# 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.

Opcionalmente, 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 Instruções para a implementação de aplicativos cliente S3.

- * 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 as seguintes informações:

- Nome de exibição para o locatário (o ID da conta do locatário é atribuído automaticamente e não pode ser alterado).
- Se a conta de locatário usará o S3 ou Swift.
- Para contas de inquilino S3: Se a conta de inquilino tem permissão para usar serviços de plataforma. Se o uso de serviços de plataforma for permitido, a grade deve ser configurada para suportar seu uso.
- Opcionalmente, uma cota de armazenamento para a conta de locatário - o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos do locatário. A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco).
- Se a federação de identidade estiver ativada para o sistema StorageGRID, qual grupo federado tem permissão de acesso root para configurar a conta de locatário.
- Se o logon único (SSO) não estiver em uso para o sistema StorageGRID, se a conta do locatário usará sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.

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:

- Configurando a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) ou criando grupos e usuários locais
- Gerenciando chaves de acesso S3
- Criação e gerenciamento de buckets do S3, incluindo buckets em conformidade
- Usando serviços de plataforma (se ativado)
- Monitoramento do uso do storage

> Embora você possa criar e gerenciar buckets do S3 com o Gerenciador do locatário, você precisa ter S3 teclas de acesso e usar a API REST do S3 para ingerir e gerenciar objetoso .

#### 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:

- Configurando a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e criando grupos e usuários locais
- Monitoramento do 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.

### Use o Gerenciador do Locatário

O Gerenciador do Locatário permite gerenciar todos os aspetos de uma conta de locatário do StorageGRID.

Você pode usar o Gerenciador do locatário para monitorar o uso do armazenamento de uma conta de locatário e gerenciar usuários com federação de identidade ou criando grupos e usuários locais. Para contas de locatários do S3, você também pode gerenciar chaves do S3, gerenciar buckets do S3 e configurar serviços de plataforma.

# 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.

**O que você vai precisar**

- Tem de ter as suas credenciais de início de sessão.
- Você deve ter 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 contém o nome de domínio totalmente qualificado (FQDN) ou o endereço IP usado para acessar um nó de administração e, opcionalmente, também pode incluir um número de porta, o ID da conta de locatário de 20 dígitos ou ambos.

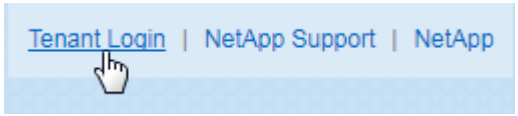
- Se o URL não incluir o ID de conta de 20 dígitos do locatário, você deve ter esse ID de conta.
- Você deve estar usando um navegador da web suportado.
- Os cookies devem estar ativados no seu navegador.
- Você deve ter permissões de acesso específicas.

**Passos**

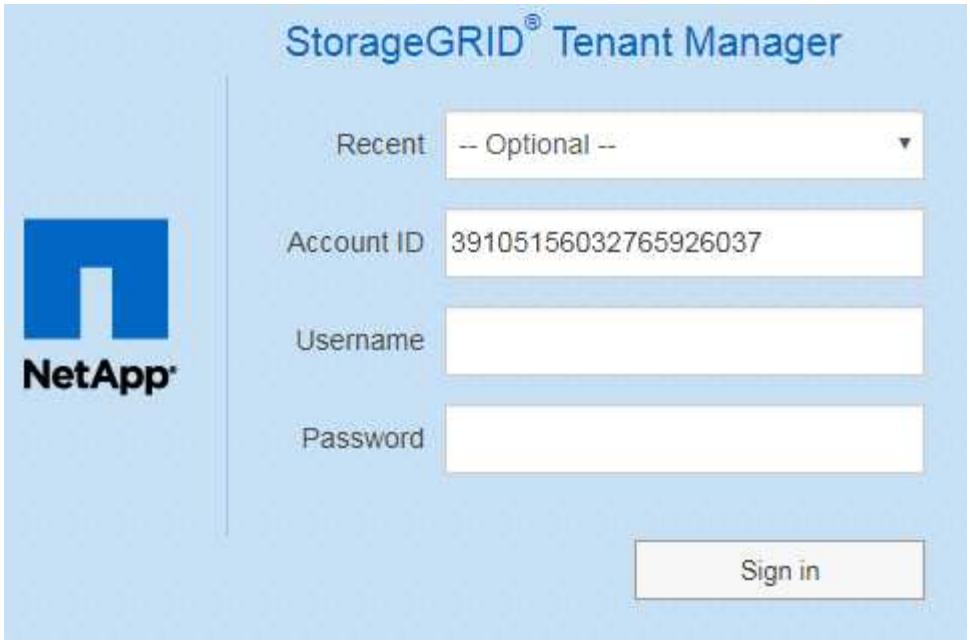
1. Inicie um navegador da web suportado.
2. Na barra de endereços do navegador, insira o URL para acessar o Gerenciador de locatários.
3. Se for solicitado um alerta de segurança, instale o certificado usando o assistente de instalação do navegador.
4. Inicie sessão no Gestor do Locatário.

   A tela de login que você vê depende do URL digitado e se sua organização está usando o logon único (SSO). Você verá uma das seguintes telas:

   - A página de login do Gerenciador de Grade. Clique no link **Login do locatário** no canto superior direito.

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



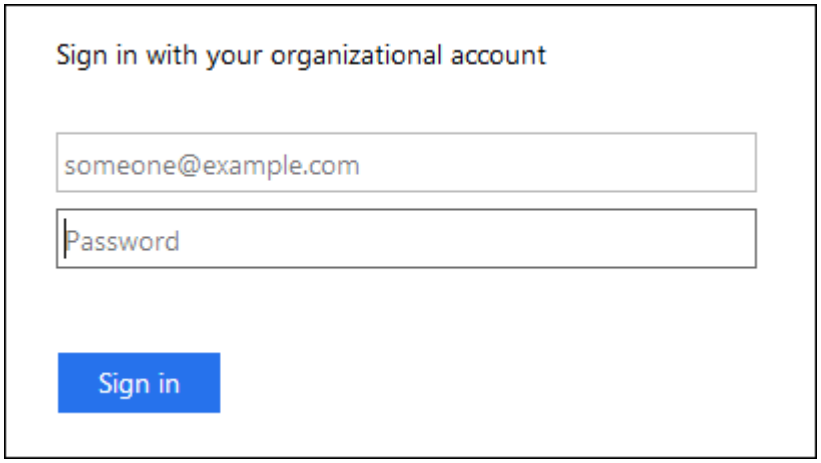

i. Se o ID da conta de 20 dígitos do locatário não for exibido, selecione o nome da conta do locatário se ele aparecer na lista de contas recentes ou insira o ID da conta.

ii. Introduza o seu nome de utilizador e palavra-passe.

iii. Clique em **entrar**.

É apresentado o Painel do Gestor do Locatário.

◦ A página SSO da sua organização, se o SSO estiver ativado na grade. Por exemplo:




Insira suas credenciais SSO padrão e clique em **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. Clique em **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 Gestor do Locatário.

5. Se você recebeu uma senha inicial de outra pessoa, altere sua senha para proteger sua conta. Selecione ***username*** **alterar senha**.

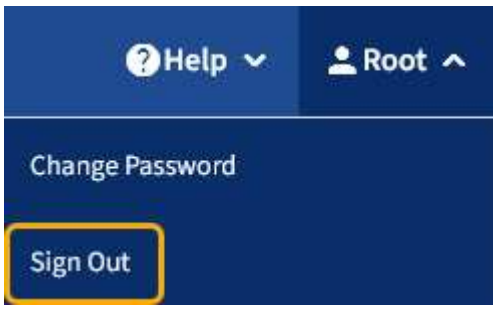
> Se o SSO estiver ativado para o sistema StorageGRID, você não poderá alterar sua senha do Gerenciador do Locatário.

## Sair do Tenant Manager

Quando terminar de trabalhar com o Gestor do Locatário, tem de terminar sessão para garantir que os utilizadores não autorizados não conseguem 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.

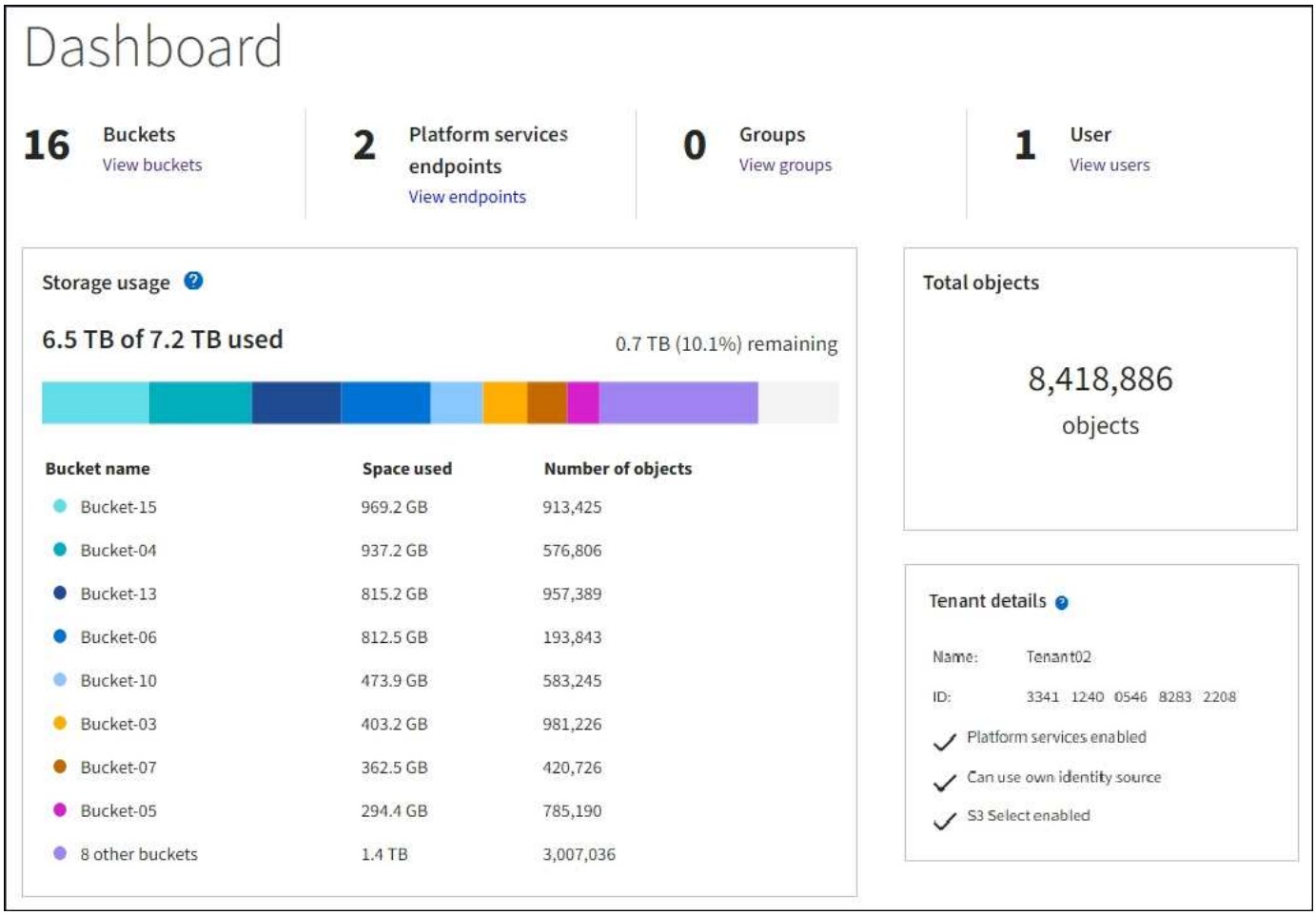
> Se o SSO estiver ativado e você também estiver conetado ao Gerenciador de Grade, você também deverá sair do Gerenciador de Grade para sair do SSO.

# Entenda o Painel do Tenant Manager

O Painel do Gerenciador do Tenant 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 em contentores (Swift). Se o locatário tiver uma cota, o Dashboard mostrará quanto da cota é usada e quanto resta. Se houver algum erro relacionado à conta de locatário, os erros serão exibidos no Painel de Controle.

> 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 de Controle 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 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 a permissão de acesso root, as diretrizes de 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 identidadeou 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.

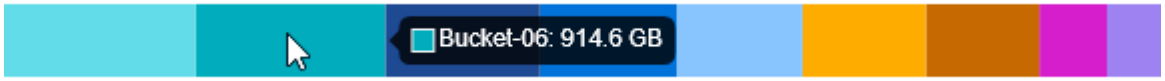
Esse valor indica a quantidade total de dados de objeto carregados e não representa o espaço usado para armazenar cópias desses objetos e seus metadados.

- 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.

A utilização de quotas baseia-se em estimativas internas e pode ser ultrapassada 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 a utilização da cota seja recalculada. Os cálculos de utilização 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.

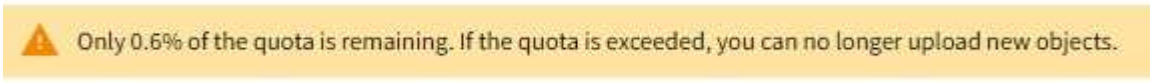
| Bucket name | Space used | Number of objects |
|---|---|---|
| Bucket-02 | 944.7 GB | 7,575 |
| Bucket-09 | 899.6 GB | 589,677 |
| Bucket-15 | 889.6 GB | 623,542 |
| Bucket-06 | 846.4 GB | 648,619 |
| Bucket-07 | 730.8 GB | 808,655 |
| Bucket-04 | 700.8 GB | 420,493 |
| Bucket-11 | 663.5 GB | 993,729 |
| 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.

### 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. Para obter mais informações, consulte a referência de alertas nas instruções para monitoramento e solução de problemas do StorageGRID.

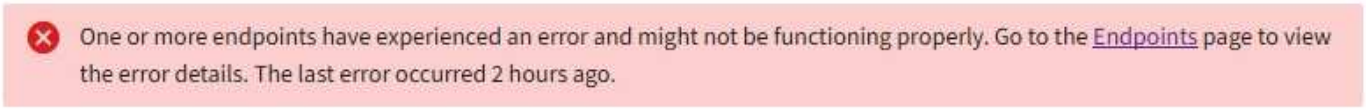



Se você exceder sua cota, não poderá carregar novos objetos.


Para exibir detalhes adicionais e gerenciar regras e notificações para alertas, consulte as instruções para monitoramento e solução de problemas do StorageGRID.

### 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 um erro de endpoint, selecione Endpoints para exibir a página Endpoints.

**Informações relacionadas**

Solucionar erros de endpoint dos serviços da plataforma

Monitorar e solucionar problemas

# 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:

**Passos**

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 sitesconsulte .

  > 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 locatário. 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, como segue:

  **S3**

  - Criar bucket (com e sem bloqueio de objeto S3 ativado)
  - Modificar a retenção padrão do bucket (para buckets com o bloqueio de objetos S3 ativado)
  - Defina o controle de consistência para operações executadas em objetos
  - Crie, atualize e exclua a configuração CORS de um bucket
  - Ative e desative as atualizações da última hora de acesso para objetos
  - Gerenciar as configurações de serviços de plataforma, incluindo replicação do CloudMirror, notificações e integração de pesquisa (notificação de metadados)
  - Exclua buckets vazios

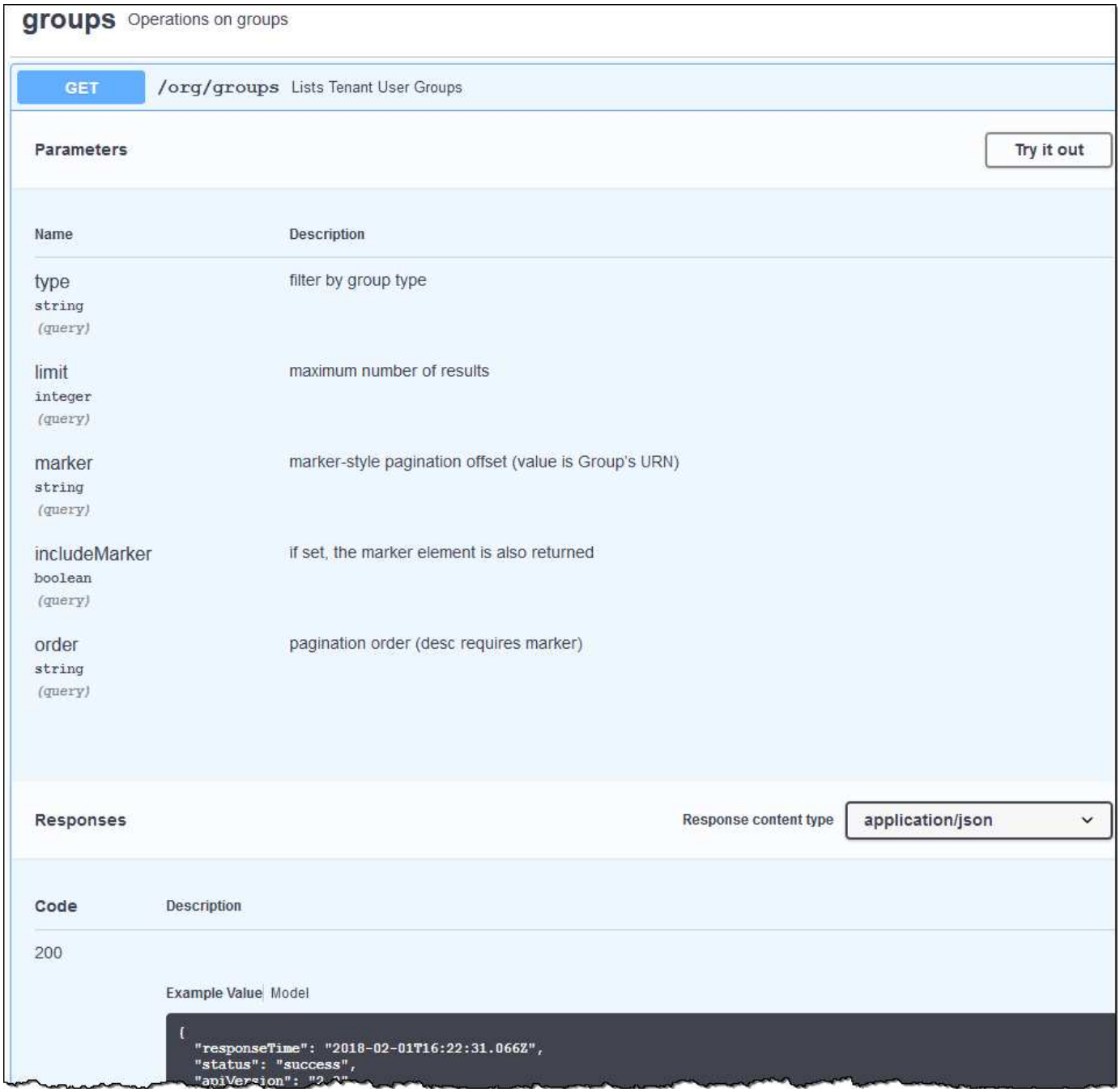
  **Swift**: Defina o nível de consistência usado para contentores

- **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.

- **Groups** — operações para gerenciar grupos de locatários locais e recuperar grupos de locatários federados de uma origem de identidade externa.
- **Identity-source** — operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo federado e de usuário.
- **Regions** — operações para determinar quais regiões foram configuradas para o sistema StorageGRID.
- **S3** — operações para gerenciar chaves de acesso S3 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 3 da API.

```
https://hostname_or_ip_address/api/v3/authorize
```

A versão principal da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que são ***not compatible*** com versões mais antigas. A versão menor da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que ***are 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 o software StorageGRID é instalado pela primeira vez, apenas a versão mais recente da API de gerenciamento de locatário é ativada. No entanto, quando o StorageGRID é atualizado para uma nova versão de recurso, você continua a ter acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID.

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

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

Use a seguinte solicitação de API para retornar uma lista das principais versões da API suportada:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

#### Especifique a versão da API para solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v3`) ou um cabeçalho (`Api-Version: 3`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" 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 `"Content-Type: application/json"` cabeçalho para qualquer solicitação que espera um corpo de solicitação JSON como uma proteção adicional contra ataques CSRF.

# Gerenciar o acesso ao sistema

## 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.

#### O que você vai precisar

- Você está conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você tem permissões de acesso específicas.
- Você está usando o ative Directory, o Azure AD, o OpenLDAP ou o Oracle Directory Server como provedor de identidade.

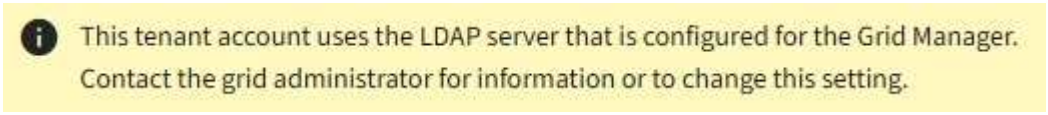
  > Se pretender utilizar um serviço LDAP v3 que não esteja listado, contacte o suporte técnico.

- 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 saídaConsulte .

#### 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

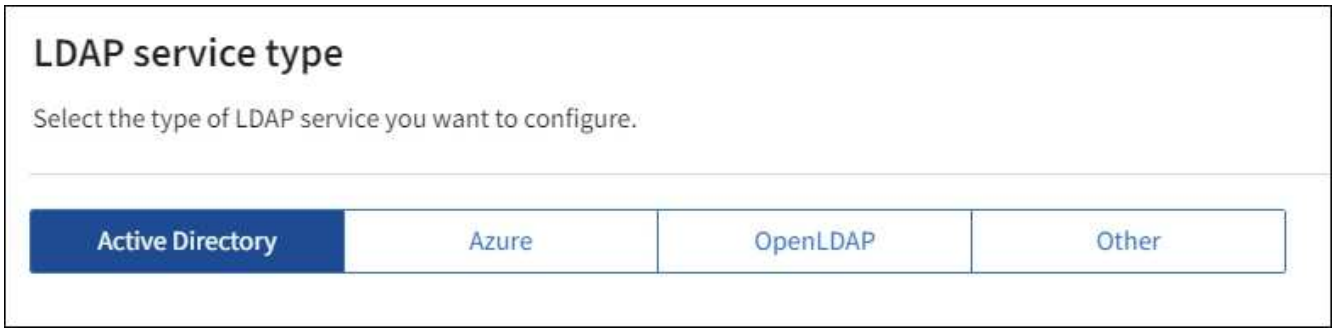
configurado para o Gerenciador de Grade. Se você vir essa mensagem ao acessar a página Federação de identidade, não será possível configurar uma origem de identidade federada separada para esse locatário.




