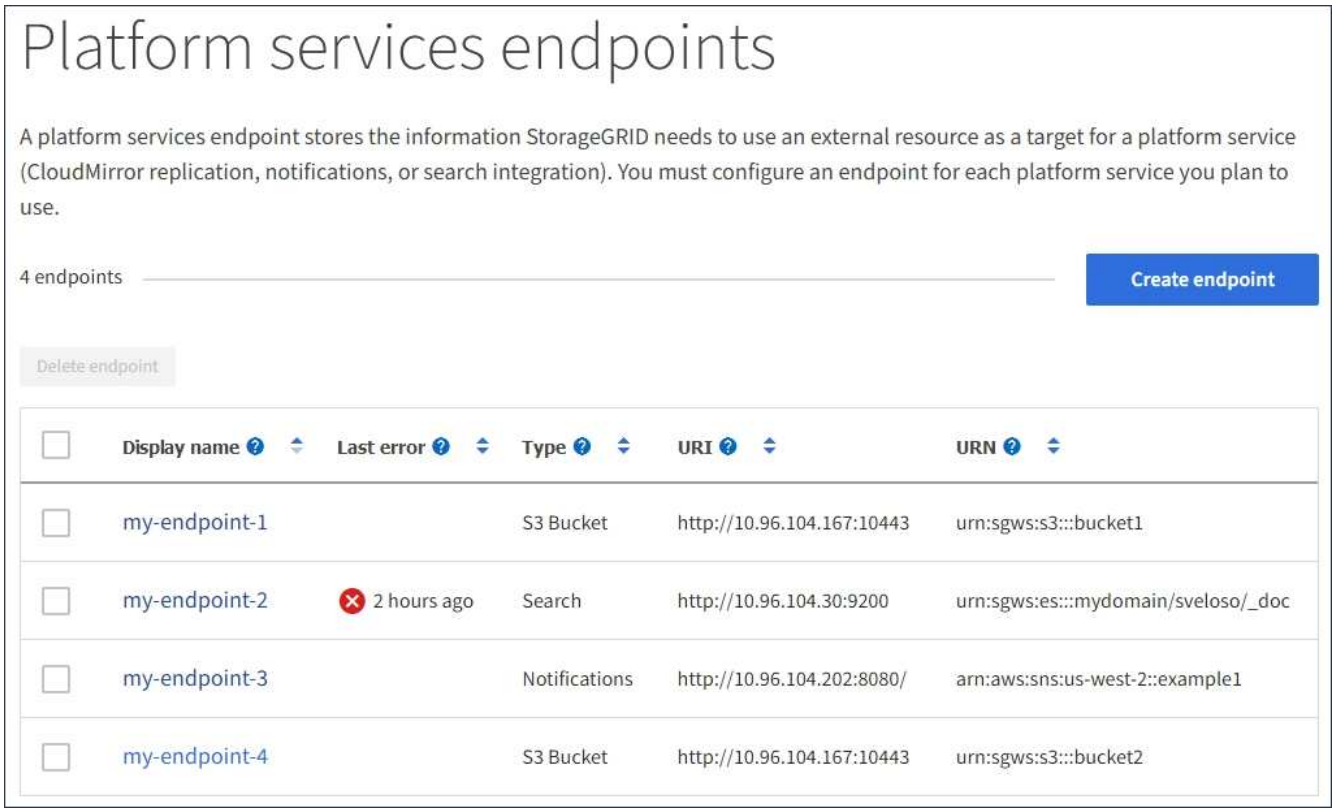
#### Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".

#### Passos

1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**.

   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.