#### Introduza a configuração

**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.
- **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.

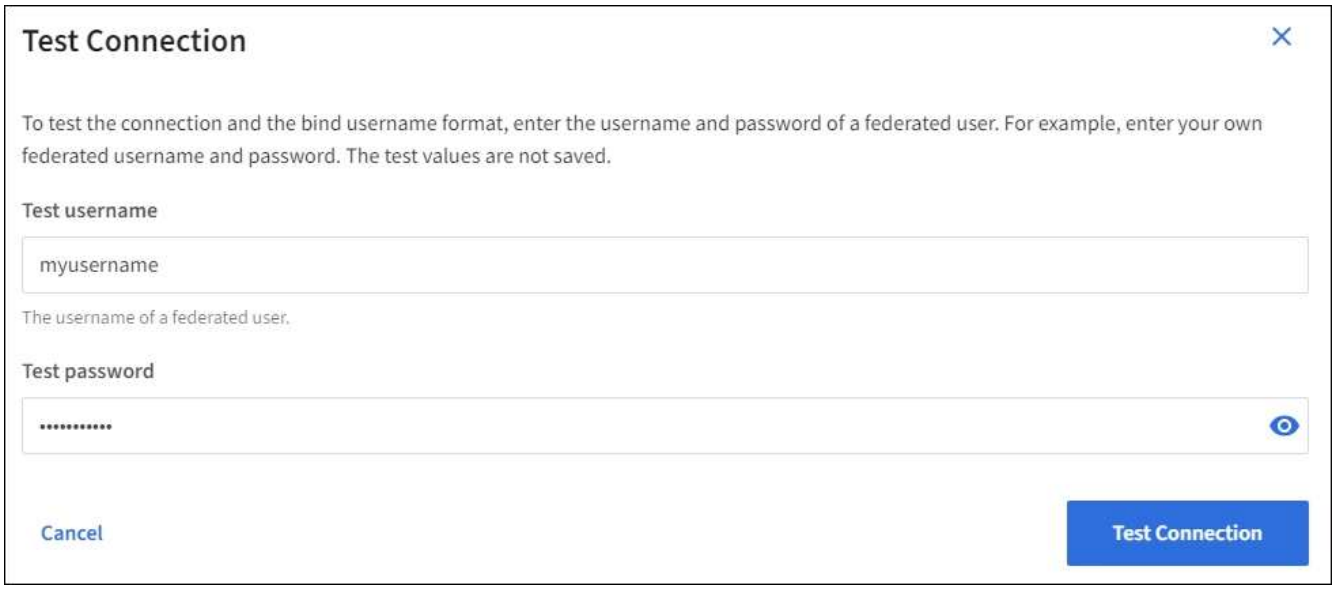
     Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

#### 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.

1. Selecione **Test Connection**.
2. Se você não forneceu um formato de nome de usuário do BIND:
   - Uma mensagem ""Teste de conexão bem-sucedida"" aparece se as configurações de conexão forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - Uma mensagem "'test Connection could not be established'" (não foi possível estabelecer ligação) é apresentada se as definições de 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 /.




- Uma mensagem ""Teste de conexão bem-sucedida"" aparece se as configurações de conexão 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 **habilitado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade. Desative o logon únicoConsulte .

**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 e 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

### Crie grupos para um locatário do S3

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

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.

- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root. Permissões de gerenciamento do locatárioConsulte .
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

Para obter informações sobre o S3, Use S3consulte .

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.


2. Selecione **criar grupo**.
3. 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.

4. 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.
5. Selecione **continuar**.
6. Selecione um modo de acesso. 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.
   - **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do Tenant e gerenciar a configuração do locatário.

- **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações nem 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.

7. Selecione as permissões de grupo para este grupo.

   Consulte as informações sobre permissões de gerenciamento de locatários.

8. Selecione **continuar**.
9. Selecione uma política de grupo para determinar quais permissões de acesso S3 os membros deste grupo terão.
   - **No S3 Access**: Padrão. Os usuários deste grupo não têm acesso a recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar essa opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
   - **Acesso somente leitura**: Os usuários deste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos. Quando você seleciona essa opção, a cadeia de 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.
   - **Custom**: Os usuários do grupo recebem as permissões que você especificar na caixa de texto. Consulte as instruções para implementar um aplicativo cliente S3 para obter informações detalhadas sobre políticas de grupo, incluindo sintaxe de linguagem e exemplos.
10. 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.

    Neste exemplo, os membros do grupo só podem listar e acessar uma pasta que corresponda ao nome de usuário (prefixo de chave) no intervalo especificado. Observe que as permissões de acesso de outras políticas de grupo e a política de bucket devem ser consideradas ao determinar a privacidade dessas pastas.


11. Selecione o botão que aparece, dependendo se você está criando um grupo federado ou um grupo local:
    - Grupo federado: **Criar grupo**
    - Grupo local: **Continuar**

    Se você estiver criando um grupo local, a etapa 4 (Adicionar usuários) será exibida após selecionar **continuar**. Esta etapa não aparece para grupos federados.

12. Marque a caixa de seleção para cada usuário que deseja adicionar ao grupo e selecione **criar grupo**.

    Opcionalmente, você pode salvar o grupo sem adicionar usuários. Você pode adicionar usuários ao grupo mais tarde ou selecionar o grupo quando adicionar novos usuários.

13. Selecione **Finish**.

    O grupo criado aparece na lista de grupos. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

### 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 que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.

- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.


2. Selecione **criar grupo**.
3. 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.

4. 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.
5. Selecione **continuar**.
6. Selecione um modo de acesso. 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.
   - **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do Tenant e gerenciar a configuração do locatário.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações nem 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.

7. Defina a permissão Grupo.
   - Marque a caixa de seleção **Root Access** se os usuários precisarem fazer login na API de Gerenciamento de Tenant ou Tenant Manager. (Predefinição)
   - Desmarque a caixa de seleção **Root Access** se os usuários não precisarem de acesso ao Gerenciador do locatário ou à API de Gerenciamento do locatário. Por exemplo, desmarque a caixa de seleção para aplicativos que não precisam acessar o locatário. Em seguida, atribua a permissão **Swift Administrator** para permitir que esses usuários gerenciem contentores e objetos.
8. Selecione **continuar**.
9. Marque a caixa de seleção **Swift administrator** se o usuário precisar usar a Swift REST API.

   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 na API REST do Swift para criar contentores e ingerir objetos. Os usuários devem ter a permissão Swift Administrator para se autenticar na API Swift REST.

10. Selecione o botão que aparece, dependendo se você está criando um grupo federado ou um grupo local:
    - Grupo federado: **Criar grupo**
    - Grupo local: **Continuar**

      Se você estiver criando um grupo local, a etapa 4 (Adicionar usuários) será exibida após selecionar **continuar**. Esta etapa não aparece para grupos federados.

11. Marque a caixa de seleção para cada usuário que deseja adicionar ao grupo e selecione **criar grupo**.

    Opcionalmente, você pode salvar o grupo sem adicionar usuários. Você pode adicionar usuários ao grupo mais tarde ou selecionar o grupo quando criar novos usuários.

12. Selecione **Finish**.

    O grupo criado aparece na lista de grupos. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

**Informações relacionadas**

Permissões de gerenciamento do locatário

Use Swift

**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. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

| Permissão | Descrição |
|---|---|
| Acesso à raiz | Fornece acesso total ao Gerenciador do Locatário e à API de Gerenciamento do Locatário.<br><br>**Observação:** os usuários do 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<br><br>**Observação:** os usuários do Swift devem ter a permissão Swift Administrator para executar qualquer operação com a Swift REST API. |
| Gerencie suas próprias credenciais S3 | Apenas S3 inquilinos. Permite que os usuários criem e removam suas próprias chaves de acesso S3. Os usuários que não têm essa permissão não veem a opção de menu **ARMAZENAMENTO (S3) My S3 Access Keys**. |
| Gerenciar todos os baldes | • S3 locatários: 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>Os usuários que não têm essa permissão não veem a opção de menu **Buckets**.<br><br>• Swift tenants: Permite que usuários Swift controlem o nível de consistência para contentores Swift usando a API de Gerenciamento do locatário.<br><br>**Observação:** você só pode atribuir a permissão Gerenciar todos os buckets a grupos Swift a partir da API de Gerenciamento de locatário. Você não pode atribuir essa permissão a grupos Swift usando o Gerenciador de inquilinos. |

| Permissão | Descrição |
| --- | --- |
| Gerir pontos finais | Apenas S3 inquilinos. Permite que os usuários usem o Gerenciador do Locatário ou a API de Gerenciamento do Locatário para criar ou editar endpoints, que são usados como o destino para os serviços da plataforma StorageGRID.<br><br>Os usuários que não têm essa permissão não veem a opção de menu **endpoints de serviços da plataforma**. |

**Informações relacionadas**

Use S3

Use Swift

### Ver e editar detalhes do grupo

Ao exibir os detalhes de um grupo, você pode alterar o nome de exibição, as permissões, as políticas e os usuários que pertencem ao grupo.

**O que você vai precisar**

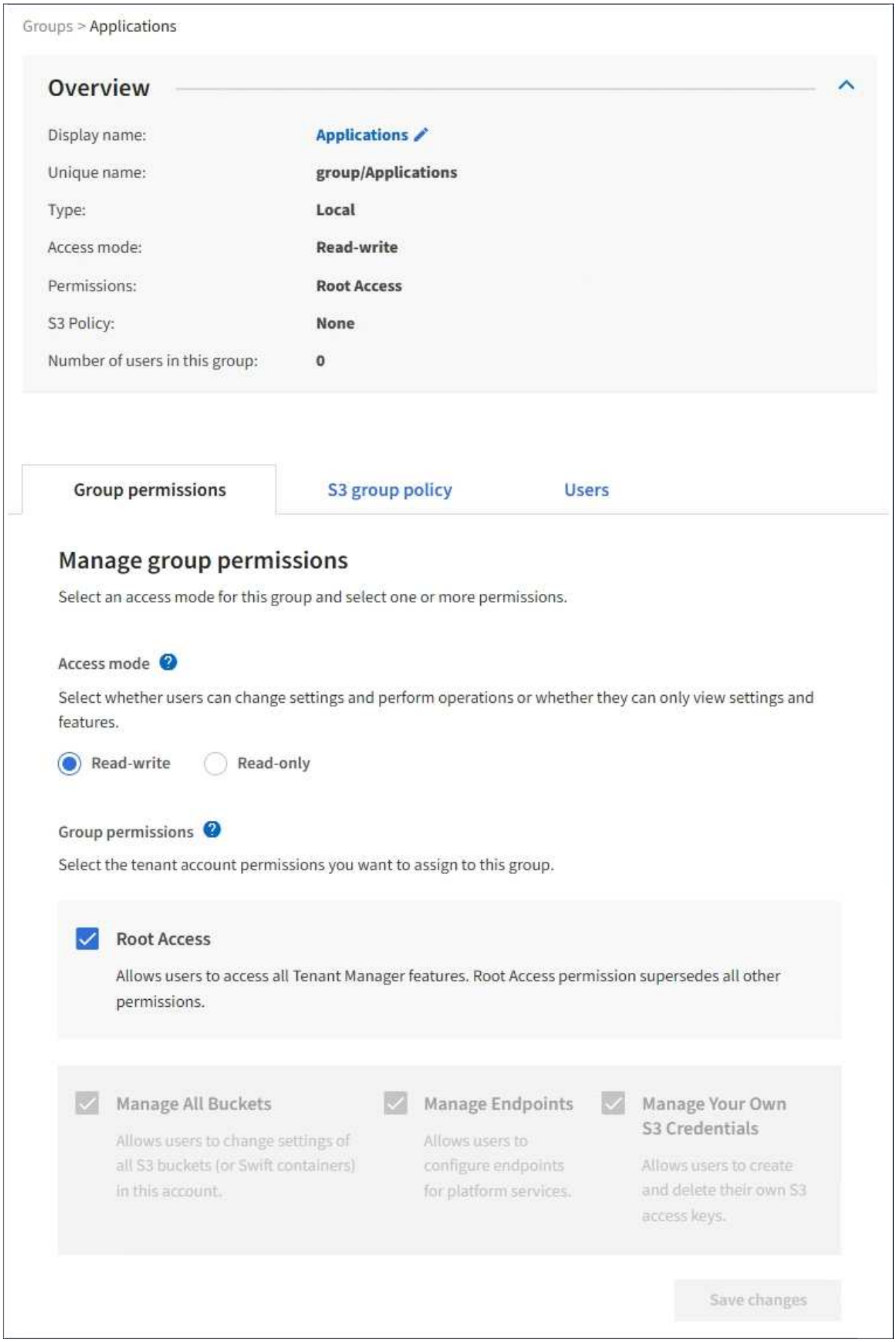
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Selecione o nome do grupo cujos detalhes deseja exibir ou editar.

   Alternativamente, você pode selecionar **ações Exibir detalhes do grupo**.

   A página de detalhes do grupo é exibida. O exemplo a seguir mostra a página de detalhes do grupo S3.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Faça alterações nas definições do grupo conforme necessário.

   Para garantir que suas alterações sejam salvas, selecione **Salvar alterações** depois de fazer alterações em cada seção. Quando as alterações são salvas, uma mensagem de confirmação aparece no canto superior direito da página.

   a. Opcionalmente, selecione o nome de exibição ou o ícone de edição para atualizar o nome de exibição.

      Não é possível alterar o nome exclusivo de um grupo. Não é possível editar o nome de exibição de um grupo federado.

   b. Opcionalmente, atualize as permissões.

   c. Para a política de grupo, faça as alterações apropriadas para o seu locatário S3 ou Swift.

      - Se você estiver editando um grupo para um locatário S3, opcionalmente, selecione uma política de grupo S3 diferente. Se você selecionar uma política S3 personalizada, atualize a cadeia de carateres JSON conforme necessário.
      - Se você estiver editando um grupo para um locatário Swift, opcionalmente selecione ou desmarque a caixa de seleção **Administrador Swift**.

        Para obter mais informações sobre a permissão Swift Administrator, consulte as instruções para criar grupos para um locatário Swift.

   d. Opcionalmente, adicione ou remova usuários.

4. Confirme que selecionou **Guardar alterações** para cada secção alterada.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

**Informações relacionadas**

Criar grupos para S3 inquilino

Crie grupos para o locatário Swift

### Adicione usuários a um grupo local

Você pode adicionar usuários a um grupo local conforme necessário.

**O que você vai precisar**

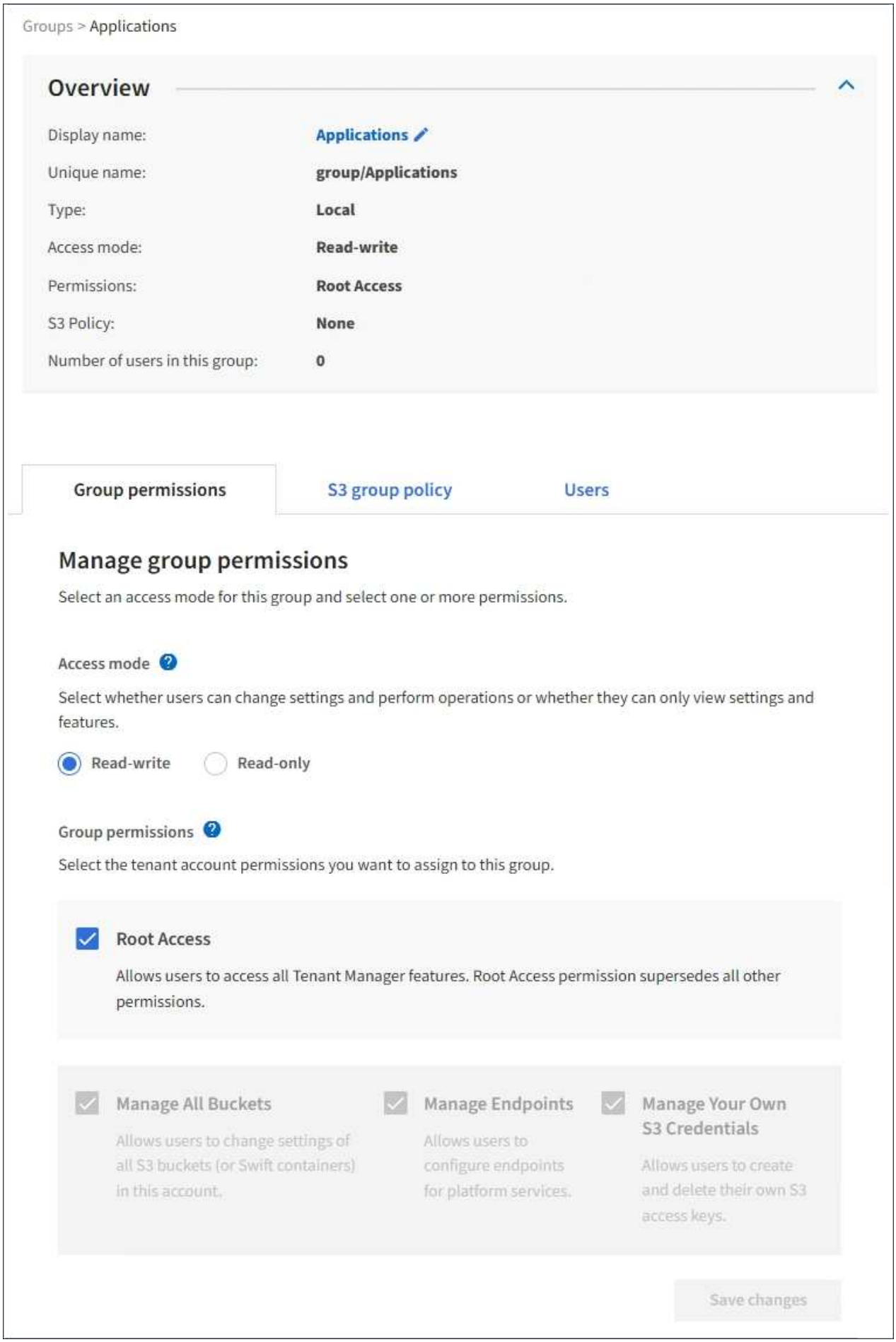
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

**Passos**

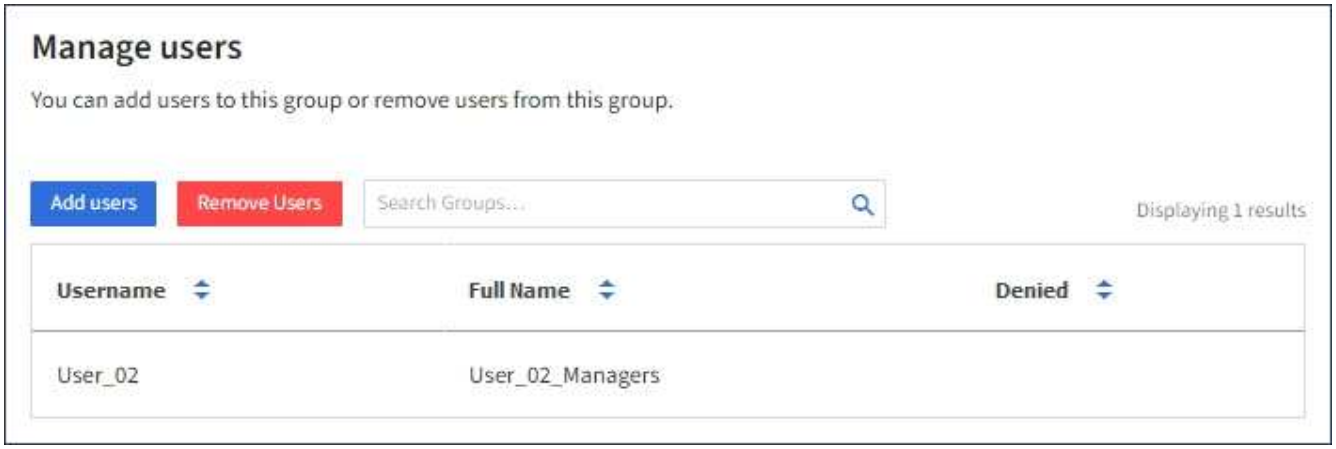
1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Selecione o nome do grupo local ao qual deseja adicionar usuários.

   Alternativamente, você pode selecionar **ações Exibir detalhes do grupo**.

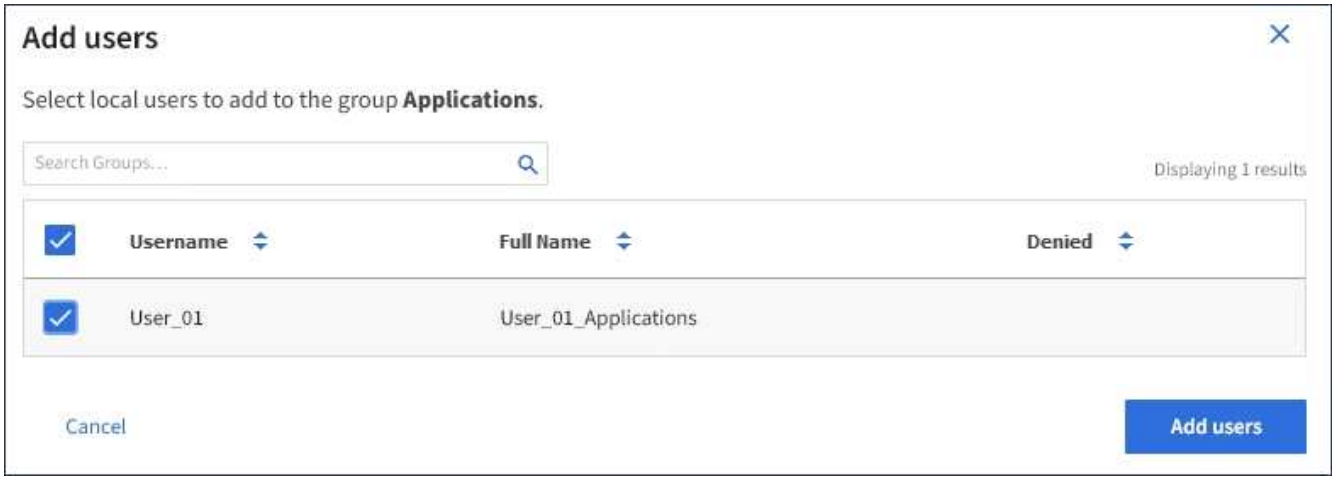
   A página de detalhes do grupo é exibida.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Selecione **Users** e, em seguida, selecione **Add Users**.




4. Selecione os usuários que deseja adicionar ao grupo e selecione **Adicionar usuários**.




Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

### Editar nome do grupo

Pode editar o nome de apresentação de um grupo. Não é possível editar o nome exclusivo de um grupo.

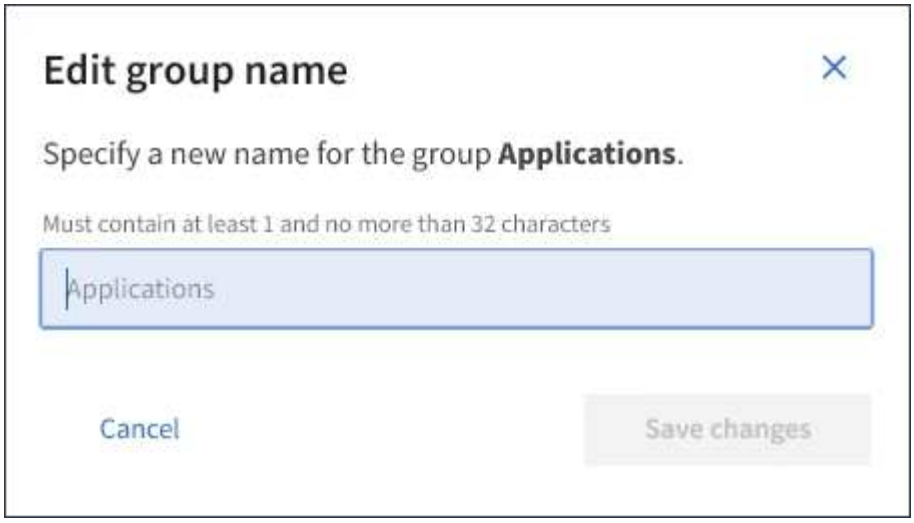
**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root. Permissões de gerenciamento do locatárioConsulte .

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Marque a caixa de seleção do grupo cujo nome de exibição deseja editar.
3. Selecione **ações** > **Editar nome do grupo**.

   A caixa de diálogo Editar nome do grupo é exibida.




4. Se estiver editando um grupo local, atualize o nome de exibição conforme necessário.

   Não é possível alterar o nome exclusivo de um grupo. Não é possível editar o nome de exibição de um grupo federado.

5. Selecione **Salvar alterações**.

   Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

### Grupo duplicado

Você pode criar novos grupos mais rapidamente duplicando um grupo existente.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root. Permissões de gerenciamento do locatárioConsulte .