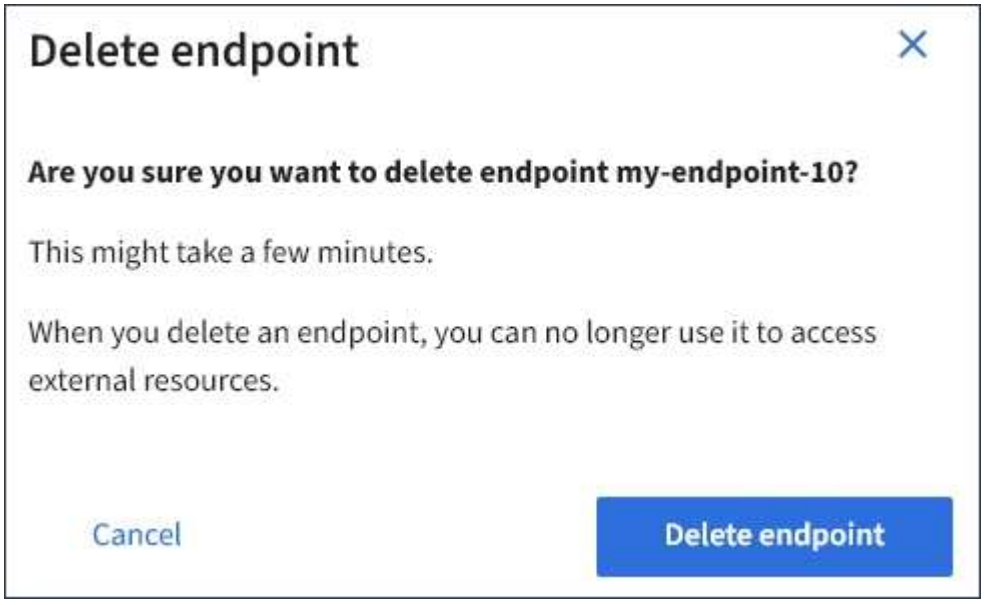



2. Selecione a caixa de verificação para cada ponto de extremidade que pretende eliminar.

> Se você excluir um endpoint de serviços de plataforma que está em uso, o serviço de plataforma associado será desativado para quaisquer buckets que usam o endpoint. Quaisquer solicitações que ainda não foram concluídas serão descartadas. Todas as novas solicitações continuarão sendo geradas até que você altere a configuração do bucket para não fazer mais referência à URNA excluída. O StorageGRID reportará essas solicitações como erros irrecuperáveis.

3. Selecione **ações** > **Excluir endpoint**.

   É apresentada uma mensagem de confirmação.



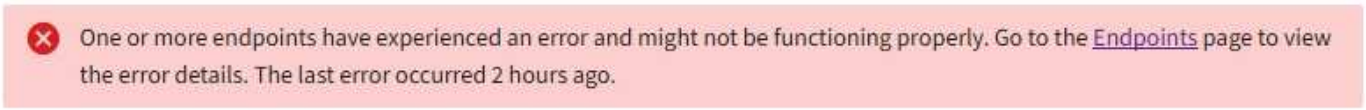
4. Selecione **Excluir endpoint**.

### Solucionar erros de endpoint dos serviços da plataforma

Se ocorrer um erro quando o StorageGRID tenta se comunicar com um endpoint de serviços de plataforma, uma mensagem é exibida no painel. Na página pontos finais dos serviços da plataforma, a coluna último erro indica quanto tempo atrás o erro ocorreu. Nenhum erro é exibido se as permissões associadas às credenciais de um endpoint estiverem incorretas.

#### Determine se ocorreu um erro

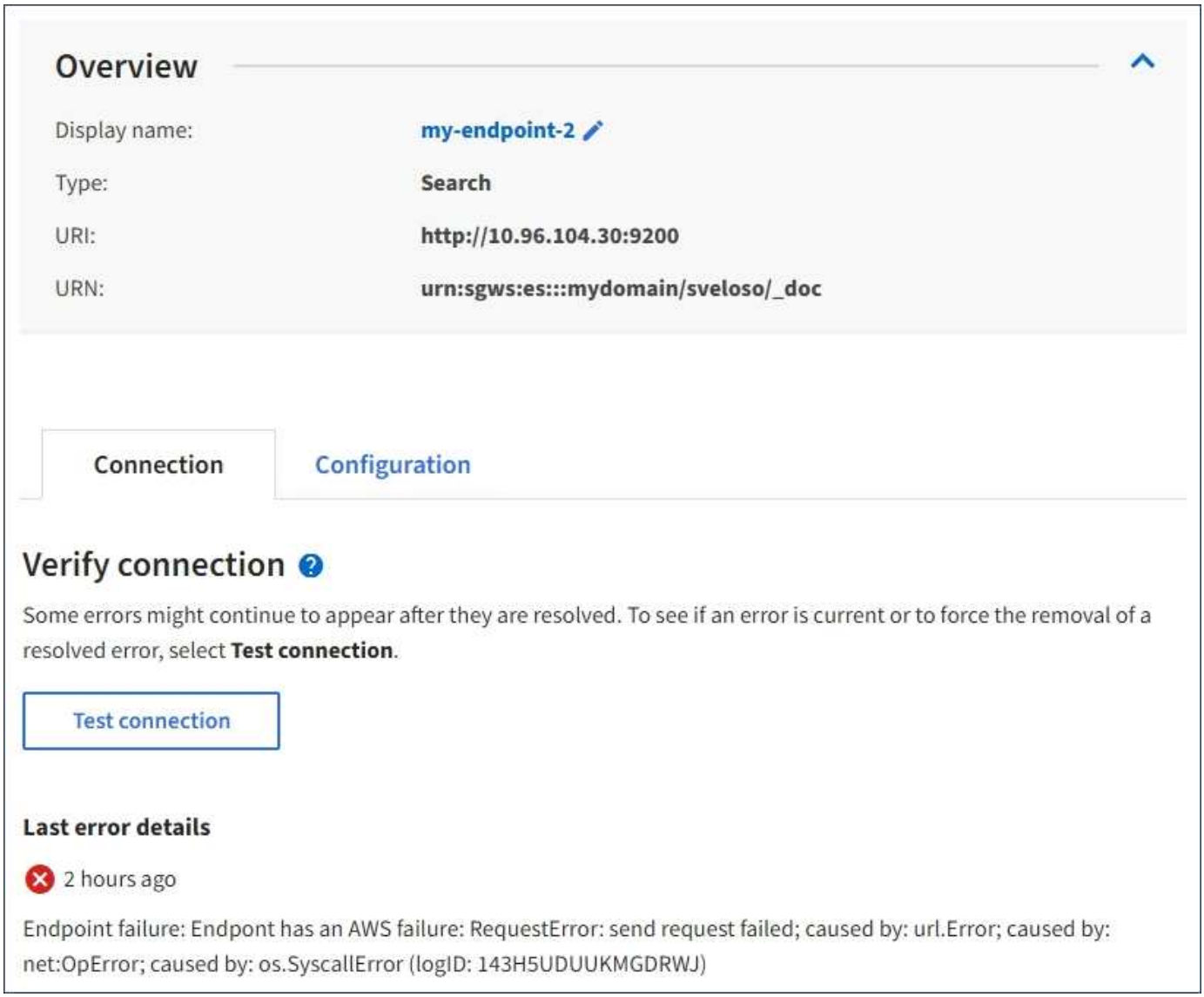
Se algum erro de endpoint de serviços de plataforma tiver ocorrido nos últimos 7 dias, o painel do Gerenciador do Locatário exibirá uma mensagem de alerta. Você pode acessar a página de endpoints dos serviços da plataforma para ver mais detalhes sobre o erro.