**Passos**

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Marque a caixa de seleção do grupo que deseja duplicar.
3. Selecione **Duplicate group**. Para obter detalhes adicionais sobre como criar um grupo, consulte as instruções para criar grupos para Um inquilino de S3 anos ou para Um inquilino Swift.
4. 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.

5. 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.

6. Selecione **continuar**.
7. Conforme necessário, modifique as permissões para este grupo.
8. Selecione **continuar**.
9. Conforme necessário, se você estiver duplicando um grupo para um locatário S3, opcionalmente, selecione uma política diferente nos botões de opção **Adicionar política S3**. Se você selecionou uma política personalizada, atualize a cadeia de carateres JSON conforme necessário.
10. Selecione **criar grupo**.

### Eliminar grupo

Pode eliminar um grupo do sistema. Quaisquer usuários que pertençam apenas a esse grupo não poderão mais entrar no Gerenciador do Locatário ou usar a conta do locatário.

#### O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root. Permissões de gerenciamento do locatárioConsulte .

#### Passos

1. Selecione **GERENCIAMENTO DE ACESSO grupos**.


2. Marque as caixas de seleção dos grupos que deseja excluir.
3. Selecione **ações** > **Excluir grupo**.

   É apresentada uma mensagem de confirmação.

4. Selecione **Excluir grupo** para confirmar que deseja excluir os grupos indicados na mensagem de confirmação.

Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

## 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, não é possível remover o usuário root.

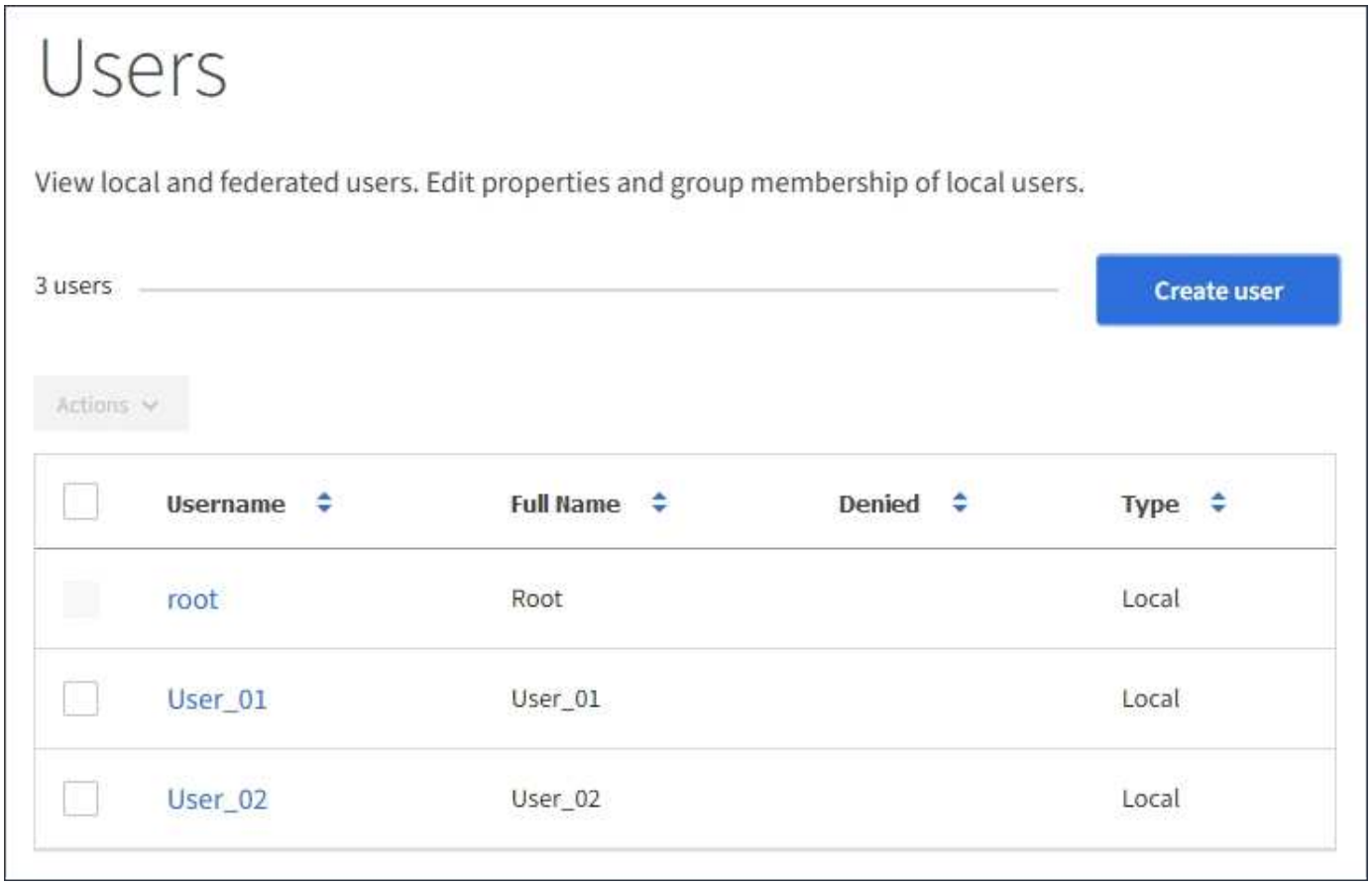
**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários de leitura e gravação que tenha a permissão de acesso root. Permissões de gerenciamento do locatárioConsulte .

> Se o logon único (SSO) estiver habilitado para o seu 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 S3 ou Swift para acessar os recursos do locatário, com base nas permissões de grupo.

**Acesse a página usuários**

Selecione **GERENCIAMENTO DE ACESSO usuários**.



### Crie usuários locais

Você pode criar usuários locais e atribuí-los 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.

**Passos**

1. Selecione **criar usuário**.
2. Preencha os campos a seguir.
   - **Nome completo**: O nome completo deste usuário, por exemplo, o nome e sobrenome de uma pessoa ou o nome de um aplicativo.
   - **Nome de usuário**: O nome que este usuário usará para entrar. Os nomes de usuário devem ser exclusivos e não podem ser alterados.
   - * Senha*: Uma senha, que é usada quando o usuário entra.
   - **Confirm password**: Digite a mesma senha digitada no campo Senha.
   - **Negar acesso**: Se você selecionar **Sim**, esse usuário não poderá entrar na conta de locatário, mesmo que o usuário ainda possa pertencer a um ou mais grupos.

     Como exemplo, você pode usar esse recurso para suspender temporariamente a capacidade de um usuário fazer login.
3. Selecione **continuar**.
4. Atribua o usuário a um ou mais grupos locais.

   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.
5. Selecione **criar usuário**.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

### Editar detalhes do utilizador

Ao editar os detalhes de um usuário, você pode alterar o nome completo e a senha do usuário, adicionar o usuário a diferentes grupos e impedir que o usuário acesse o locatário.

**Passos**

1. Na lista Users (utilizadores), selecione o nome do utilizador cujos detalhes pretende ver ou editar.

   Alternativamente, você pode selecionar a caixa de seleção para o usuário e, em seguida, selecionar **ações Exibir detalhes do usuário**.
2. Faça alterações nas definições do utilizador, conforme necessário.
   a. Altere o nome completo do usuário conforme necessário selecionando o nome completo ou o ícone de edição na seção Visão geral.

Você não pode alterar o nome de usuário.

b. Na guia **Senha**, altere a senha do usuário conforme necessário.
c. Na guia **Access**, permita que o usuário faça login (selecione **não**) ou impeça que o usuário faça login (selecione **Sim**) conforme necessário.
d. Na guia **Groups**, adicione o usuário aos grupos ou remova o usuário dos grupos conforme necessário.
e. Conforme necessário para cada seção, selecione **Salvar alterações**.

As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

### Duplicar usuários locais

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

**Passos**

1. Na lista usuários, selecione o usuário que deseja duplicar.
2. Selecione **Duplicate user**.
3. Modifique os campos a seguir para o novo usuário.
   - **Nome completo**: O nome completo deste usuário, por exemplo, o nome e sobrenome de uma pessoa ou o nome de um aplicativo.
   - **Nome de usuário**: O nome que este usuário usará para entrar. Os nomes de usuário devem ser exclusivos e não podem ser alterados.
   - * Senha*: Uma senha, que é usada quando o usuário entra.
   - **Confirm password**: Digite a mesma senha digitada no campo Senha.
   - **Negar acesso**: Se você selecionar **Sim**, esse usuário não poderá entrar na conta de locatário, mesmo que o usuário ainda possa pertencer a um ou mais grupos.

     Como exemplo, você pode usar esse recurso para suspender temporariamente a capacidade de um usuário fazer login.
4. Selecione **continuar**.
5. Selecione um ou mais grupos locais.

   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.
6. Selecione **criar usuário**.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

### Eliminar utilizadores locais

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

Usando o Gerenciador do Locatário, você pode excluir usuários locais, mas não usuários federados. Você deve usar a origem de identidade federada para excluir usuários federados.

**Passos**

1. Na lista Users (utilizadores), selecione a caixa de verificação para o utilizador local que pretende eliminar.
2. Selecione **ações** > **Excluir usuário**.
3. Na caixa de diálogo de confirmação, selecione **Excluir usuário** para confirmar que deseja excluir o usuário do sistema.

   As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

# Gerenciar contas de locatários do S3

## Gerenciar S3 chaves de acesso

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.

### Sobre esta tarefa

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

- Os usuários que têm a permissão **Gerenciar suas próprias credenciais do S3** podem criar ou remover suas próprias chaves de acesso do 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 na conta de locatário do S3.

#### O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve ter a permissão Gerenciar suas próprias credenciais do S3. Permissões de gerenciamento do locatárioConsulte .

#### 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 novas chaves periodicamente, não será necessário definir um tempo de expiração para suas chaves. Se você decidir mais tarde criar novas chaves, exclua as chaves antigas manualmente.

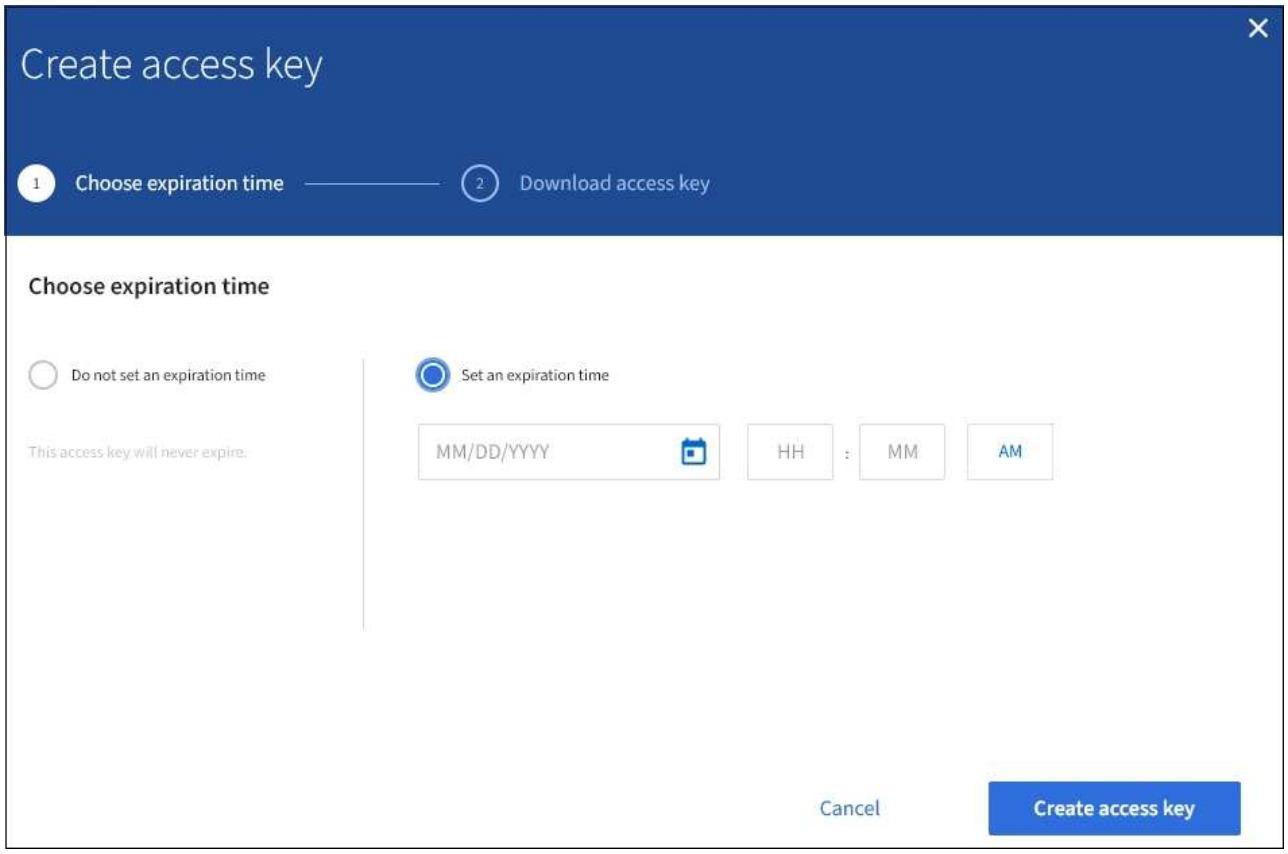
> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para a sua conta no Gerenciador do Locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova 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.

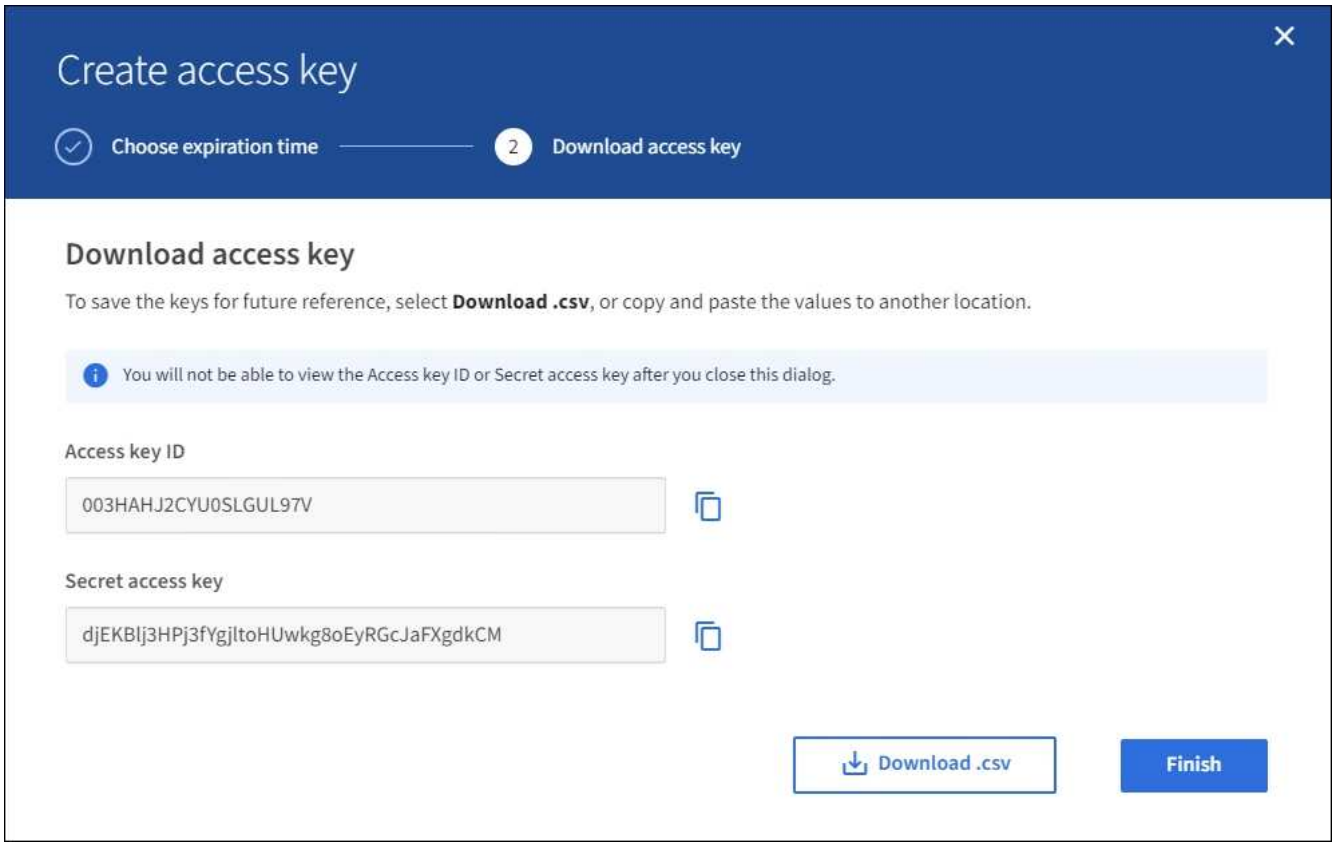



4. Selecione **criar chave de acesso**.

   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. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

### Veja as suas teclas de acesso S3

Se você estiver usando um locatário do S3 e tiver a permissão apropriada, você poderá exibir uma lista de suas 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 criar novas chaves ou excluir chaves que você não está mais usando.

#### O que você vai precisar

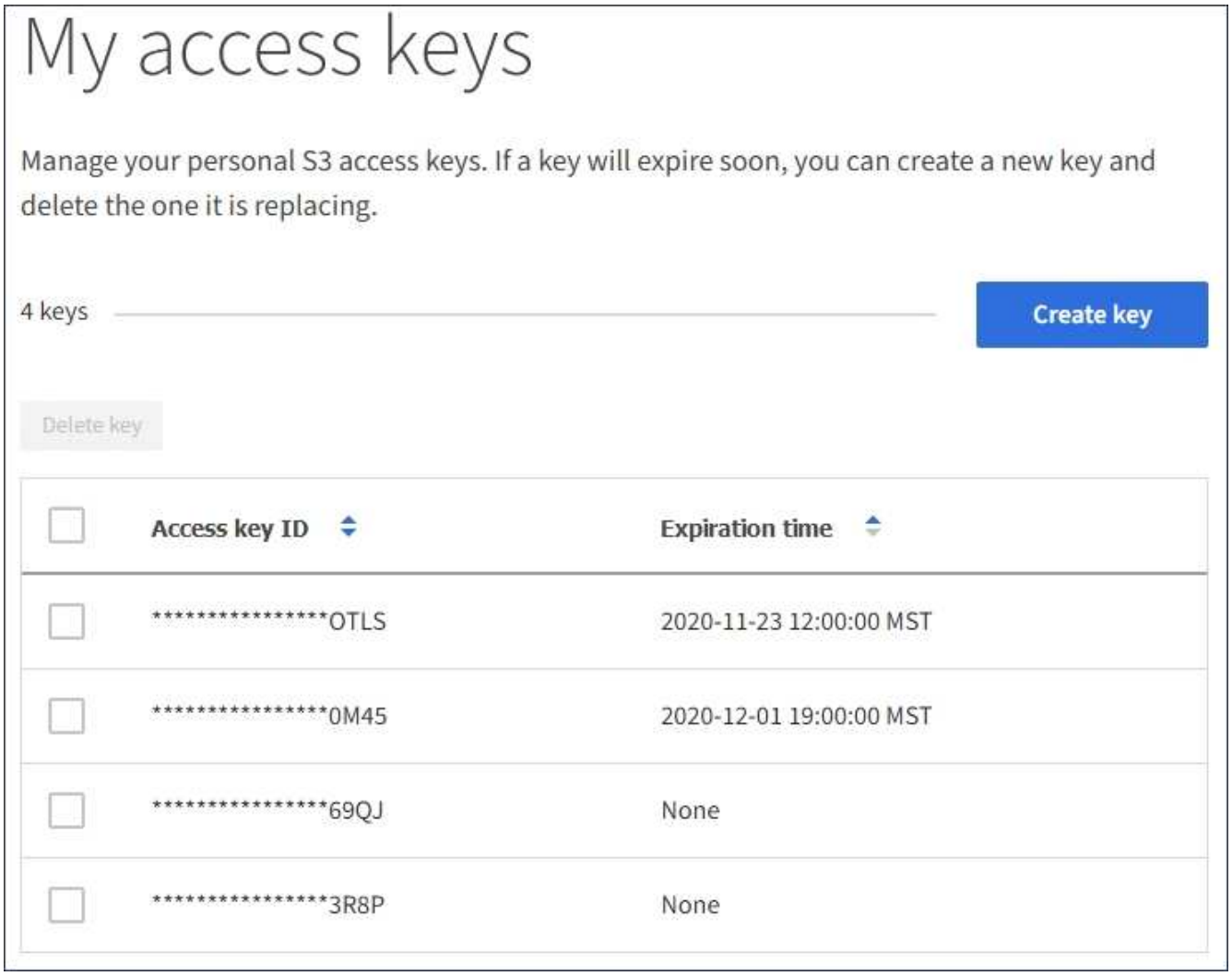
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve ter a permissão Gerenciar suas próprias credenciais do S3.

Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para 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. Classifique as chaves por **tempo de expiração** ou **ID da chave de acesso**.
3. Conforme necessário, crie novas chaves e exclua manualmente as chaves que você não está 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.

**Informações relacionadas**

Crie suas próprias chaves de acesso S3

Elimine as suas próprias chaves de acesso S3

### 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.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve ter a permissão Gerenciar suas próprias credenciais do S3. Permissões de gerenciamento do locatárioConsulte .

> 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.

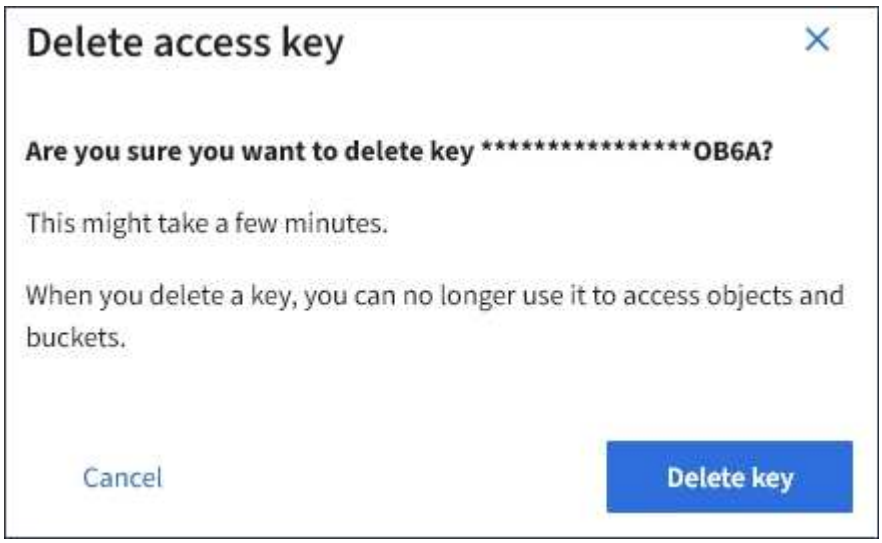
**Passos**

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. Marque a caixa de seleção para cada chave de acesso que deseja remover.
3. Selecione **Delete key**.

   É apresentada uma caixa de diálogo de confirmação.




4. Selecione **Delete key**.

   Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

### 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.

#### O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve ter a permissão de acesso root.

#### Sobre esta tarefa

Você pode criar uma ou mais chaves de acesso S3 para outros usuários para que eles possam criar e gerenciar buckets para 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:

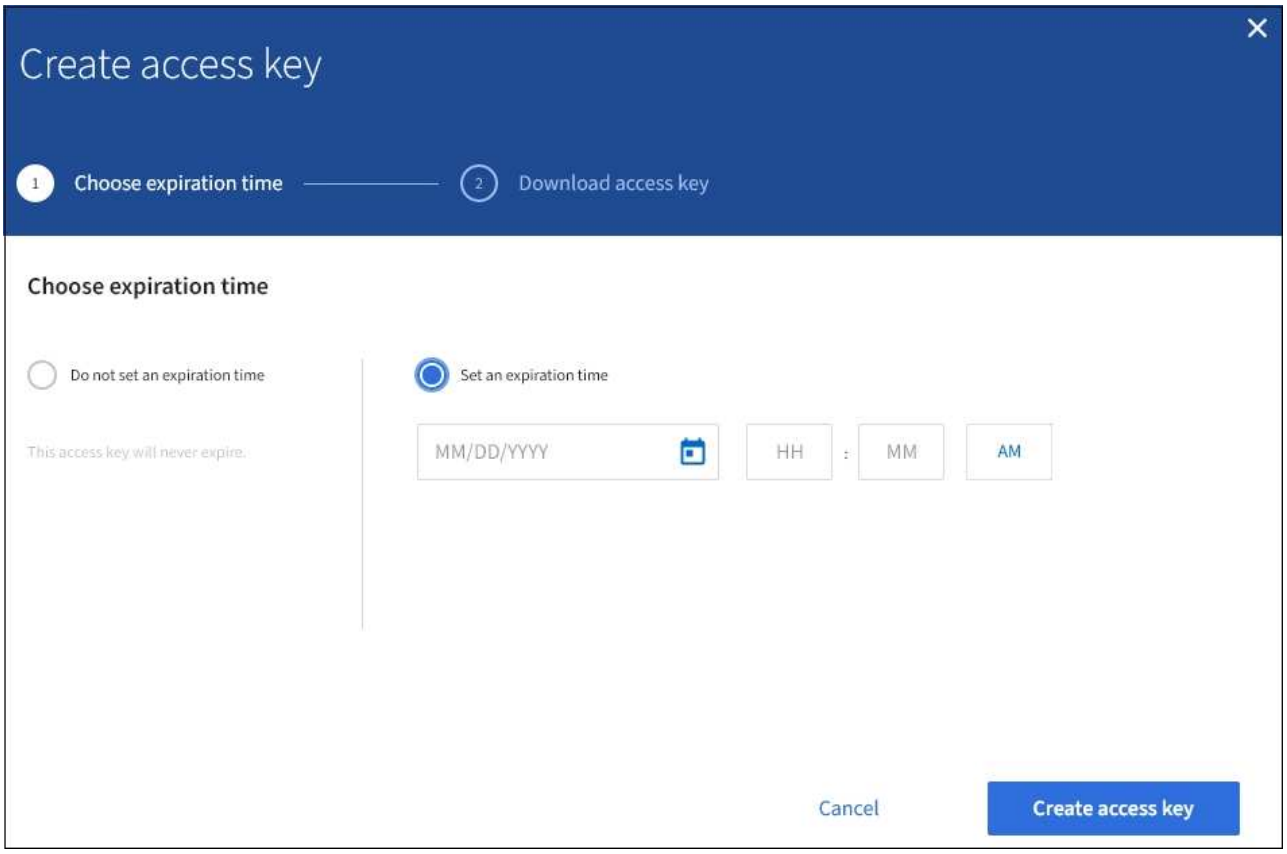
- Defina um tempo de expiração para as teclas para limitar o acesso do usuário a um determinado período de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco se o ID da chave de acesso e a chave de acesso secreta forem acidentalmente expostos. As chaves expiradas são removidas automaticamente.
- Se o risco de segurança em seu ambiente for baixo e você não precisar criar periodicamente novas chaves, não será necessário 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.

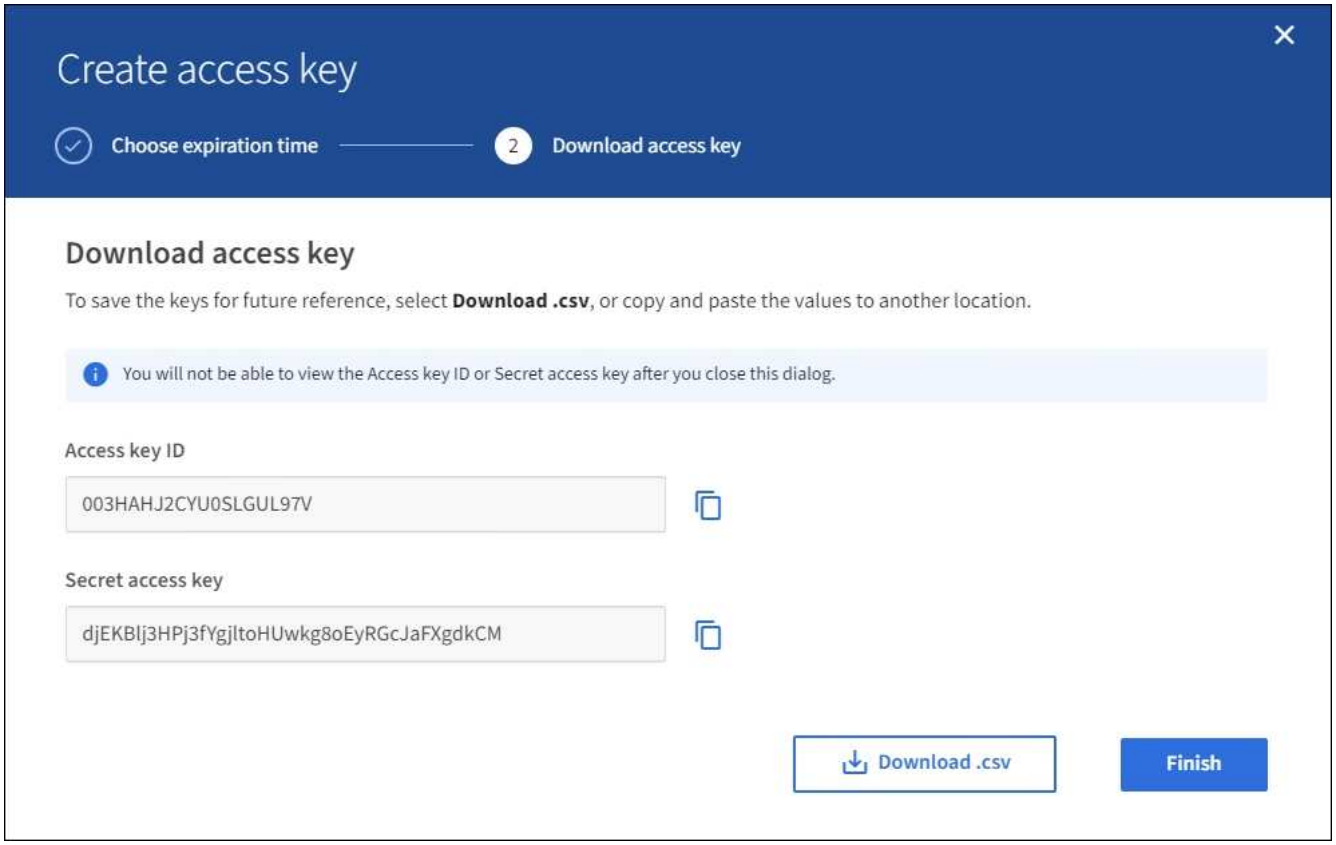



5. Selecione **criar chave de acesso**.

   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. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

**Informações relacionadas**

Permissões de gerenciamento do locatário

### 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.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve ter a permissão de acesso root.

> Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para esse usuário no 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**

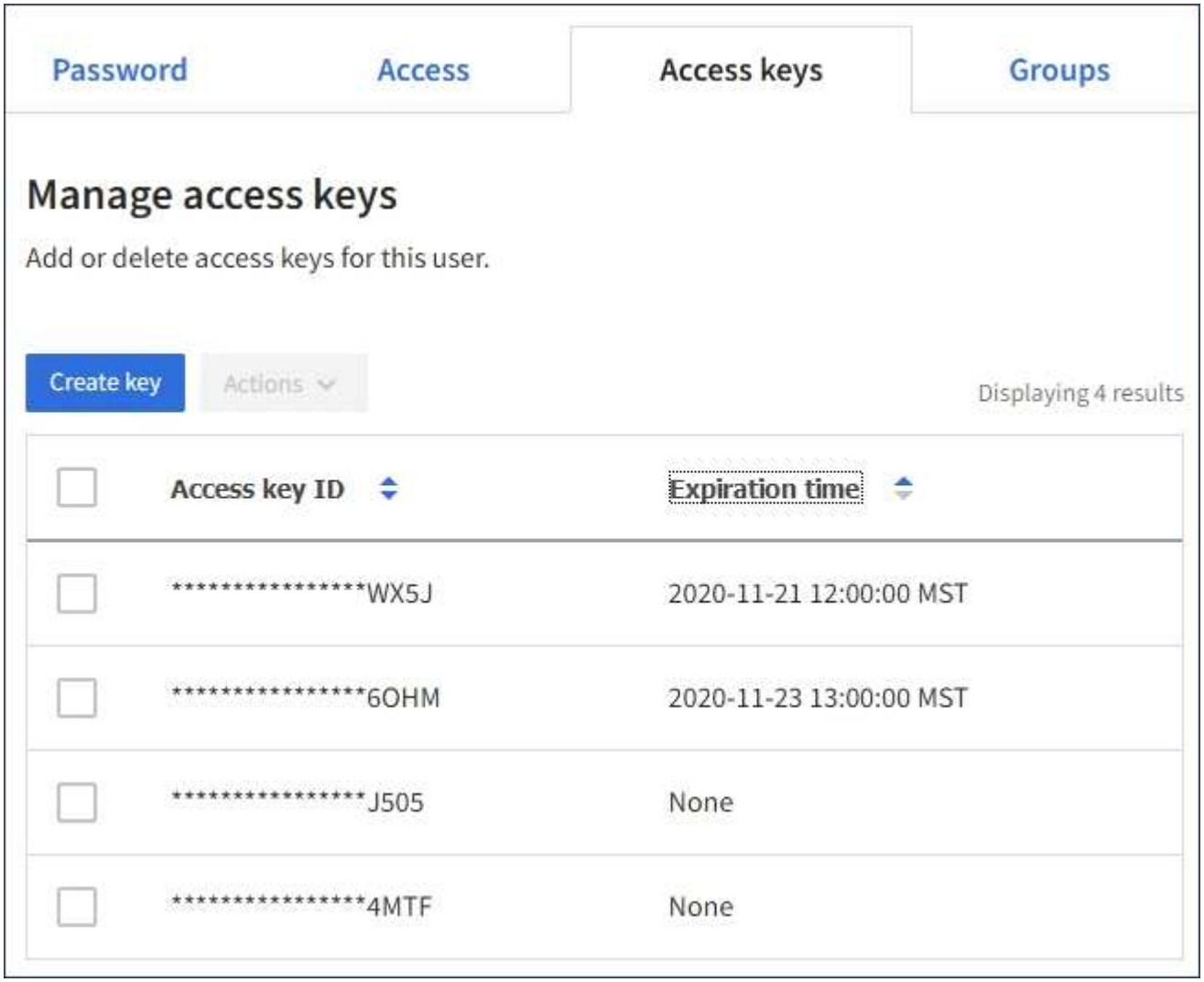
1. Selecione **GERENCIAMENTO DE ACESSO usuários**.

   A página usuários é exibida e lista os usuários existentes.

2. Selecione o utilizador cujas teclas de acesso S3 pretende visualizar.

   É apresentada a página Detalhes do utilizador.

3. 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.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve ter a permissão de acesso root. Permissões de gerenciamento do locatárioConsulte .

> 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**.

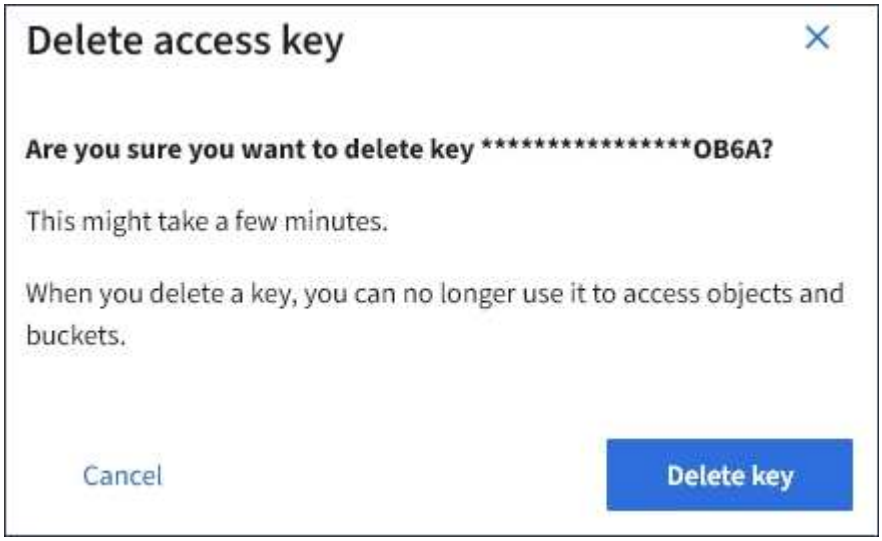
   A página usuários é exibida e lista os usuários existentes.

2. Selecione o usuário cujas chaves de acesso S3 você deseja gerenciar.

   É apresentada a página Detalhes do utilizador.

3. 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**.

   É apresentada uma caixa de diálogo de confirmação.




5. Selecione **Delete key**.

Uma mensagem de confirmação aparece no canto superior direito da página. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

## Gerenciar buckets do S3

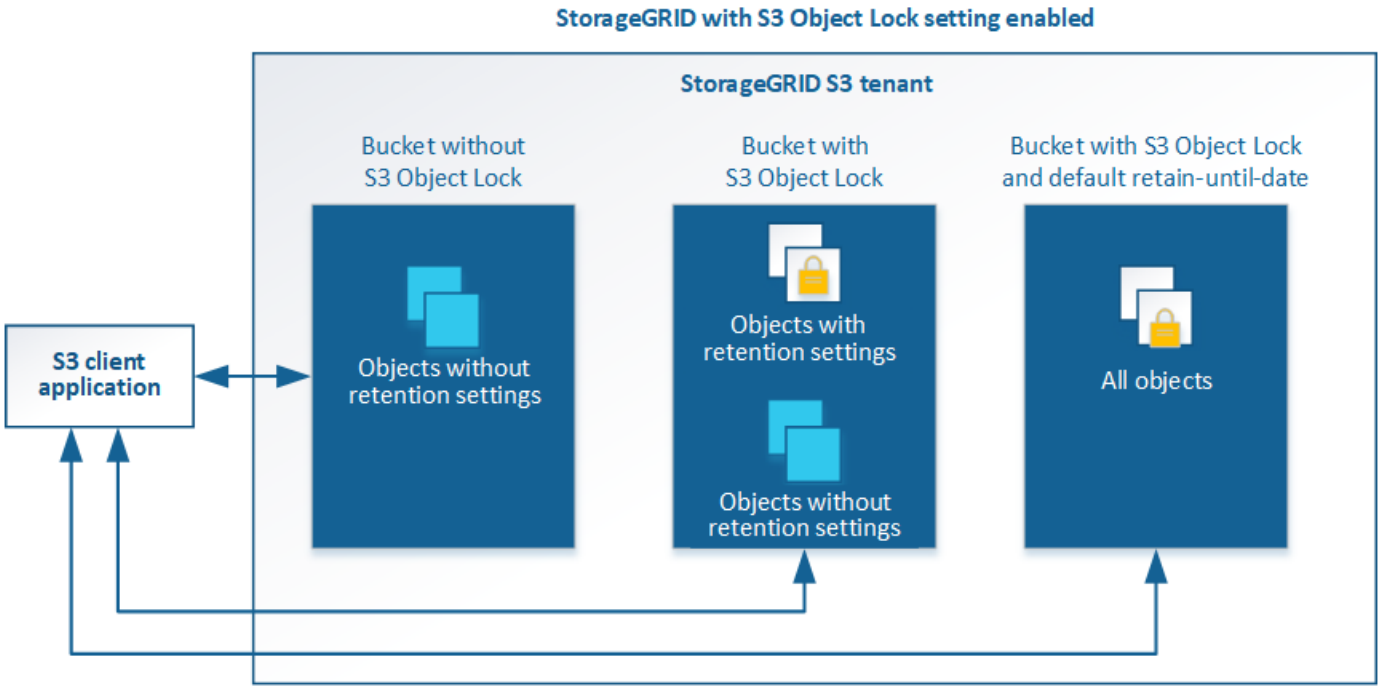
### Use o bloqueio de objetos S3 com locatários

Você pode usar o recurso bloqueio de objetos S3 no StorageGRID se seus objetos precisarem cumprir com 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 objeto S3 ativado, os aplicativos cliente S3 podem, opcionalmente, especificar configurações de retenção para qualquer versão de objeto nesse bucket. Uma versão de objeto deve ter configurações de retenção especificadas para ser protegida pelo bloqueio de objeto S3.




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

Se um bucket tiver o bloqueio de objeto S3 ativado, o aplicativo cliente S3 pode, opcionalmente, especificar uma ou ambas as seguintes configurações de retenção no nível do objeto ao criar ou atualizar um objeto:

- **Retent-until-date**: Se a data de retent-until de uma versão de objeto for no futuro, o objeto pode ser recuperado, mas não pode ser modificado ou excluído. Conforme necessário, a data de retenção até um objeto pode ser aumentada, mas essa data não pode ser diminuída.

- **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.

Você também especifique um modo de retenção padrão e um período de retenção padrão para o bucketpode . Eles são aplicados a cada objeto adicionado ao bucket que não especifica suas próprias configurações de retenção.

Para obter detalhes sobre essas configurações, Use o bloqueio de objetos S3D.consulte .

#### 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, consulte o artigo da base de dados de Conhecimento da NetApp.

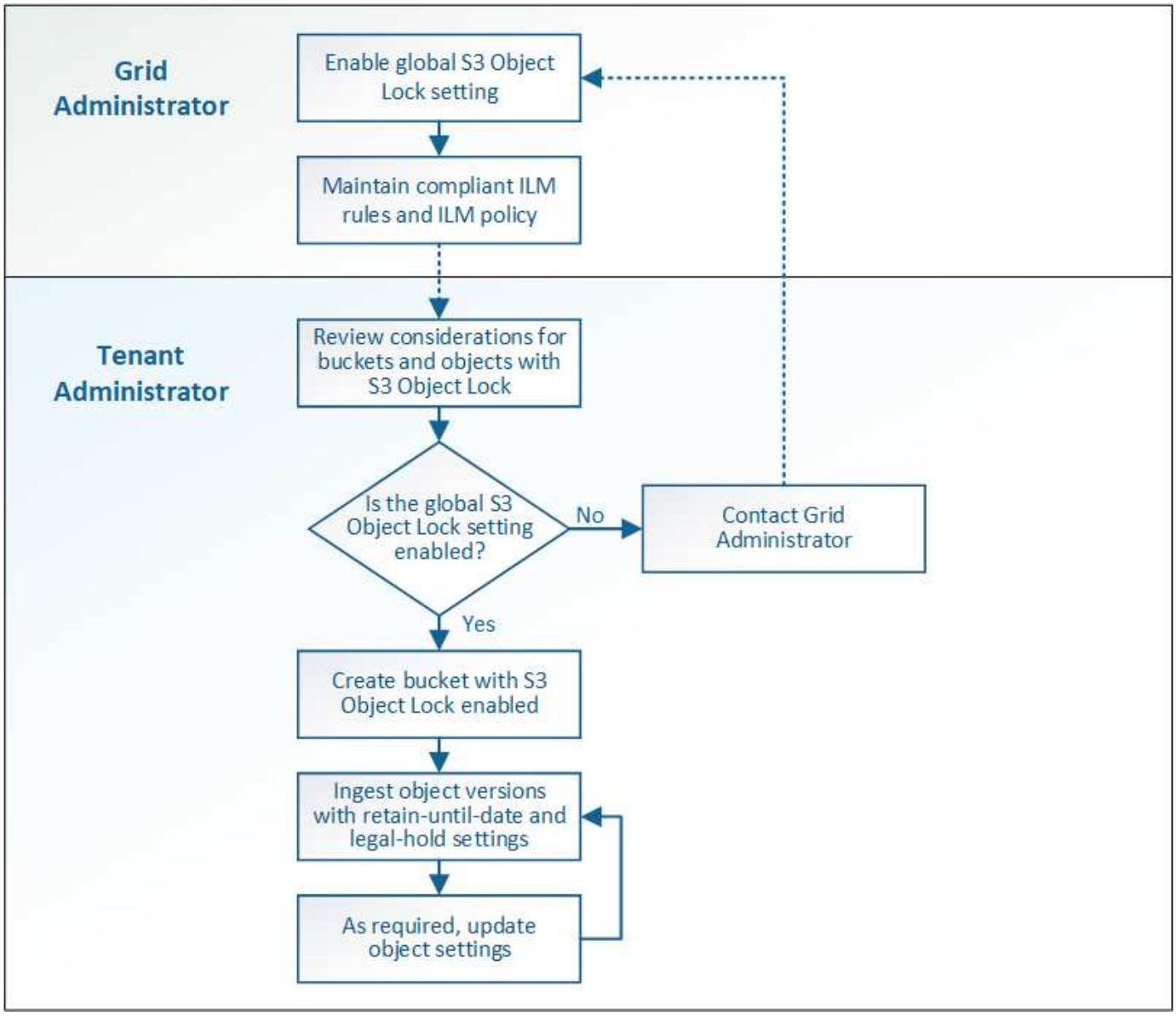
"Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

#### 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 o Política de gerenciamento do ciclo de vida das informações (ILM) seja "compatível"; ele deve atender aos requisitos dos buckets com o bloqueio de objeto S3 ativado. Para obter detalhes, entre em Contato com o administrador da grade ou consulte as instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.

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



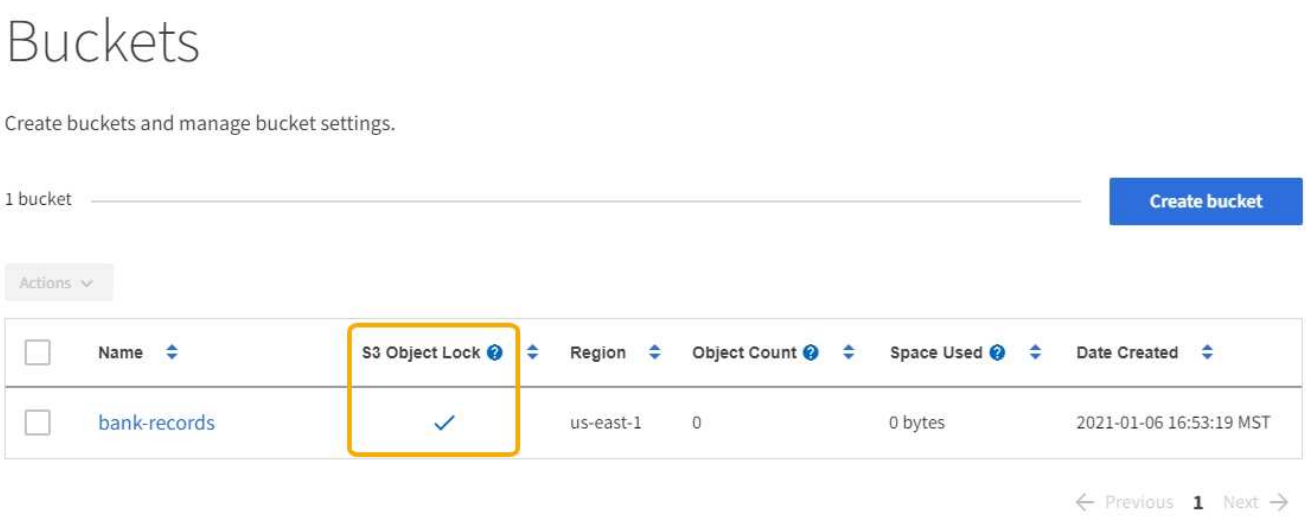

**Requisitos para o bloqueio de objetos S3**

Antes de ativar o bloqueio de objeto S3 para um bucket, revise os requisitos para buckets e objetos do bloqueio de objeto S3 e o ciclo de vida dos objetos em buckets com o bloqueio de objeto S3 ativado.