O mesmo erro que aparece no painel também aparece na parte superior da página de endpoints dos serviços da plataforma. Para ver uma mensagem de erro mais detalhada:

**Passos**

1. Na lista de endpoints, selecione o endpoint que tem o erro.
2. Na página de detalhes do endpoint, selecione **conexão**. Esta guia exibe apenas o erro mais recente para um endpoint e indica quanto tempo atrás o erro ocorreu. Erros que incluem o ícone X vermelho  ocorreram nos últimos 7 dias.




#### Verifique se o erro ainda está atual

Alguns erros podem continuar a ser mostrados na coluna **último erro** mesmo depois de resolvidos. Para ver se um erro é atual ou forçar a remoção de um erro resolvido da tabela:

**Passos**

1. Selecione o ponto final.

   A página de detalhes do ponto final é exibida.

2. Selecione **Connection** > **Test Connection**.

Selecionar **testar conexão** faz com que o StorageGRID valide que o endpoint dos serviços da plataforma existe e que ele pode ser alcançado com as credenciais atuais. A conexão com o endpoint é validada a partir de um nó em cada local.

#### 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 de espelhamento de nuvem pode ocorrer se o StorageGRID não conseguir acessar o

bucket do destino S3 porque ele não tem as permissões de acesso corretas ou a chave de acesso expirou. A mensagem é "as credenciais de endpoint ou o acesso de destino precisa ser atualizado", e os detalhes são "AccessDenied" ou "InvalidAccessKeyId".

Se você precisar editar o endpoint para resolver um erro, selecionar **testar e salvar alterações** faz com que o StorageGRID valide o endpoint atualizado e confirme que ele pode ser alcançado com as credenciais atuais. A conexão com o endpoint é validada a partir de um nó em cada local.

**Passos**

1. Selecione o ponto final.
2. Na página de detalhes do endpoint, selecione **Configuração**.
3. Edite a configuração do endpoint conforme necessário.
4. Selecione **Connection** > **Test Connection**.

#### Credenciais de endpoint com permissões insuficientes

Quando o StorageGRID valida um endpoint de serviços de plataforma, ele confirma que as credenciais do endpoint podem ser usadas para entrar em Contato com o recurso de destino e faz uma verificação básica de permissões. No entanto, o StorageGRID não valida todas as permissões necessárias para determinadas operações de serviços de plataforma. Por esse motivo, se você receber um erro ao tentar usar um serviço de plataforma (como "403 proibido"), verifique as permissões associadas às credenciais do endpoint.

**Informações relacionadas**

- **Administrar o StorageGRID › solucionar problemas de serviços da plataforma**
- "Criar endpoint de serviços de plataforma"
- "Teste a conexão para endpoint de serviços de plataforma"
- "Editar endpoint de serviços de plataforma"

## Configurar a replicação do CloudMirror

O "Serviço de replicação do CloudMirror" é um dos três serviços de plataforma StorageGRID. Você pode usar a replicação do CloudMirror para replicar automaticamente objetos para um bucket externo do S3.

**Antes de começar**

- Os serviços de plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket para agir como a origem de replicação.
- O endpoint que você pretende usar como destino para a replicação do CloudMirror já existe e você tem sua URN.
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador do locatário.

**Sobre esta tarefa**

A replicação do CloudMirror copia objetos de um bucket de origem para um bucket de destino especificado em um endpoint.