### 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.

  Este exemplo do Gerenciador do Locatário mostra um bucket 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 S3D para um bucket existente.
- O controle de versão do bucket é necessário com o S3 Object Lock. Quando o bloqueio de objeto S3 está ativado para um bucket, o StorageGRID ativa automaticamente o controle de versão desse bucket.
- Depois de criar um bucket com o bloqueio de objetos S3 ativado, não é possível desativar o bloqueio de objetos S3 ou suspender o controle de versão desse bucket.
- Opcionalmente, você pode configurar a retenção padrão para um bucket. Quando uma versão de objeto é carregada, a retenção padrão é aplicada à versão do objeto. Você pode substituir o intervalo padrão especificando um modo de retenção e manter até a data na solicitação para carregar uma versão de objeto.
- A configuração do ciclo de vida do bucket é compatível com buckets do ciclo de vida do objeto do S3.
- 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, o aplicativo cliente S3 deve configurar a retenção padrão de bucket ou especificar configurações de retenção em cada solicitação de upload.
- Você pode aumentar a data de retenção até uma versão de objeto, mas nunca pode diminuir esse valor.
- Se você for notificado de uma ação legal pendente ou investigação regulatória, poderá preservar informações relevantes colocando uma retenção legal em uma versão de objeto. Quando uma versão de objeto está sob uma retenção legal, esse objeto não pode ser excluído do StorageGRID, mesmo que tenha atingido sua data de retenção até. Assim que a retenção legal for levantada, a versão do objeto pode ser excluída se a data de retenção for atingida.
- S3 Object Lock requer o uso de buckets versionados. 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 três estágios:

1. * Ingestão de objetos*

- Ao adicionar uma versão de objeto a um bucket com o bloqueio de objeto S3 ativado, o aplicativo cliente S3 pode, opcionalmente, especificar configurações de retenção para o objeto (reter até a data, retenção legal ou ambos). Em seguida, o StorageGRID gera metadados para esse objeto, que inclui um identificador de objeto exclusivo (UUID) e a data e hora de ingestão.
- Depois que uma versão de objeto com configurações de retenção é ingerida, seus dados e metadados S3 definidos pelo usuário não podem ser modificados.
- O StorageGRID armazena os metadados do objeto independentemente dos dados do objeto. Ele mantém três cópias de todos os metadados de objetos em cada local.

2. **Retenção de objetos**
   - Várias cópias do objeto são armazenadas pelo StorageGRID. O número exato e o tipo de cópias e os locais de storage são determinados pelas regras em conformidade na política de ILM ativa.
3. **Exclusão de objeto**
   - Um objeto pode ser excluído quando sua data de retenção é alcançada.
   - Não é possível eliminar um objeto que esteja sob uma guarda legal.

**Crie um balde S3D.**

Você pode usar o Gerenciador do locatário para criar buckets do S3 para dados de objetos. Ao criar um intervalo, você deve especificar o nome e a região do intervalo. Se a configuração global de bloqueio de objetos S3D estiver ativada para o sistema StorageGRID, você poderá ativar opcionalmente o bloqueio de objetos S3D para o bucket.

**O que você vai precisar**

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

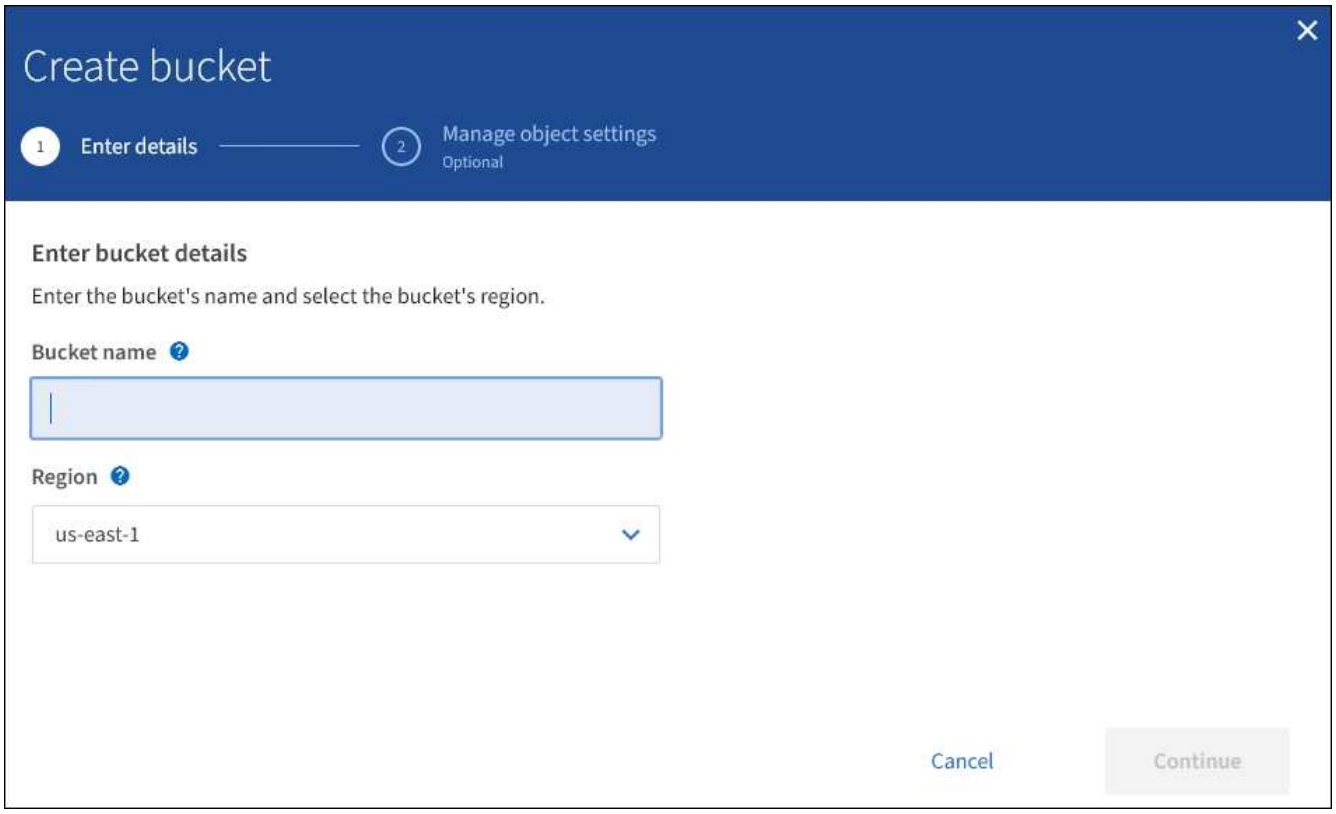
> As permissões para definir ou modificar as propriedades de bloqueio de objetos S3D de buckets ou objetos podem ser concedidas pelo política de bucket ou política de grupo.

- Se você planeja criar um bucket com o bloqueio de objeto S3, 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.

**Passos**

1. Selecione **STORAGE (S3)** > **Buckets**.
2. Selecione **criar bucket**.




3. Introduza um nome exclusivo para o intervalo.

   Não é possível alterar o nome do bucket depois de criar o bucket.

   Os nomes dos buckets devem cumprir com estas regras:

   - Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário).
   - Deve ser compatível com DNS.
   - Deve conter pelo menos 3 e não mais de 63 carateres.
   - Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens.
   - Não deve usar períodos em solicitações de estilo hospedadas virtuais. Os períodos causarão problemas com a verificação do certificado curinga do servidor.

   Para obter mais informações, consulte "Documentação da Amazon Web Services (AWS) sobre regras de nomenclatura de bucket" .

4. Selecione a região para este intervalo.

   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.

   Não é possível alterar a região depois de criar o intervalo.

5. Selecione **continuar**.
6. 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.

7. Se a seção S3 Object Lock aparecer, ative opcionalmente o S3 Object Lock para o bucket.

   Não é possível ativar ou desativar o bloqueio de objetos S3 depois de criar o bucket.

   A seção S3 Object Lock (bloqueio de objetos) só será exibida se a configuração global S3 Object Lock estiver ativada.

   O bloqueio de objetos S3 deve ser ativado para o bucket antes que um aplicativo cliente S3 possa especificar as configurações de retenção legal e de retenção para os objetos adicionados ao bucket.

   Se você ativar o bloqueio de objeto S3 para um bucket, o controle de versão do bucket será ativado automaticamente. Você também pode especifique um modo de retenção padrão e um período de retenção padrão para o bucketaplicar a cada objeto ingerido ao bucket que não especifica suas próprias configurações de retenção.

8. Selecione **criar bucket**.

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

**Informações relacionadas**

Gerenciar objetos com ILM

Entenda a API de gerenciamento do locatário

Use S3

### Veja os detalhes do balde S3

Você pode exibir uma lista dos buckets e configurações do bucket em sua conta de locatário.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.

**Passos**

1. Selecione **STORAGE (S3)** > **Buckets**.

   A página Buckets é exibida e lista todos os buckets da conta de locatário.


2. Reveja as informações de cada balde.

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

   - Nome: O nome exclusivo do bucket, que não pode ser alterado.
   - S3 Object Lock: Se o S3 Object Lock está ativado para este bucket.

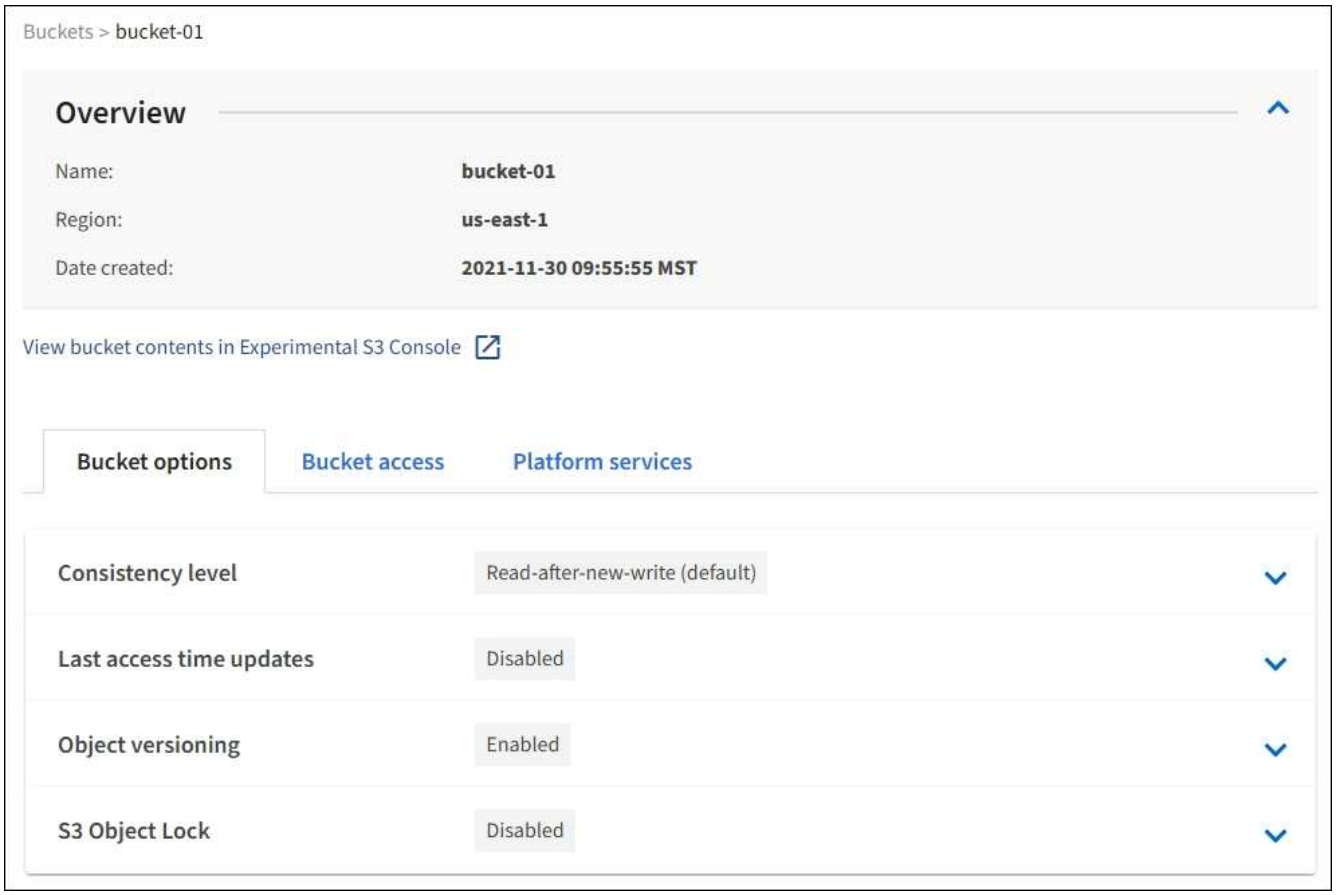
     Esta coluna não será exibida se a configuração global de bloqueio de objetos S3D estiver desativada. Esta coluna também mostra informações para quaisquer buckets em conformidade com o legado.

   - Região: A região do balde, que não pode ser alterada.
   - Contagem de objetos: O número de objetos neste intervalo.
   - Espaço usado: O tamanho lógico de todos os objetos neste 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.

   > 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. Para ver e gerir as definições de um intervalo, selecione o nome do intervalo.

   A página de detalhes do balde permite visualizar e editar as definições das opções do balde, acesso ao balde e serviços de plataforma.




### Altere o nível de consistência

Se você estiver usando um locatário do S3, poderá usar o Gerenciador do Locatário ou a API de Gerenciamento do Locatário para alterar o controle de consistência para operações executadas nos objetos nos buckets do S3.

#### O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root. Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket. Permissões de gerenciamento do locatárioConsulte .

#### Sobre esta tarefa

O nível de consistência fornece um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de storage e locais. Em geral, você deve usar o nível de consistência **Read-after-novo-write** para seus buckets.

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

> Quando você altera o nível de consistência de um balde, apenas os objetos que são ingeridos após a alteração são garantidos para atender ao nível revisado.

#### Passos

1. Selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do intervalo na lista.

   É apresentada a página de detalhes do balde.

3. Selecione **Opções de balde nível de consistência**.
4. Selecione um nível de 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**.

#### 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** nas instruções de colocação. Você pode ignorar essas instruções se o seu sistema StorageGRID não incluir essa regra.

##### O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root. Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket. Permissões de gerenciamento do locatárioConsulte .

**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.

> Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

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 |

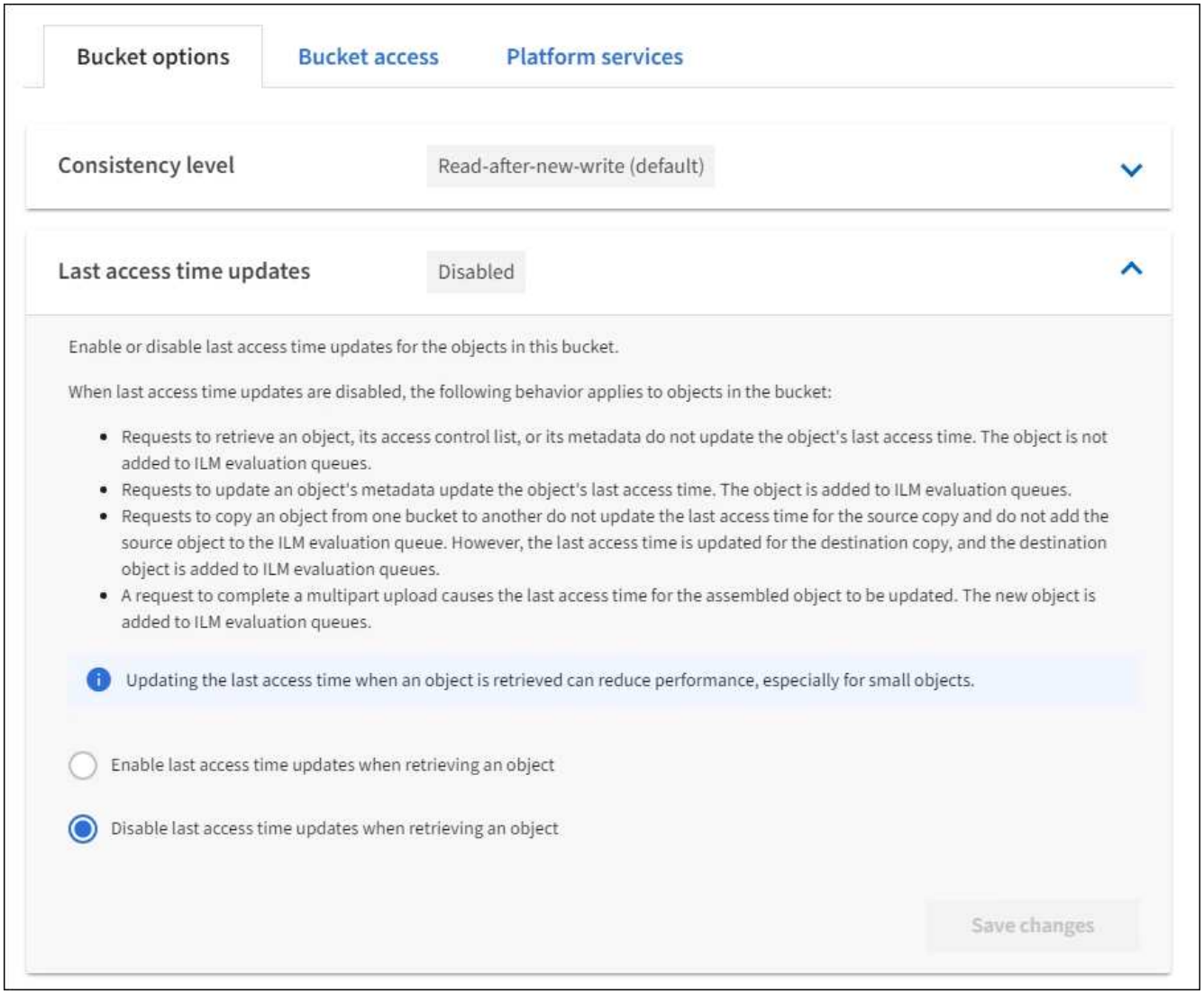
| | | | | |
|---|---|---|---|---|
| Pedido para concluir um carregamento multipart | Sim, para o objeto montado | Sim, para o objeto montado | Sim, para o objeto montado | Sim, para o objeto montado |

**Passos**

1. Selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do intervalo na lista.

   É apresentada a página de detalhes do balde.

3. Selecione **Opções de intervalo atualizações do último tempo de acesso**.
4. Selecione o botão de opção apropriado para ativar ou desativar as atualizações da última hora de acesso.




5. Selecione **Salvar alterações**.

**Informações relacionadas**

Permissões de gerenciamento do locatário

Gerenciar objetos com ILM

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

Se você estiver usando um locatário do S3, poderá usar o Gerenciador do locatário ou a API de gerenciamento do locatário para alterar o estado de controle de versão para buckets do S3.

#### O que você vai precisar

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

  Permissões de gerenciamento do locatário

#### 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.

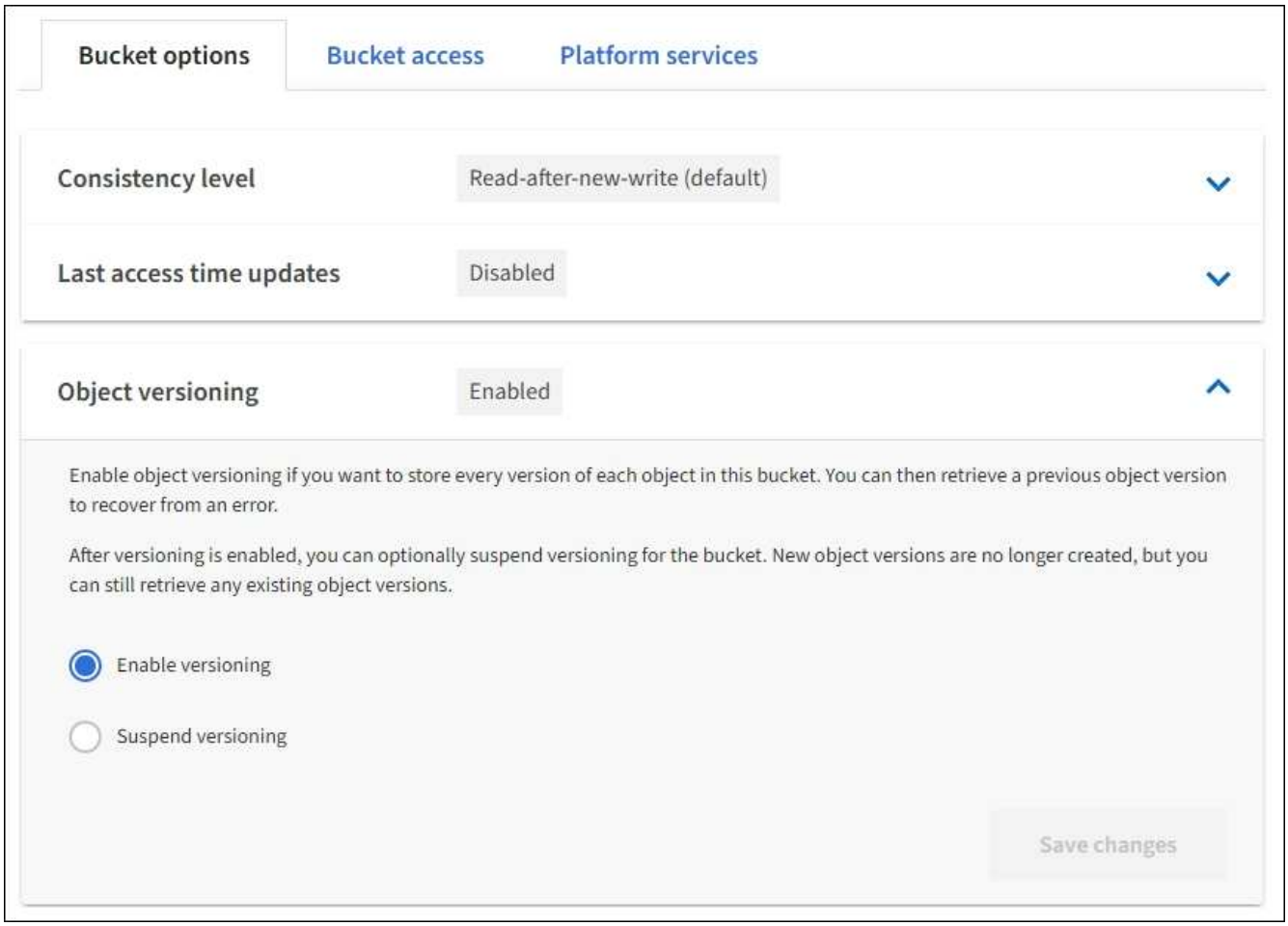
- Desativado: O controle de versão nunca foi habilitado
- Habilitado: O controle de versão está habilitado
- Suspenso: O controle de versão foi ativado anteriormente e está suspenso

Controle de versão de objeto S3

Regras e políticas do ILM para objetos com versão S3 (exemplo 4)

#### Passos

1. Selecione **STORAGE (S3)** > **Buckets**.
2. Selecione o nome do intervalo na lista.
3. Selecione **Opções de balde versão de objetos**.




4. Selecione um estado de controle de versão para os objetos neste intervalo.

> 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**.

#### Configurar a partilha 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.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou 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 de 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`.