A replicação do CloudMirror tem semelhanças e diferenças importantes com o recurso de replicação entre grades. Para saber mais, "Compare a replicação entre redes e a replicação do CloudMirror"consulte .

Para ativar a replicação do CloudMirror para um bucket, você deve criar e aplicar um XML de configuração de replicação de bucket válido. O XML de configuração de replicação deve usar a URN de um endpoint de bucket do S3 para cada destino.

A replicação não é suportada para buckets de origem ou destino com o bloqueio de objetos S3 ativado.

Para obter informações gerais sobre replicação de bucket e como configurá-la, "Documentação do Amazon Simple Storage Service (S3): Replicação de objetos" consulte . Para obter informações sobre como o StorageGRID implementa o GetBucketReplication, DeleteBucketReplication e o PutBucketReplication, consulte o "Operações em baldes".

Se você habilitar a replicação do CloudMirror em um bucket que contém objetos, novos objetos adicionados ao bucket serão replicados, mas os objetos existentes no bucket não serão replicados. Você deve atualizar objetos existentes para acionar a replicação.

Se você especificar uma classe de armazenamento no XML de configuração de replicação, o StorageGRID usará essa classe ao executar operações no endpoint S3 de destino. O endpoint de destino também deve suportar a classe de armazenamento especificada. Certifique-se de seguir quaisquer recomendações fornecidas pelo fornecedor do sistema de destino.

**Passos**

1. Habilite a replicação para o bucket de origem:

   Use um editor de texto para criar a configuração de replicação XML necessária para habilitar a replicação, conforme especificado na API de replicação S3. Ao configurar o XML:

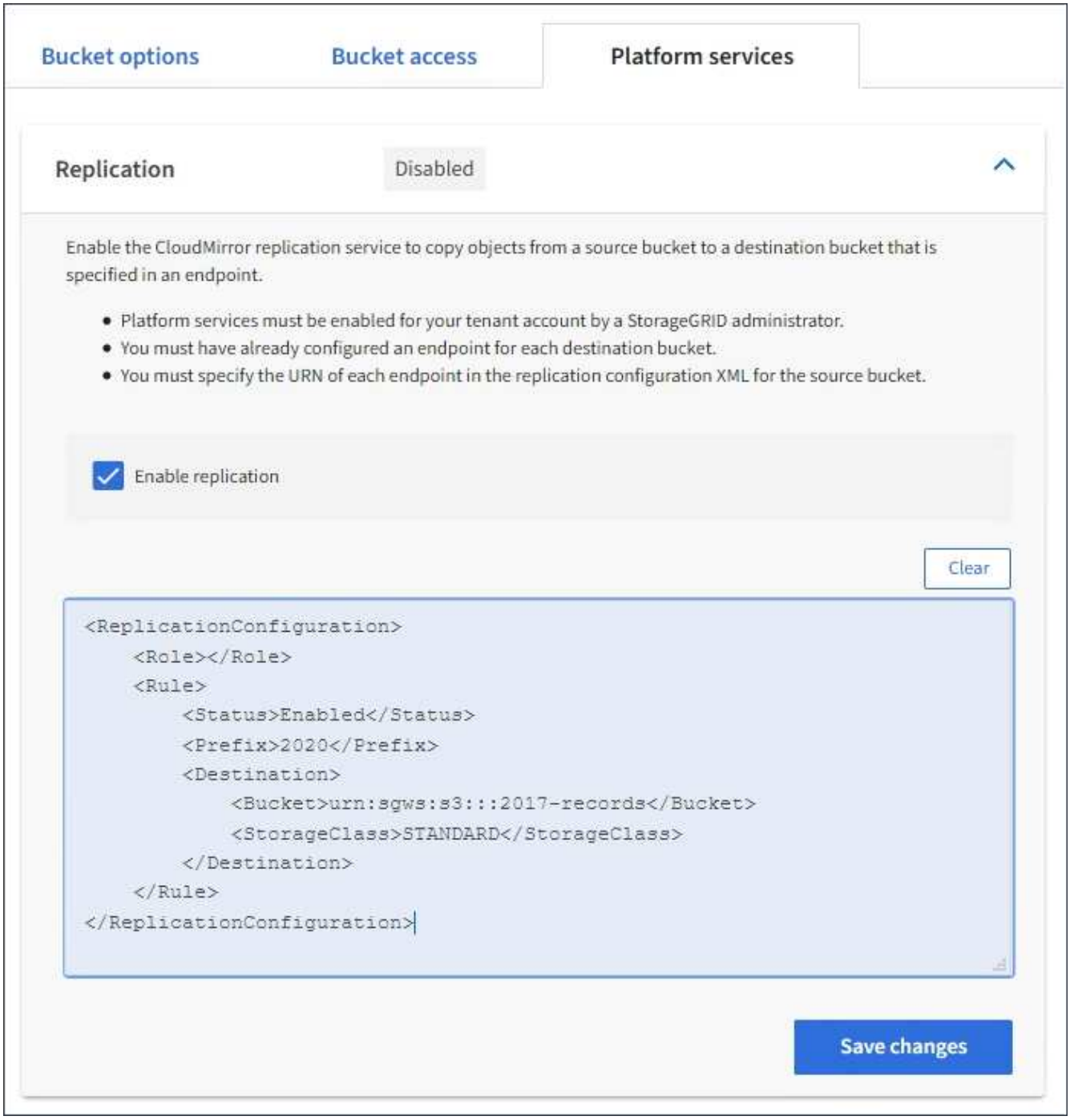
   - Observe que o StorageGRID só suporta V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue convenções V1 para exclusão de versões de objetos. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes.
   - Use a URNA de um endpoint de bucket S3 como o 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 será usada.
     - `STANDARD_IA`: (Standard - Acesso não frequente.) Use essa classe de storage para dados acessados com menos frequência, mas que ainda exigem acesso rápido quando necessário.
     - `REDUCED_REDUNDANCY`: Use esta classe de armazenamento para dados não críticos e reprodutíveis 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. Este valor não é utilizado 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 **View buckets** no painel ou selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do intervalo de origem.