**Passos**

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

   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>
   ```

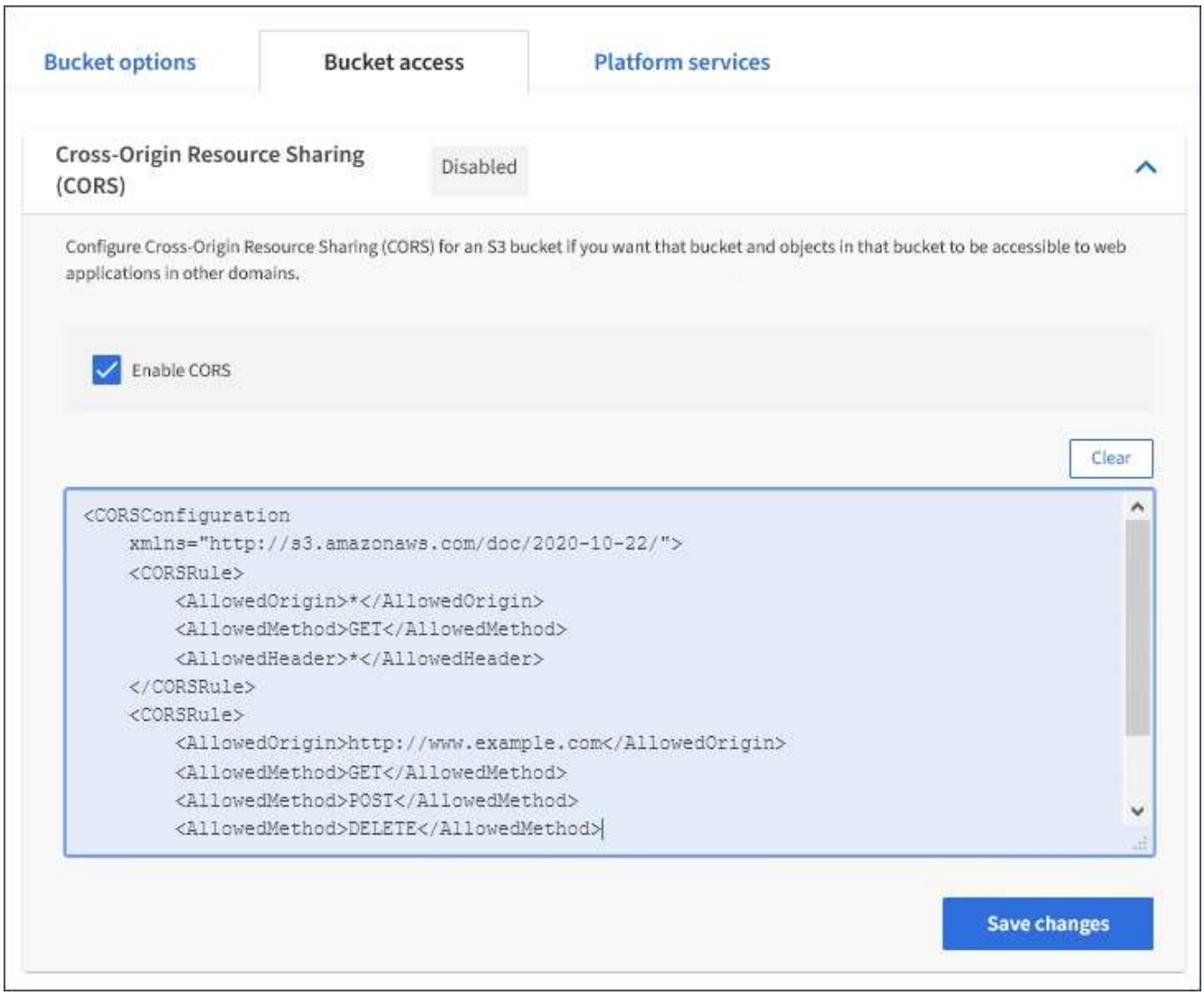
   Para obter mais informações sobre o XML de configuração do CORS, "Documentação do Amazon Web Services (AWS): Guia do desenvolvedor do Amazon Simple Storage Service" consulte .

2. No Gerenciador do Locatário, selecione **STORAGE (S3) Buckets**.
3. Selecione o nome do intervalo na lista.

   É apresentada a página de detalhes do balde.

4. Selecione **Bucket Access Cross-Origin Resource Sharing (CORS)**.

5. Marque a caixa de seleção **Enable CORS** (Ativar VRF*).
6. Cole o XML de configuração do CORS na caixa de texto e selecione **Salvar alterações**.




7. Para modificar a configuração CORS para o bucket, atualize o XML de configuração do CORS na caixa de texto ou selecione **Limpar** para recomeçar. Em seguida, selecione **Salvar alterações**.
8. Para desativar o CORS para o bucket, desmarque a caixa de seleção **Ativar CORS** e selecione **Salvar alterações**.

### Eliminar o balde S3

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

#### O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root. Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket. Permissões de gerenciamento do locatárioConsulte .
- Os intervalos que você deseja excluir estão vazios.

**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 ou versões de objetos não atuais. Para obter informações sobre como os objetos com versão S3 são excluídos, consulte instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

**Passos**

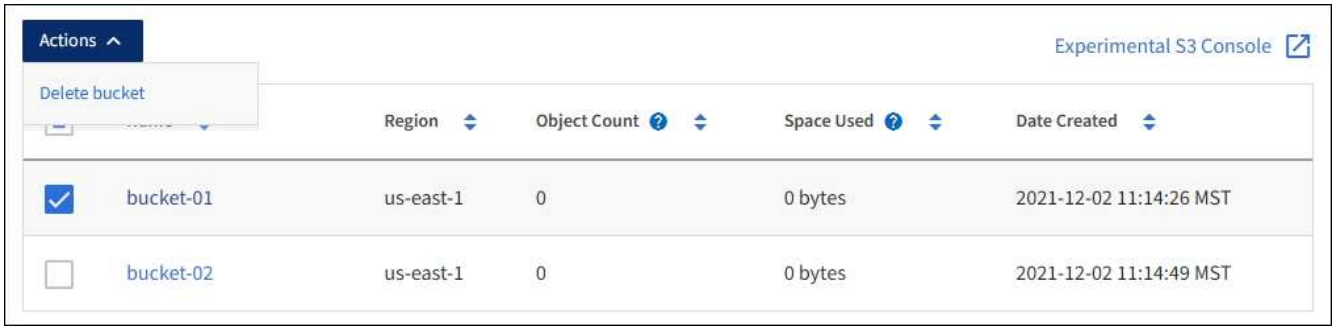
1. Selecione **STORAGE (S3)** > **Buckets**.

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


2. Marque a caixa de seleção do intervalo vazio que deseja excluir. Pode selecionar mais de um balde de cada vez.

   O menu ações está ativado.

3. No menu ações, selecione **Excluir bucket** (ou **Excluir buckets** se você tiver escolhido mais de um).




4. Quando a caixa de diálogo de confirmação for exibida, selecione **Sim** para excluir todos os buckets escolhidos.

   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 excluir todos os objetos antes de excluir um bucket.

### Use o experimental S3 Console

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

Você também pode usar o console S3 para fazer o seguinte:

- Adicione e exclua objetos, versões de objetos e pastas
- Renomeie objetos
- Mover e copiar objetos entre buckets e pastas
- Gerenciar tags de objeto
- Exibir metadados de objetos
- Transferir objetos

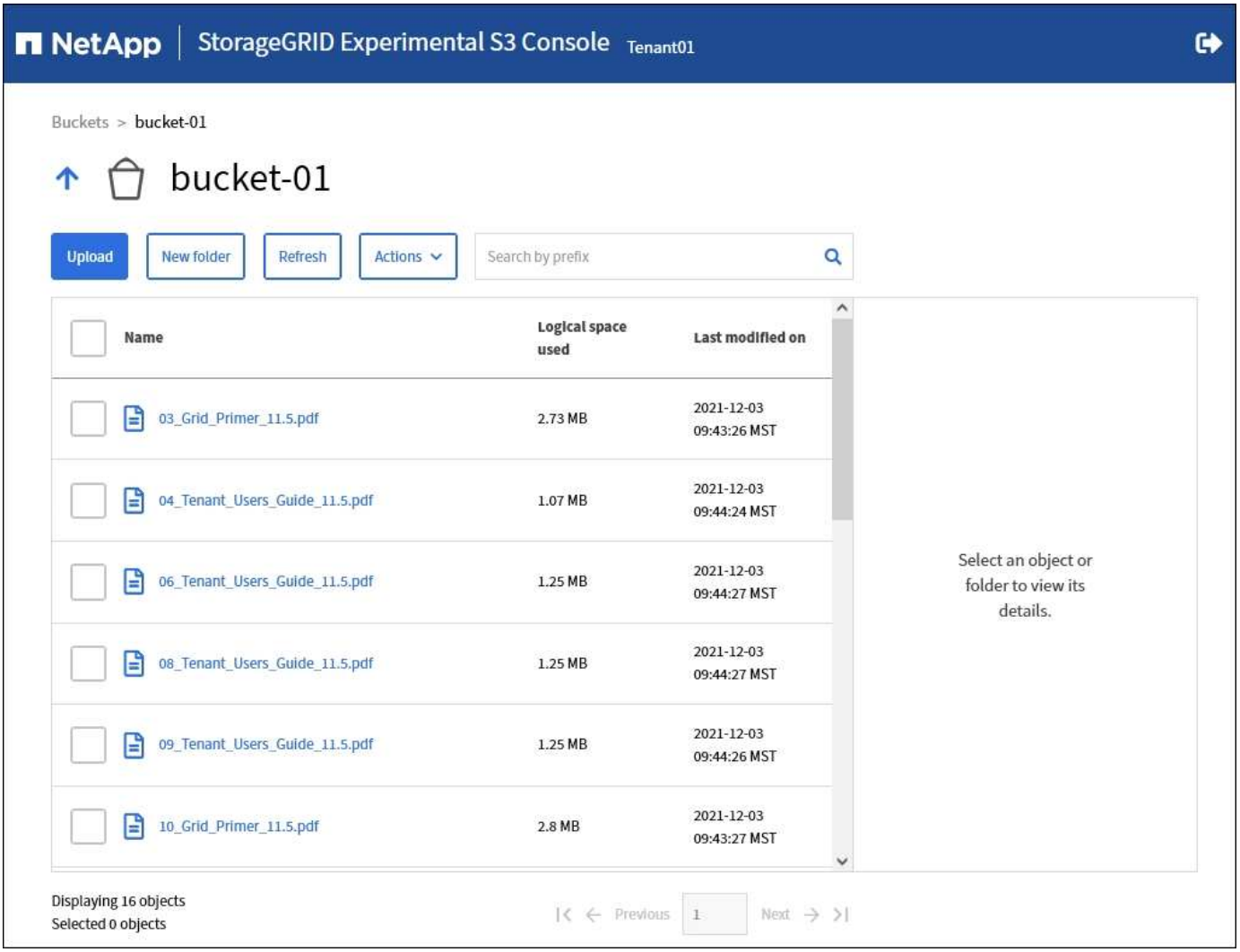
> O console S3 não foi totalmente testado e está marcado como "experimental". Não se destina ao gerenciamento em massa de objetos ou para uso em um ambiente de produção. Os locatários só devem usar o Console S3 ao executar funções para um pequeno número de objetos, como ao carregar objetos para simular uma nova política de ILM, solucionar problemas de ingestão ou usar grades de prova de conceito ou não de produção.

**O que você vai precisar**

- Você está conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você tem a permissão Gerenciar suas próprias credenciais S3.
- Você criou um bucket.
- 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 **baldes**.
2. Experimental S3 Console Selecione . Você também pode acessar este link a partir da página de detalhes do bucket.
3. Na página experimental de login do Console S3, 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. Gerencie objetos conforme necessário.




# Gerenciar os serviços da plataforma S3

## O que são serviços de plataforma?

Os serviços de plataforma da StorageGRID podem ajudar você a implementar uma estratégia de nuvem híbrida.

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**: O Serviço de replicação do StorageGRID CloudMirror é usado 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**: Notificações de eventos por bucket São usadas para enviar notificações sobre ações específicas executadas em objetos para um Amazon Simple Notification Service (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**: O serviço de integração de pesquisa é usado 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 Gerenciador do locatário ou a 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 serviço de notificação simples (SNS) ou um cluster do Elasticsearch hospedado localmente, na AWS ou em outro lugar.

Depois de criar um endpoint, 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:

1. 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.

2. Se você também quiser enviar notificações quando esses objetos estiverem armazenados no bucket, adicione uma configuração de notificações.
3. 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 |
|---|---|
| Replicação do CloudMirror | • OBTER replicação do bucket<br>• COLOQUE a replicação do balde |
| Notificações | • OBTER notificação Bucket<br>• COLOCAR notificação de balde |
| Integração de pesquisa | • OBTER configuração de notificação de metadados do bucket<br>• COLOQUE a configuração de notificação de metadados do bucket<br>Essas operações são personalizadas para o StorageGRID. |

Consulte as instruções para implementar aplicativos cliente S3 para obter detalhes sobre como o StorageGRID implementa essas APIs.

**Informações relacionadas**

Considerações sobre o uso de serviços de plataforma

Use S3

**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 da política de ILM ativa 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.

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 AWS 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. Você não pode 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 bucket de destino, o StorageGRID os marca como "replicas". 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 SNS (Serviço de notificação simples) do Amazon de destino.

Você pode configurar notificações de eventosassociar 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 SNS de destino 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

A notificação de eventos do StorageGRID segue a API do Amazon S3 com as seguintes limitações:

- Não é possível configurar uma notificação para os seguintes tipos de eventos. Esses tipos de eventos são **não** suportados.
  - `s3:ReducedRedundancyLostObject`
  - `s3:ObjectRestore:Completed`
- As notificações de eventos enviadas do StorageGRID usam o formato JSON padrão, exceto que elas não incluem algumas chaves e usam valores específicos para outras, como mostrado na 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 sobre o uso de 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 S3consulte .

**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 dos serviços AWS CRR e SNS, 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. |

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

| Consideração | Detalhes |
| --- | --- |
| Estado da replicação | O StorageGRID não suporta o `x-amz-replication-status` colhedor. |

| Consideração | Detalhes |
| --- | --- |
| 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 operação de um único objeto PUT 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. |
| Marcação para versões de objetos | O serviço CloudMirror não replica nenhuma solicitação de marcação PUT Object ou EXCLUI solicitações de marcação de objetos que forneçam um 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 de marcação DE objetos ou EXCLUI solicitações de marcação de objetos 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 bucket S3 de destino para replicação do CloudMirror tiver o bloqueio de objetos S3 ativado, a tentativa de configurar a replicação de bucket (PUT Bucket replicação) 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 a permissão Gerenciar endpoints ou acesso root, em uma grade cuja rede foi configurada para permitir que os nós de armazenamento acessem recursos de endpoint externos. 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 AWS 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 AWS.

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 um destino, o que permite que você faça coisas como enviar notificações sobre a criação de objetos para um tópico do SNS e notificações sobre a exclusão de objetos para um segundo tópico do 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 oferece suporte a pontos de extremidade do Serviço de notificação simples (SNS). Os endpoints do Simple Queue Service (SQS) ou do AWS Lambda não são suportados.

### 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. Não é necessário 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 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), `arn:aws` use o .
- Se o serviço estiver hospedado no Google Cloud Platform (GCP), `arn:aws` use o .
- 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 |
| 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 | nome do balde |
| Notificações | sns-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:

```
urn:mysite:sns:optional:optional:sns-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.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar Endpoints.
- O recurso referenciado pelo endpoint de serviços da plataforma deve ter sido criado:
  - Replicação do CloudMirror: Bucket do S3
  - Notificação de evento: Tópico SNS
  - Notificação de pesquisa: Índice Elasticsearch, se o cluster de destino não estiver configurado para criar índices automaticamente.
- Você deve ter 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)

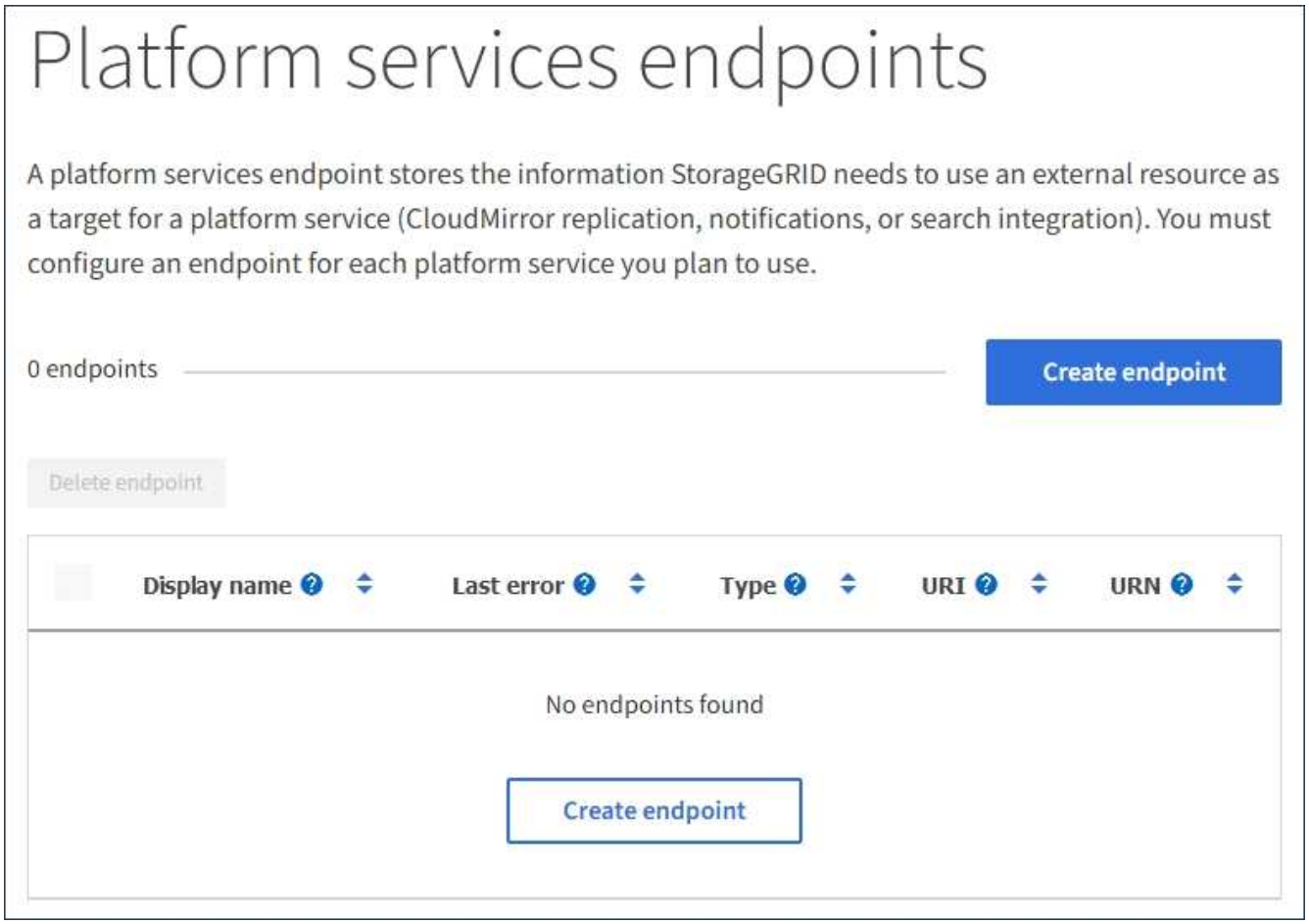
    Especifique URN para endpoint de serviços de plataforma

  - Credenciais de autenticação (se necessário):
    - Chave de acesso: ID da chave de acesso e chave de acesso secreta
    - HTTP básico: Nome de usuário e senha
    - 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.
  - Certificado de segurança (se estiver usando um certificado de CA personalizado)

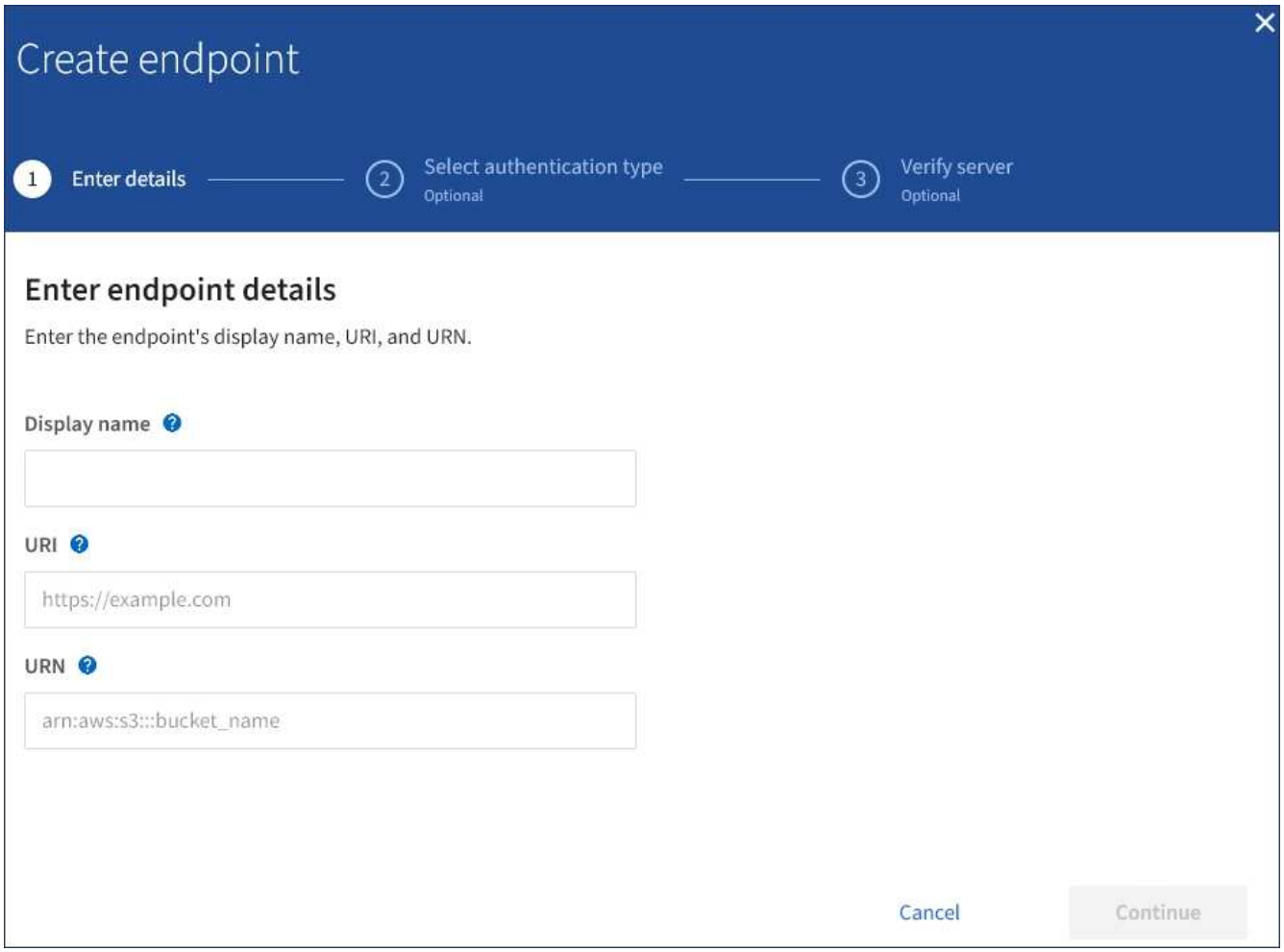
**Passos**

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, portanto, você não precisa 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, a porta 443 será usada para URIs HTTPS e a porta 80 será usada para URIs HTTP.