   É apresentada a página de detalhes do balde.

4. Selecione **Serviços de plataforma** > **replicação**.
5. Marque a caixa de seleção **Ativar replicação**.
6. Cole o XML de configuração de replicação na caixa de texto e selecione **Salvar alterações**.




Os serviços de plataforma devem estar habilitados para cada conta de locatário por um administrador do StorageGRID usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Contacte o administrador do StorageGRID se ocorrer um erro ao guardar 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, conforme especificado 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 intervalo de destino.

Para objetos pequenos, a replicação acontece rapidamente.

**Informações relacionadas**

"Criar endpoint de serviços de plataforma"

## Configurar notificações de eventos

O serviço de notificações é um dos três serviços da plataforma StorageGRID. Você pode habilitar notificações de um bucket para enviar informações sobre eventos especificados para um cluster ou serviço do Kafka de destino que suporte o AWS Simple Notification Service (Amazon SNS).

**Antes de começar**

- Os serviços de plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket para agir como a fonte das notificações.
- O endpoint que você pretende usar como destino para notificações de eventos já existe, e você tem sua URNA.
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador do locatário.

**Sobre esta tarefa**

Depois de configurar notificações de eventos, sempre que um evento especificado ocorre para um objeto no bucket de origem, uma notificação é gerada e enviada para o tópico Amazon SNS ou Kafka usado como o endpoint de destino. Para ativar notificações para um bucket, você deve criar e aplicar XML de configuração de notificação válida. O XML de configuração de notificação deve usar a URNA de um endpoint de notificações de eventos para cada destino.

Para obter informações gerais sobre notificações de eventos e como configurá-las, consulte a documentação da Amazon. Para obter informações sobre como o StorageGRID implementa a API de configuração de notificação de bucket do S3, consulte o "Instruções para a implementação de aplicativos cliente S3".

Se você ativar notificações de eventos para um bucket que contém objetos, as notificações serão enviadas apenas para ações executadas após a configuração de notificação ser salva.