   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:

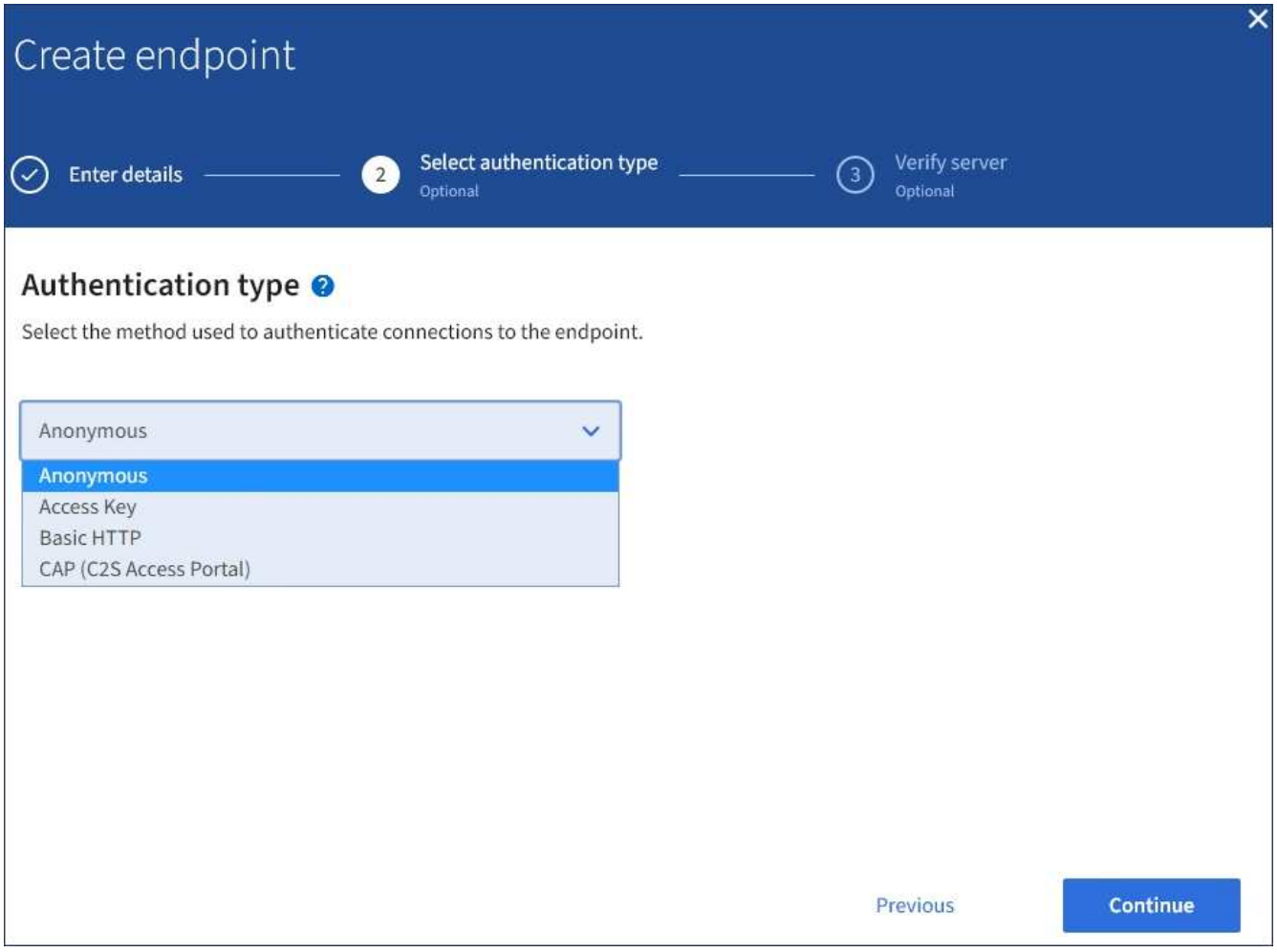
```
https://s3-aws-region.amazonaws.com
```

> 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.

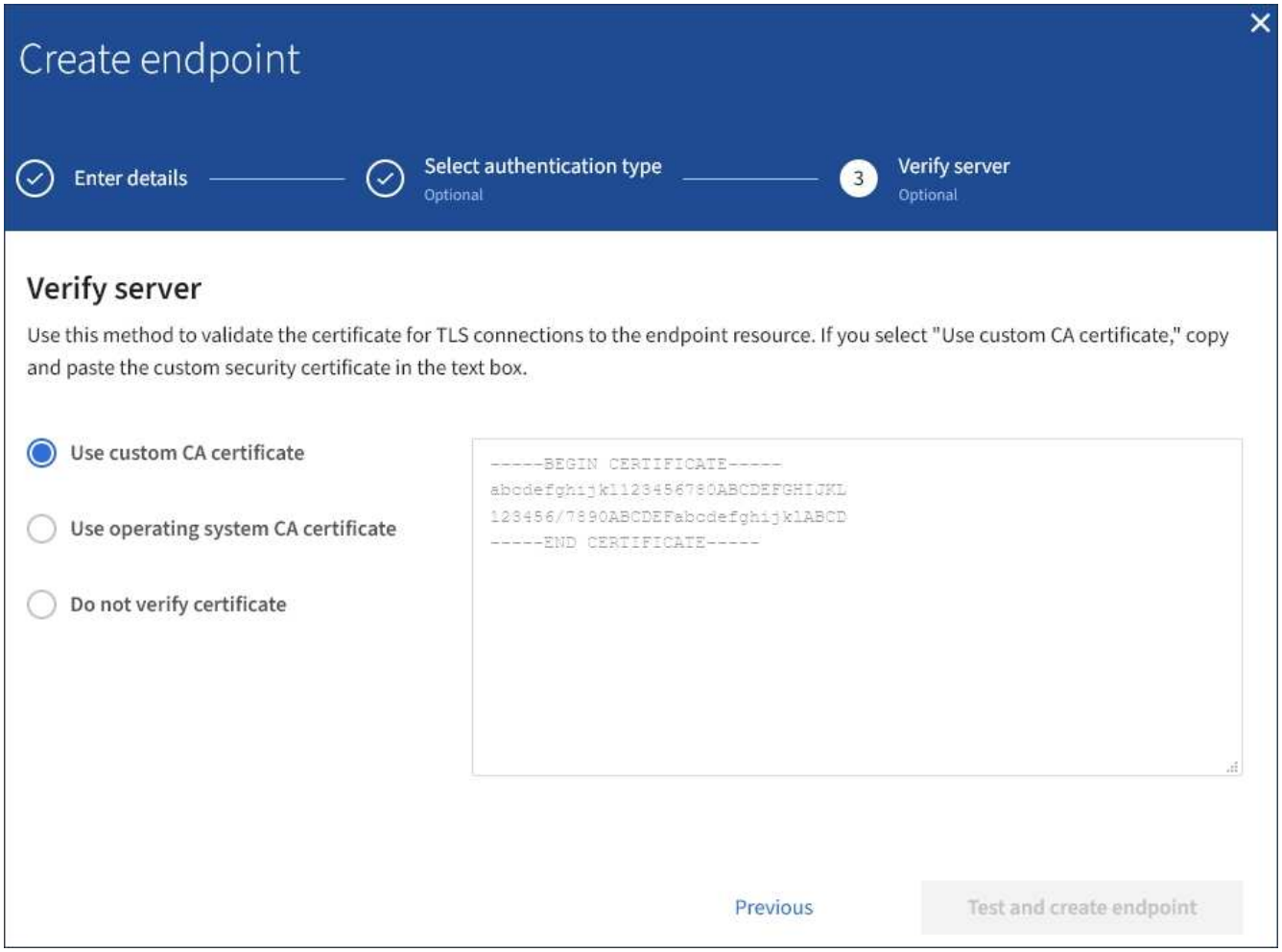
6. Selecione **continuar**.
7. Selecione um valor para **tipo de autenticação** e insira ou carregue as credenciais necessárias.




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 |
| 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) |

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.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar Endpoints.

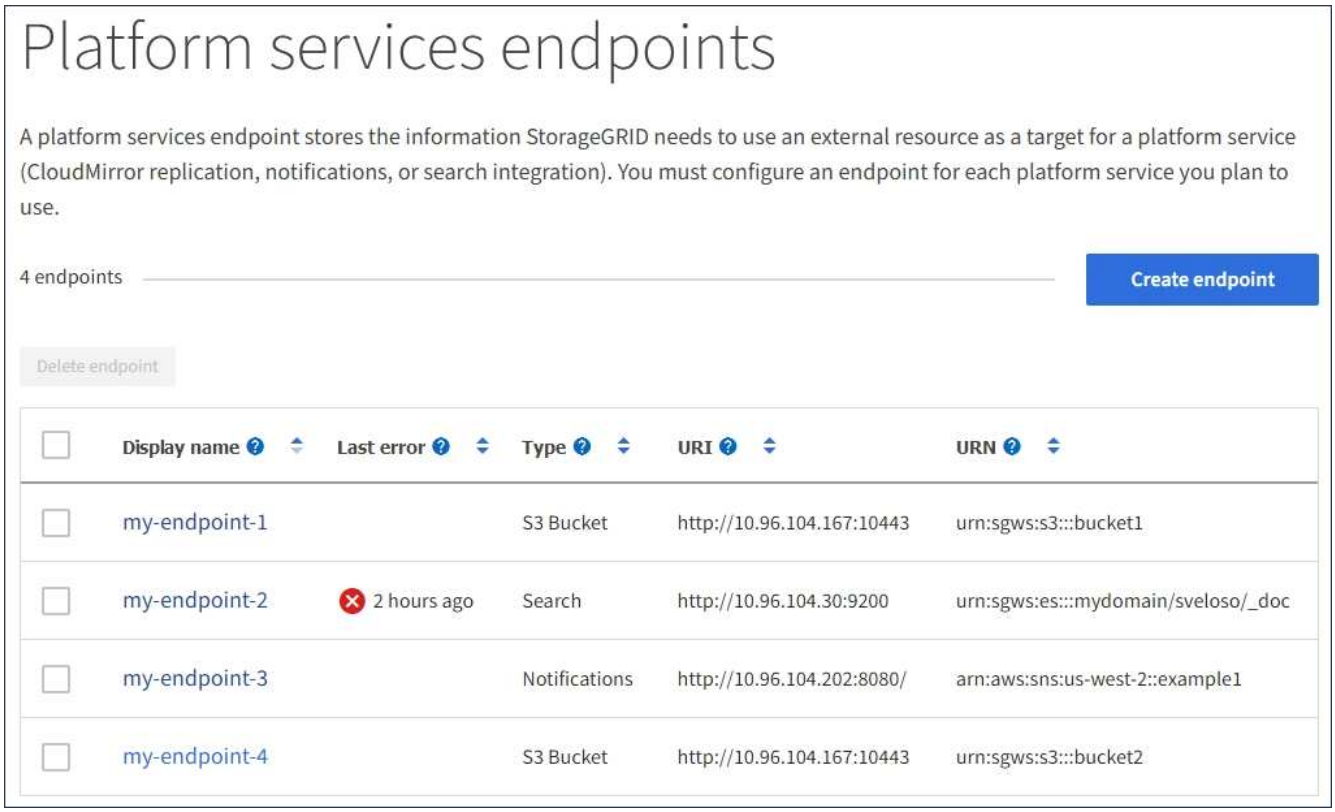
**Sobre esta tarefa**

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

**Passos**

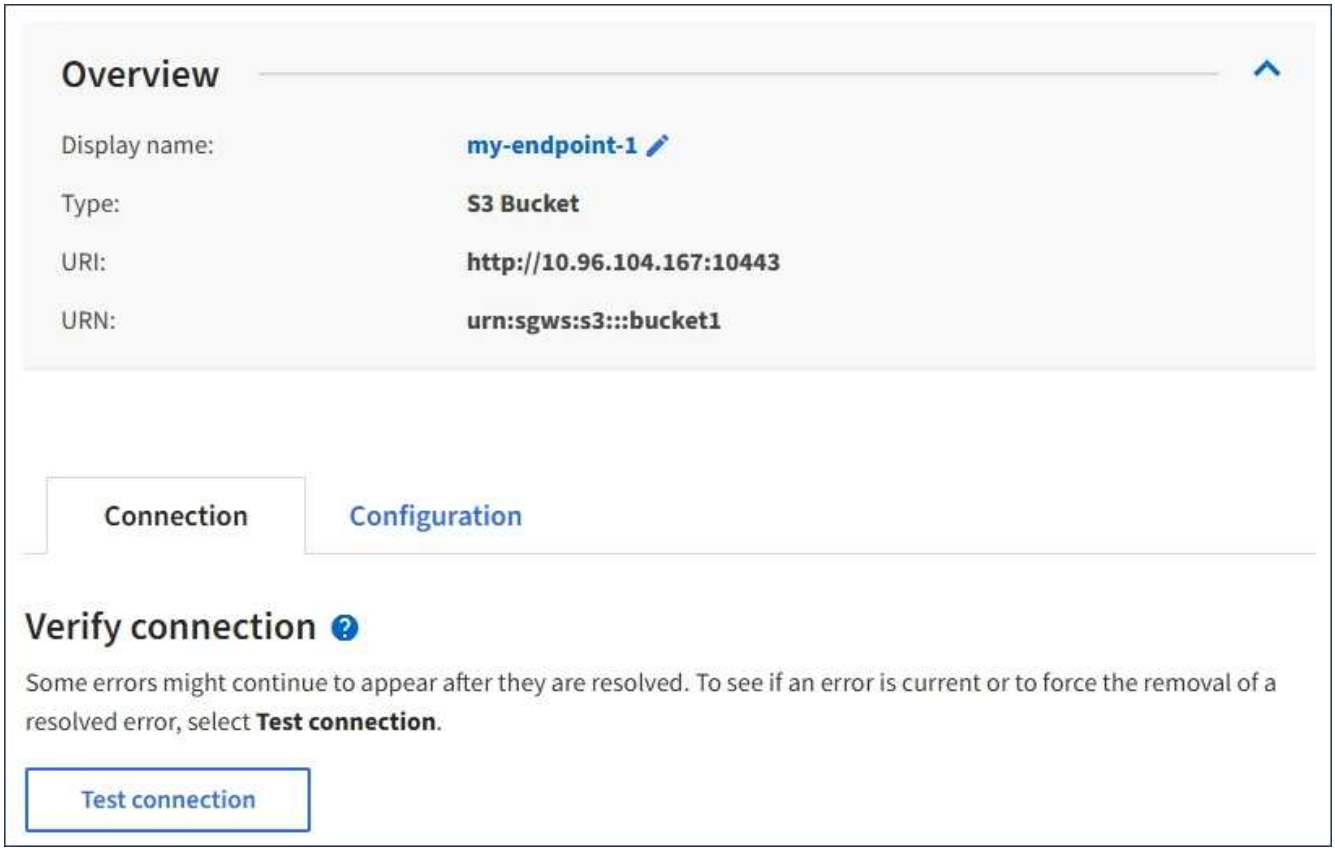
1. Selecione **STORAGE (S3) endpoints de serviços de plataforma**.

   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. Você não pode alterar a URN para um endpoint de serviços de plataforma.

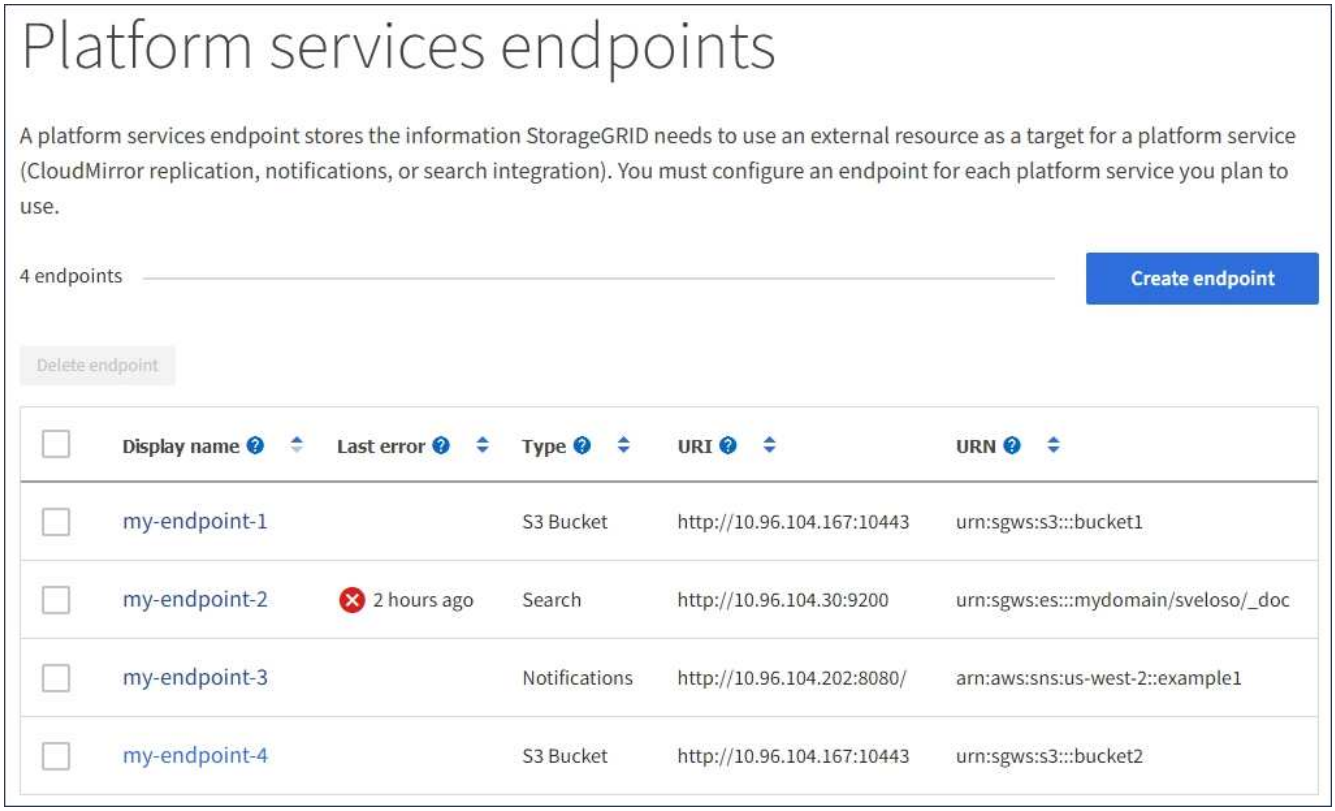
#### O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar Endpoints. Permissões de gerenciamento do locatárioConsulte .

#### Passos

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

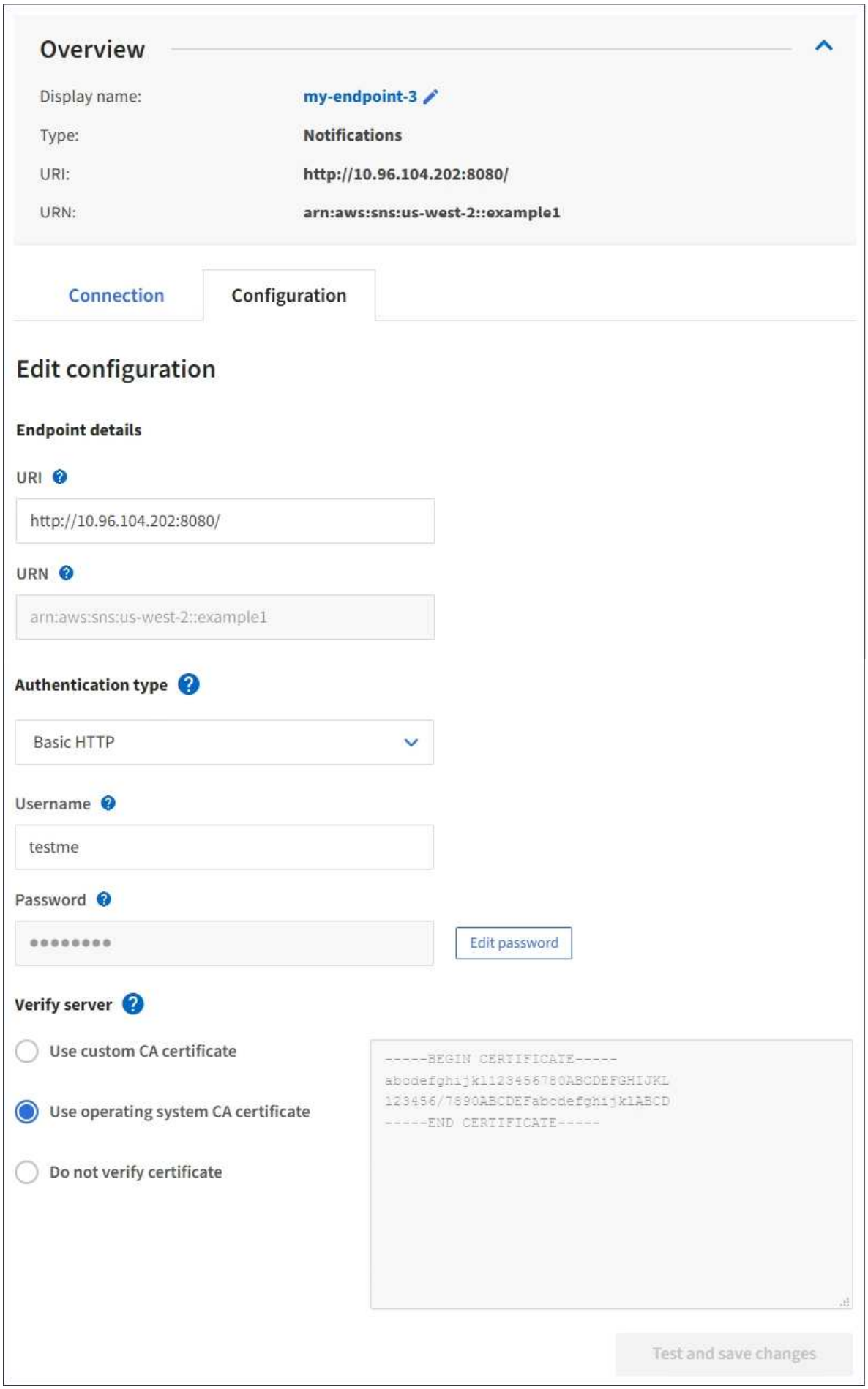
   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.




2. Selecione o ponto de extremidade que pretende editar.

   A página de detalhes do ponto final é exibida.

3. Selecione **Configuração**.


Overview
Display name:
my-endpoint-3
Type:
Notifications
URI:
http://10.96.104.202:8080/
URN:
arn:aws:sns:us-west-2::example1
Connection
Configuration
Edit configuration
Endpoint details
URI
http://10.96.104.202:8080/
URN
arn:aws:sns:us-west-2::example1
Authentication type
Basic HTTP
Username
testme
Password
Edit password
Verify server
Use custom CA certificate
Use operating system CA certificate
Do not verify certificate
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

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 HTTP básica, altere o nome de usuário conforme necessário. Altere a senha conforme necessário selecionando **Editar senha** e inserindo a nova senha. Se você precisar cancelar suas alterações, selecione **Revert password 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.