**Passos**

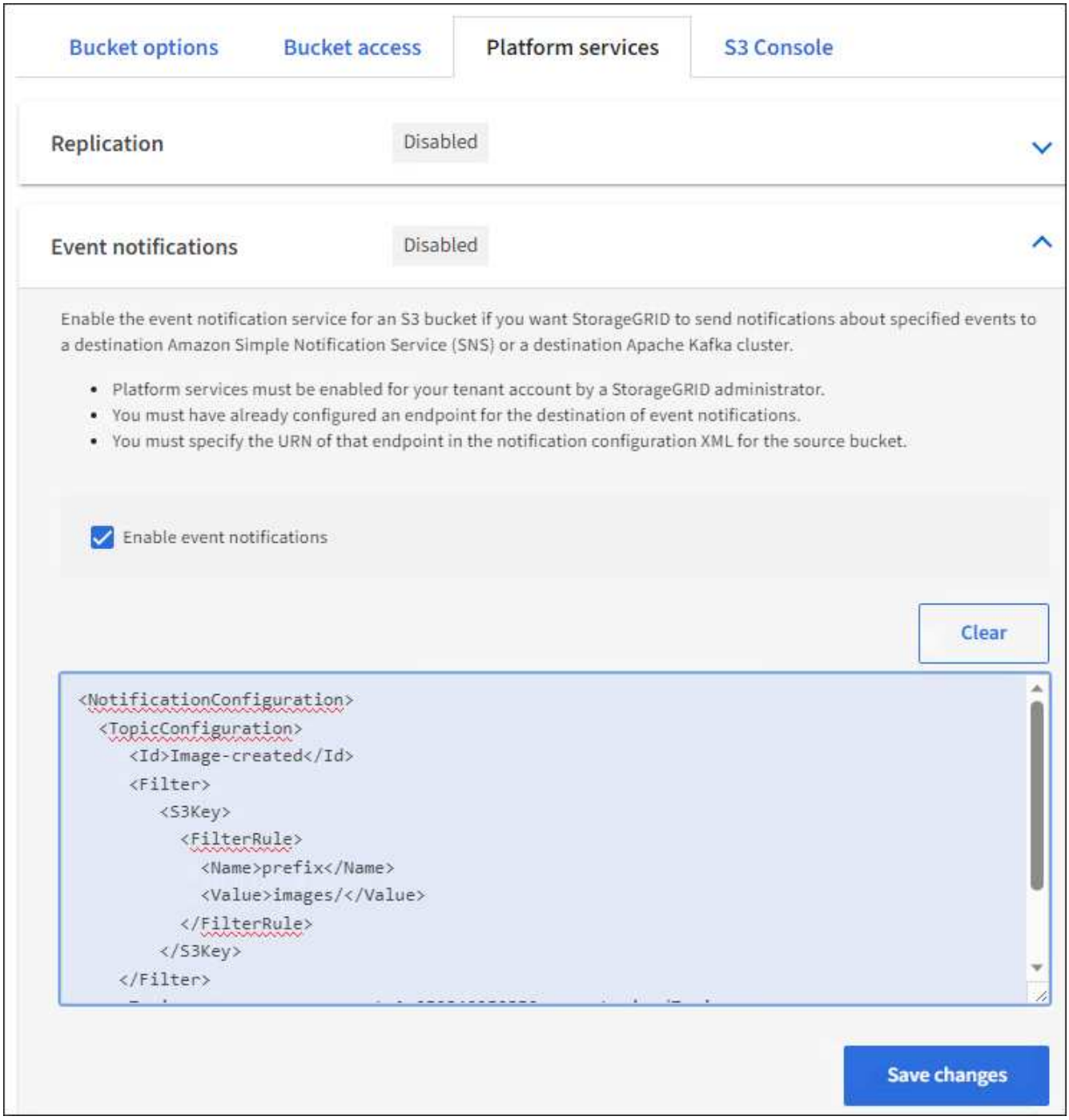
1. Ativar notificações para o intervalo de origem:
    - Use um editor de texto para criar a configuração de notificação XML necessário para habilitar notificações de eventos, conforme especificado na API de notificação S3.
    - Ao configurar o XML, use a URNA de um endpoint de notificações de eventos 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 Gerenciador do Locatário, selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do intervalo de origem.

   É apresentada a página de detalhes do balde.

4. Selecione **Serviços de plataforma** > **notificações de eventos**.
5. Marque 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 de plataforma devem estar habilitados para cada conta de locatário por um administrador do StorageGRID usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Contacte o administrador do StorageGRID se ocorrer um erro ao guardar 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 se uma notificação foi entregue ao tópico do Amazon SNS ou Kafka de destino.

Por exemplo, se o tópico de destino estiver hospedado no Amazon SNS, você poderá 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 êxito o bucket de origem para notificações do StorageGRID.

**Informações relacionadas**

"Entenda as notificações para buckets"

"USE A API REST DO S3"

"Criar endpoint de serviços de plataforma"

## Use o serviço de integração de pesquisa

O serviço de integração de pesquisa é um dos três serviços da plataforma StorageGRID. Você pode habilitar esse serviço para enviar metadados de objetos para um índice de pesquisa de destino sempre que um objeto for criado, excluído ou seus metadados ou tags forem atualizados.

Você pode configurar a integração de pesquisa usando o Gerenciador de inquilinos para aplicar XML de configuração personalizada do StorageGRID a um bucket.

> Como o serviço de integração de pesquisa faz com que os metadados de objeto sejam enviados para um destino, seu XML de configuração é chamado de configuração de notificação de *metadata XML*. Esse XML de configuração é diferente da configuração *notificação XML* usada para ativar notificações de eventos.

Consulte o "Instruções para a implementação de aplicativos cliente S3" para obter detalhes sobre as seguintes operações personalizadas da API REST do StorageGRID S3:

- ELIMINAR configuração de notificação de metadados do bucket
- OBTER configuração de notificação de metadados do bucket
- COLOQUE a configuração de notificação de metadados do bucket

**Informações relacionadas**

"Configuração XML para integração de pesquisa"

"Metadados de objetos incluídos nas notificações de metadados"

"JSON gerado pelo serviço de integração de pesquisa"

"Configurar o serviço de integração de pesquisa"

"USE A API REST DO S3"

### Configuração XML para integração de pesquisa

O serviço de integração de pesquisa é configurado usando um conjunto de regras contidas nas `<MetadataNotificationConfiguration>` tags e `</MetadataNotificationConfiguration>` . Cada regra especifica os objetos aos quais a regra se aplica e o destino ao qual o StorageGRID deve enviar os metadados desses objetos.