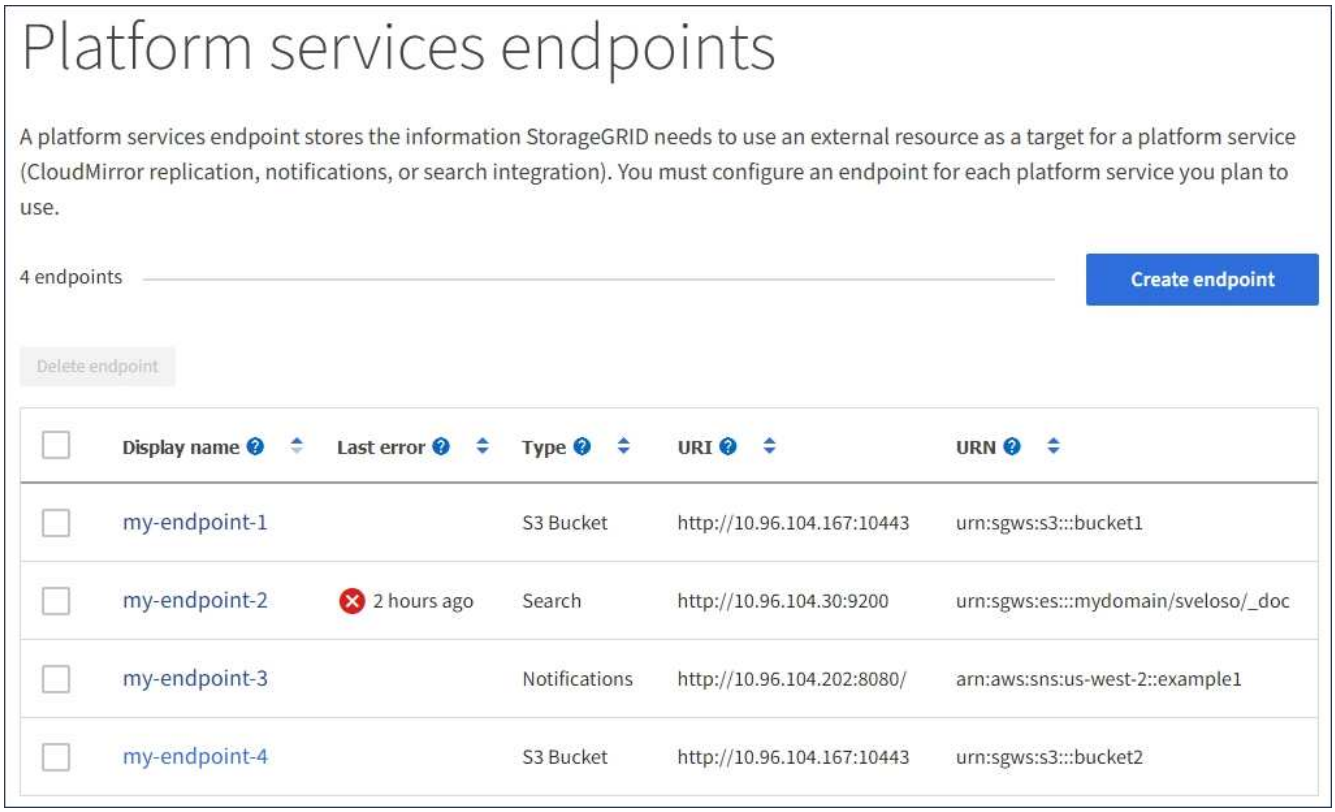
#### O que você vai precisar

- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão **Manage Endpoints**. Permissões de gerenciamento do locatárioConsulte .

#### 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.

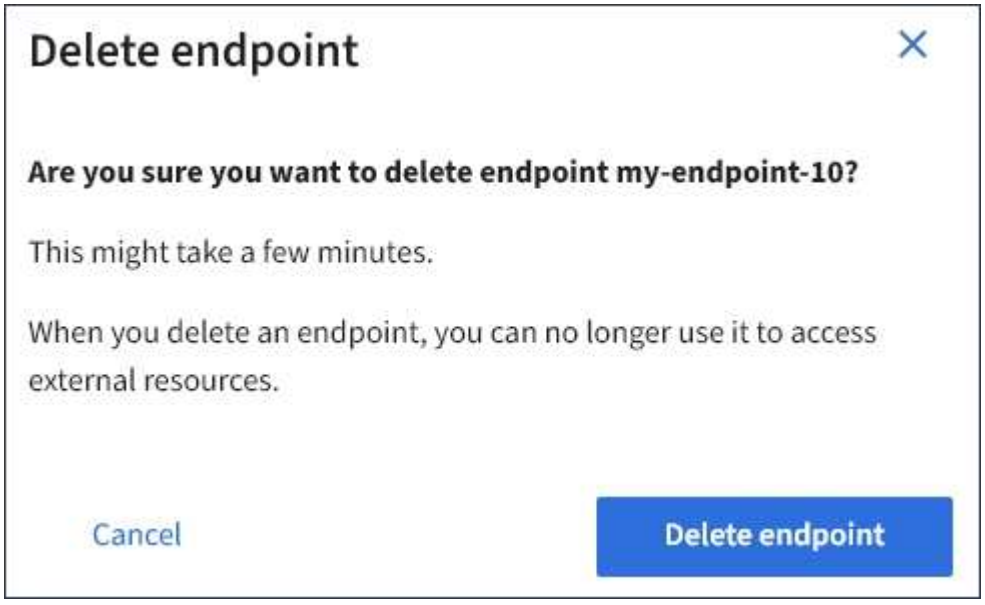



2. Marque a caixa de seleção para cada ponto de extremidade que deseja excluir.

> 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.



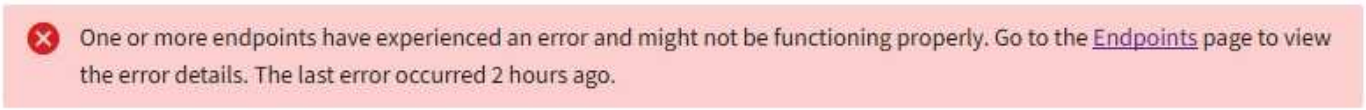
4. Selecione **Excluir endpoint**.

### 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 Dashboard. 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

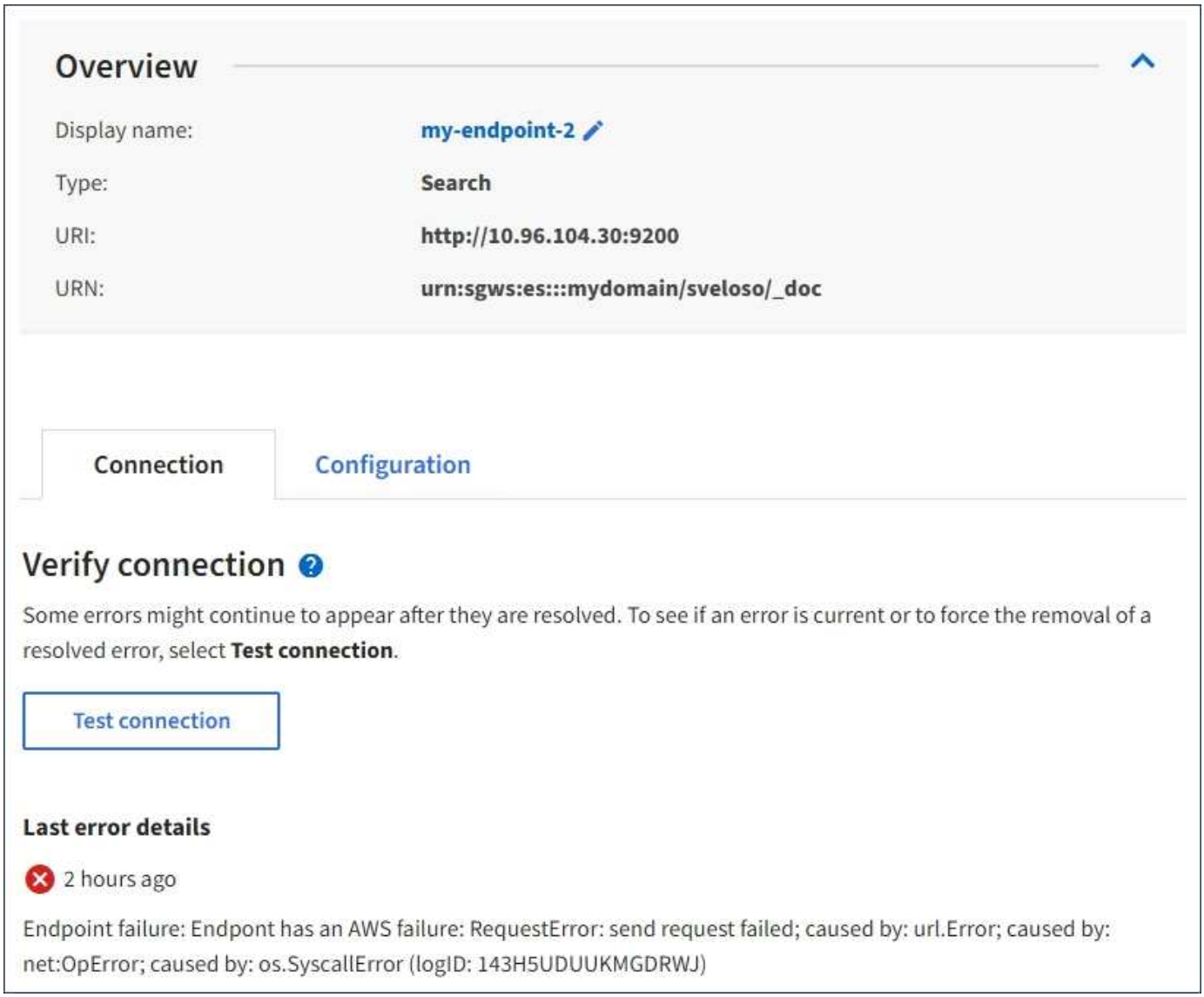
Se algum erro de endpoint de serviços de plataforma tiver ocorrido nos últimos 7 dias, o Painel do Gerenciador do Locatário exibirá uma mensagem de alerta. Você pode acessar a página de endpoints dos serviços da plataforma para ver mais detalhes sobre o erro.




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 do endpoint ou o acesso ao 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.

#### Solução de problemas de serviços de plataforma adicionais

Para obter informações adicionais sobre os serviços de plataforma de solução de problemas, consulte as instruções de administração do StorageGRID.

Administrar o StorageGRID

**Informações relacionadas**

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.

**O que você vai precisar**

- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você já deve ter criado um bucket para agir como a origem da replicação.
- O endpoint que você pretende usar como destino para a replicação do CloudMirror já deve existir, e você deve ter sua URN.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root, que permite gerenciar as configurações de todos os buckets do S3 em sua conta de locatário. 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. Para ativar a replicação do CloudMirror para um bucket, você deve criar e aplicar XML de configuração de replicação de bucket válida. 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, consulte a documentação do Amazon Simple Storage Service (S3) sobre replicação entre regiões (CRR). Para obter informações sobre como o StorageGRID implementa a API de configuração de replicação de bucket do S3, consulte o Instruções para a implementação de aplicativos cliente S3.

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. 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:

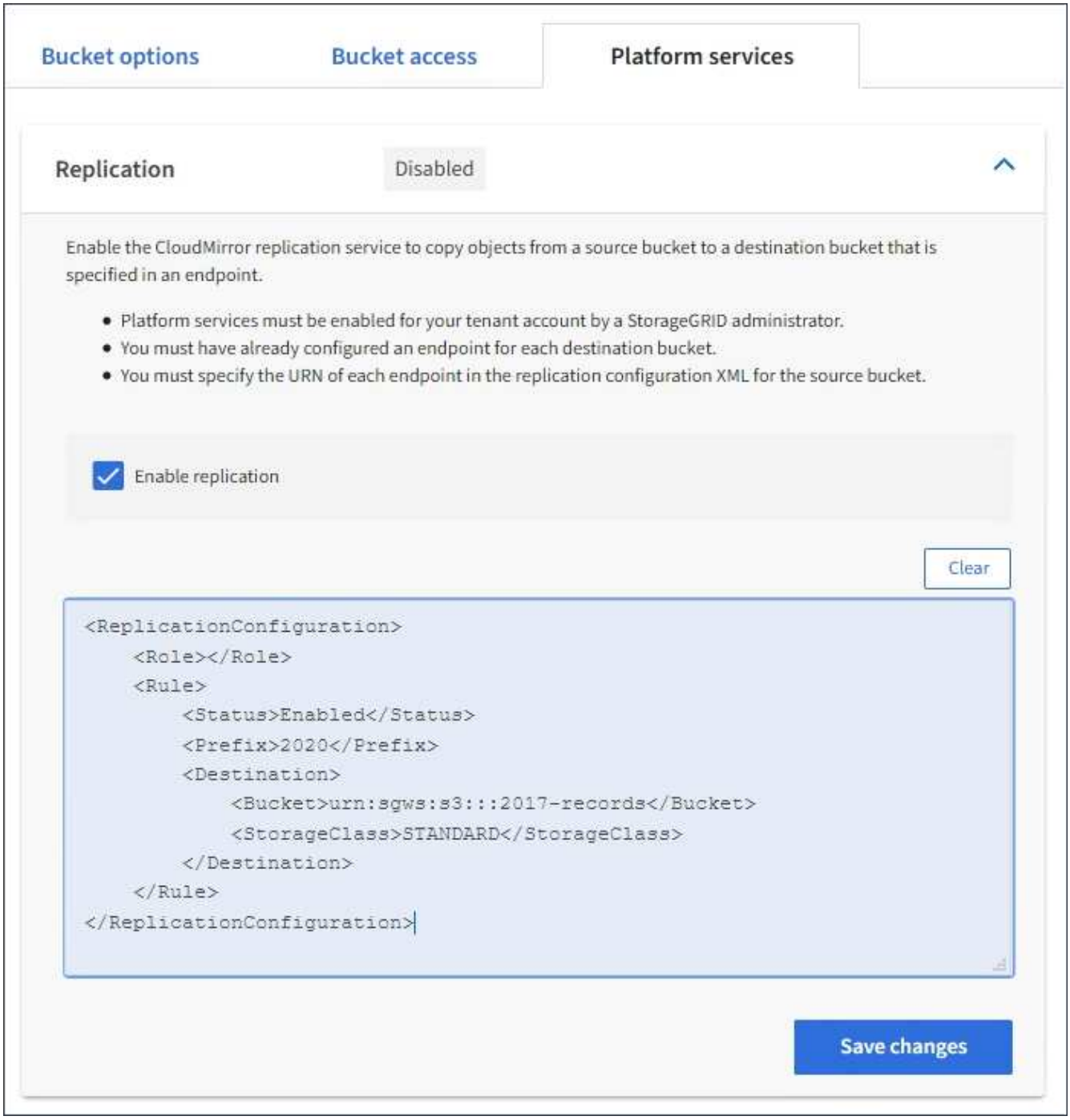
   - Observe que o StorageGRID só suporta V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue convenções V1 para exclusão de versões de objetos. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes.
   - 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. 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 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**

Use S3

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 serviço de destino compatível com o AWS Simple Notification Service (SNS).

**O que você vai precisar**

- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você já deve ter criado um bucket para agir como a fonte das notificações.
- O endpoint que você pretende usar como destino para notificações de eventos já deve existir, e você deve ter sua URNA.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root, que permite gerenciar as configurações de todos os buckets do S3 em sua conta de locatário. 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 as notificações de eventos, sempre que um evento especificado ocorre para um objeto no intervalo de origem, uma notificação é gerada e enviada para o tópico Serviço de notificação simples (SNS) usado como ponto de extremidade 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 as instruções para implementar aplicativos cliente do 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**

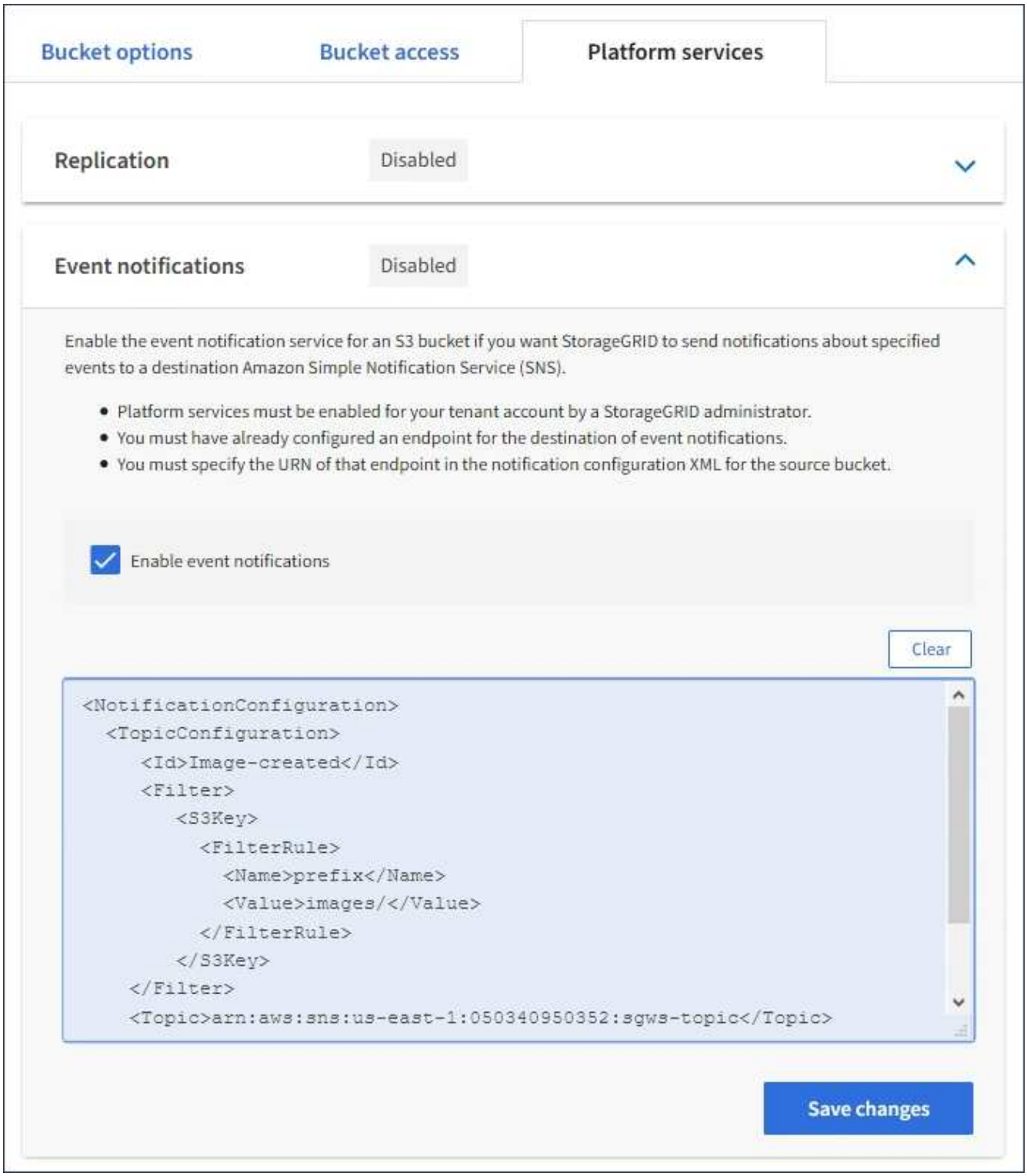
1. Ativar notificações para o intervalo de origem:
    - Use um editor de texto para criar a configuração de notificação XML necessário para habilitar notificações de eventos, conforme especificado na API de notificação S3.
    - Ao configurar o XML, use a URNA de um endpoint de notificações de eventos 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 SNS de destino.

Por exemplo, se o tópico de destino estiver hospedado no AWS Simple Notification Service (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 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:

- EXCLUIR solicitação de configuração de notificação de metadados do bucket
- OBTER solicitação de configuração de notificação de metadados do bucket
- COLOCAR solicitação de 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 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 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.

**O que você vai precisar**

- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você já deve ter criado 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 deve existir, e você deve ter sua URNA.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root, que permite gerenciar as configurações de todos os buckets do S3 em sua conta de locatário. 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**

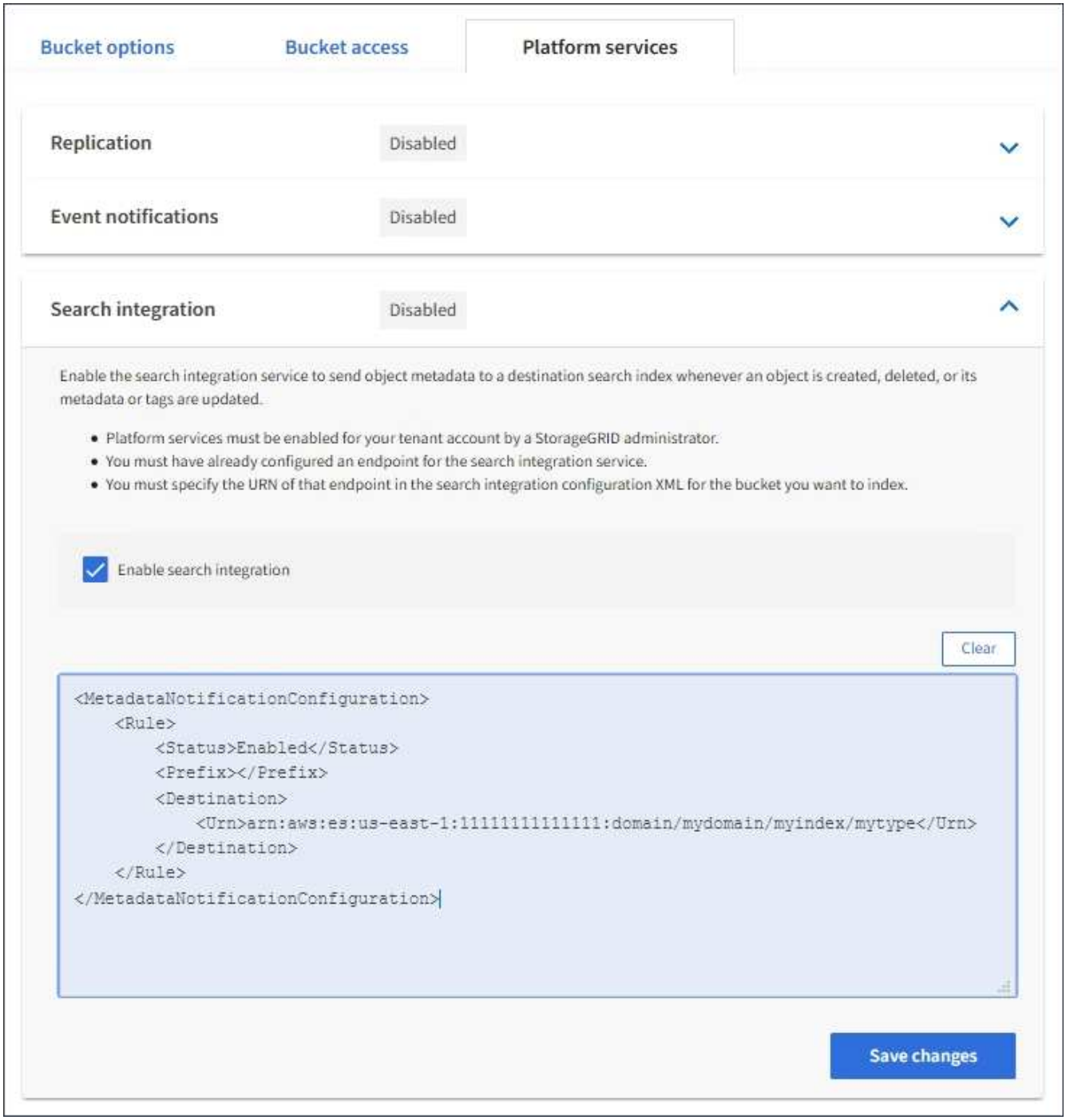
1. Use um editor de texto para criar o XML de notificação de metadados necessário para habilitar a integração de pesquisa.
   - Consulte as informações sobre o XML de configuração para integração de pesquisa.
   - Ao configurar o XML, use a URNA de um endpoint de integração de pesquisa como o destino.

```
<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 **Serviços de plataforma integração de pesquisa**
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 **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 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