Os objetos podem ser filtrados no prefixo do nome do objeto. Por exemplo, você pode enviar metadados para objetos com o prefixo `images` para um destino e metadados para objetos com o prefixo `videos` para outro. As configurações que têm prefixos sobrepostos não são válidas e são rejeitadas quando são enviadas. Por exemplo, uma configuração que inclua uma regra para objetos com o prefixo `test` e uma segunda regra para

objetos com o prefixo `test2` não é permitida.

Os destinos devem ser especificados usando a URNA de um endpoint StorageGRID que foi criado para o serviço de integração de pesquisa. Esses endpoints referem-se a um índice e tipo definidos em um cluster do Elasticsearch.

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

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

| Nome | Descrição | Obrigatório |
|---|---|---|
| MetadataNotificationConfiguration | Tag de contentor para regras usadas para especificar os objetos e o destino para notificações de metadados.<br><br>Contém um ou mais elementos de regra. | Sim |
| Regra | Tag container para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado.<br><br>Regras com prefixos sobrepostos são rejeitadas.<br><br>Incluído no elemento MetadataNotificationConfiguration. | Sim |
| ID | Identificador exclusivo para a regra.<br><br>Incluído no elemento regra. | Não |

| Nome | Descrição | Obrigatório |
| --- | --- | --- |
| Estado | O estado pode ser "ativado" ou "Desativado". Nenhuma ação é tomada para regras que são desativadas.<br><br>Incluído no elemento regra. | 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 regra. | Sim |
| Destino | Etiqueta de contentor para o destino de uma regra.<br><br>Incluído no elemento regra. | Sim |
| Urna | URNA do destino onde os metadados do objeto são enviados. Deve ser a URNA de um endpoint StorageGRID com as seguintes propriedades:<br><br>• `es` deve ser o terceiro elemento.<br>• A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário `domain-name/myindex/mytype`.<br><br>Os endpoints são configurados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário. Eles assumem a seguinte forma:<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 que o XML de configuração seja enviado, ou a configuração falhará com um erro 404.<br><br>URNA está incluído no elemento destino. | Sim |

Use o XML de configuração de notificação de metadados de amostra para aprender a construir seu próprio XML.

#### Configuração de notificação de metadados que se aplica a todos os objetos

Neste exemplo, metadados de objetos para todos os 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>
```

#### Configuração de notificação de metadados com duas regras

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

```
<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>
```

**Informações relacionadas**

"USE A API REST DO S3"

"Metadados de objetos incluídos nas notificações de metadados"

"JSON gerado pelo serviço de integração de pesquisa"

"Configurar o serviço de integração de pesquisa"

### Configure o serviço de integração de pesquisa

O serviço de integração de pesquisa envia metadados de objetos para um índice de pesquisa de destino sempre que um objeto é criado, excluído ou seus metadados ou tags são atualizados.

#### Antes de começar

- Os serviços de plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket do 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 tem sua URNA.
- Você pertence a um grupo de usuários que tem o "Gerencie todos os buckets ou permissão de acesso root". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador do locatário.

#### Sobre esta tarefa

Depois de configurar o serviço de integração de pesquisa para um bucket de origem, criar um objeto ou atualizar metadados ou tags de um objeto aciona metadados de objeto para serem enviados 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 objetos existentes. Você deve atualizar esses objetos existentes para garantir que seus metadados sejam adicionados ao índice de pesquisa de destino.

#### Passos

1. Use um editor de texto para criar o XML de notificação de metadados necessário para habilitar a integração de pesquisa.
   - Consulte as informações sobre o XML de configuração para integração de pesquisa.
   - Ao configurar o XML, use a URNA de um endpoint de integração de pesquisa como o destino.

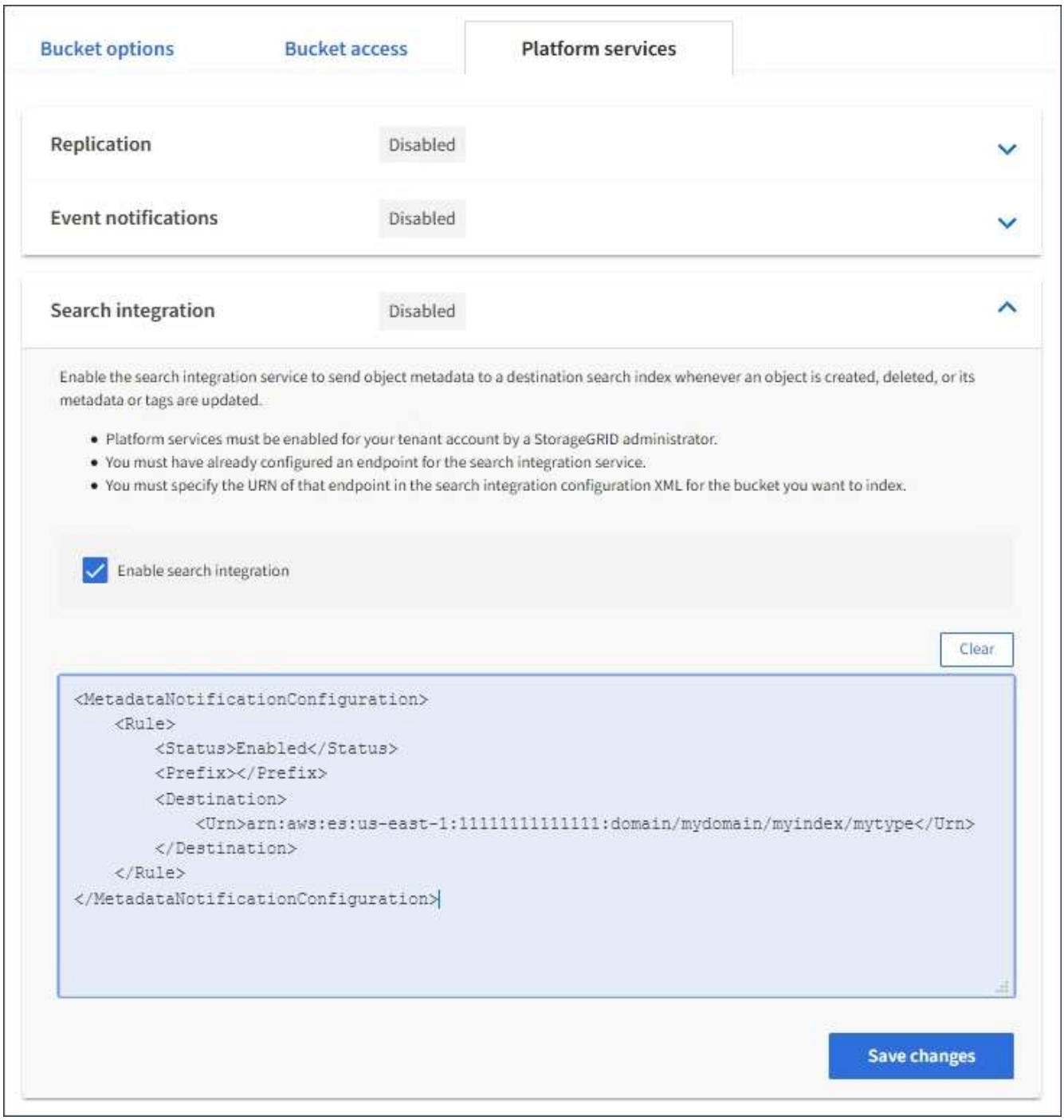
```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. No Gerenciador do Locatário, selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do intervalo de origem.

   É apresentada a página de detalhes do balde.

4. Selecione **Platform services** > **Search integration**

5. Marque a caixa de seleção **Ativar integração de pesquisa**.
6. Cole a configuração de notificação de metadados na caixa de texto e selecione **Salvar alterações**.




Os serviços de plataforma devem estar habilitados para cada conta de locatário por um administrador do StorageGRID usando o Gerenciador de Grade ou a API de gerenciamento. Contacte o administrador do StorageGRID se ocorrer um erro ao guardar 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 que contém metadados e tags do objeto foi adicionado ao índice de pesquisa especificado no endpoint.

**Depois de terminar**

Conforme 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** (Ativar integração de pesquisa).
- Se você estiver usando a API do S3 diretamente, use uma solicitação de notificação de metadados de DELETE Bucket. Consulte as instruções para a implementação de aplicativos cliente S3.

**Informações relacionadas**

"Compreender o serviço de integração de pesquisa"

"Configuração XML para integração de pesquisa"

"USE A API REST DO S3"

"Criar endpoint de serviços de plataforma"

**JSON gerado pelo serviço de integração de pesquisa**

Quando você ativa o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado para o endpoint de destino cada vez que metadados ou tags de objeto são adicionados, atualizados ou excluídos.

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

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

#### Metadados de objetos incluídos nas notificações de metadados

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

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

| Tipo | Nome e descrição do item |
|---|---|
| Informações sobre o balde e o objeto | `bucket`: Nome do balde |
| `key`: Nome da chave do objeto | `versionID`: Versão do objeto, para objetos em buckets versionados |
| `region`: Região do balde, por exemplo `us-east-1` | Metadados do sistema |
| `size`: Tamanho do objeto (em bytes) como visível para um cliente HTTP | `md5`: Hash de objeto |
| Metadados do usuário | `metadata`: Todos os metadados de usuário para o objeto, como pares de chave-valor<br><br>`key:value` |
| Tags | `tags`: Todas as tags de objeto definidas para o objeto, como pares chave-valor<br><br>`key:value` |

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

## Informações sobre direitos autorais



## Informações sobre marcas comerciais