Use uma conta de tenant

StorageGRID software

NetApp
July 23, 2026

Índice

Use uma conta de tenant

Use uma conta de locatário do StorageGRID

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

O que é uma conta de tenant?

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

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

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

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

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

Como criar uma conta de locatário

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

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

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

Configurar locatários do S3

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

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

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

Como iniciar sessão e terminar sessão

Faça login no StorageGRID Tenant Manager

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

Antes de começar

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

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

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

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

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

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

Passos

1. Inicie um "navegador web compatível".
2. Na barra de endereços do navegador, digite a URL para acessar o Tenant Manager.
3. Se você receber um alerta de segurança, instale o certificado usando o assistente de instalação do navegador.

4. Faça login no Tenant Manager.

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

   Não usar SSO

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

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

     O painel de controle do Tenant Manager é exibido.

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

   Utilizando SSO

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

   - Página de SSO da sua organização.

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

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

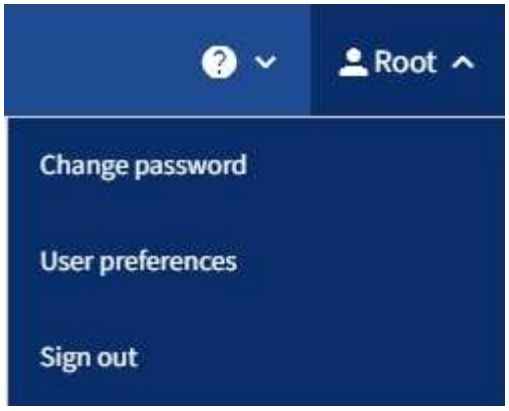
     O painel de controle do Tenant Manager é exibido.

Saia do StorageGRID Tenant Manager

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

Passos

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



2. Selecione o nome de usuário e, em seguida, selecione **Sair**.
   - Se o SSO não estiver em uso:

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

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

   - Se o SSO estiver ativado:

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

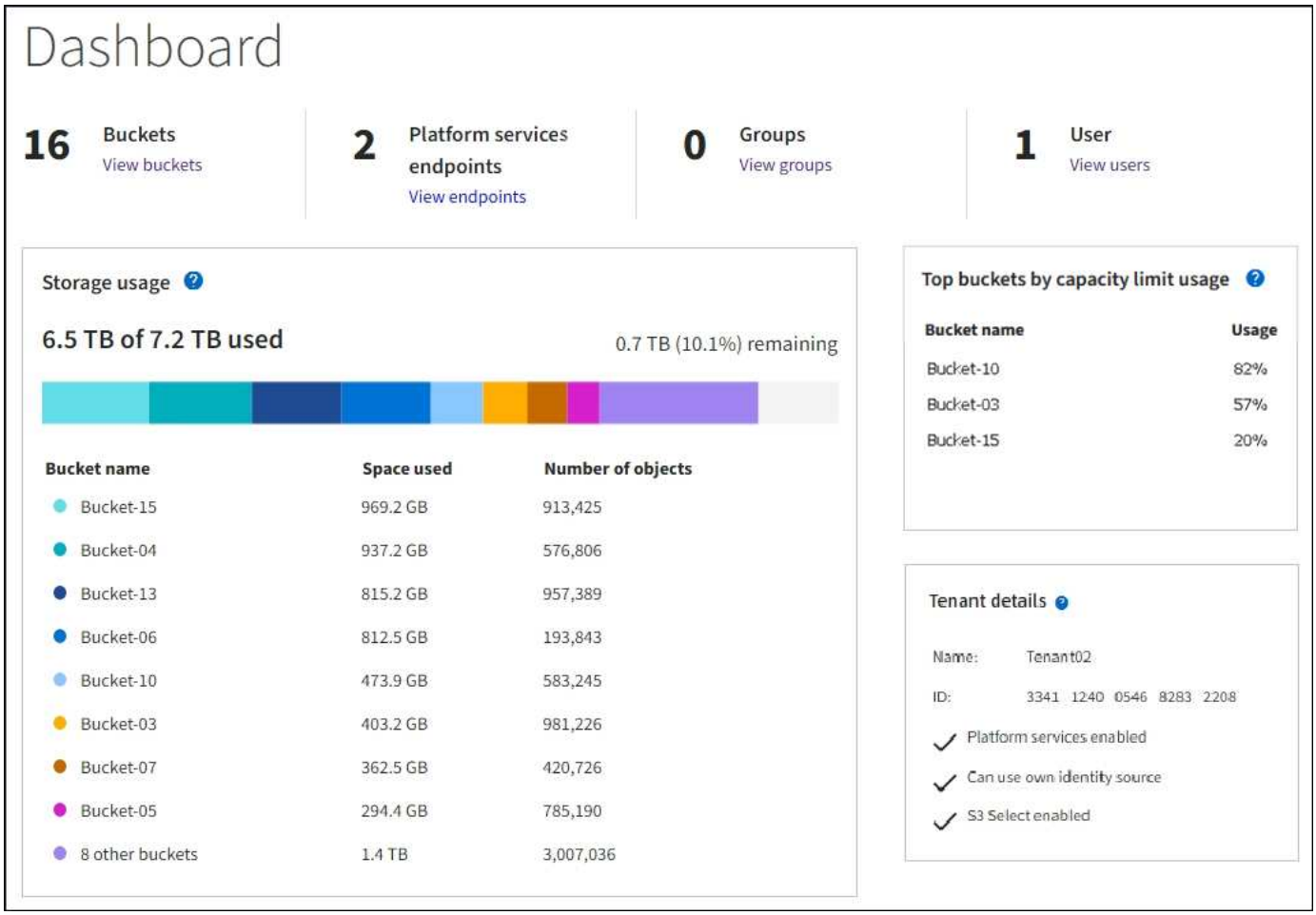
Se o SSO estiver ativado e você também estiver conectado ao Grid Manager, você deve sair do Grid Manager para sair do SSO.

Painel de controle do Tenant Manager no StorageGRID

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

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

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



Informações da conta do tenant

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

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

Uso de armazenamento e cotas

O painel de utilização de armazenamento contém as seguintes informações:

- A quantidade de dados de objetos para o locatário.

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

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

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

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

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

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

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

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

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

Alertas de uso de quota

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

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

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

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

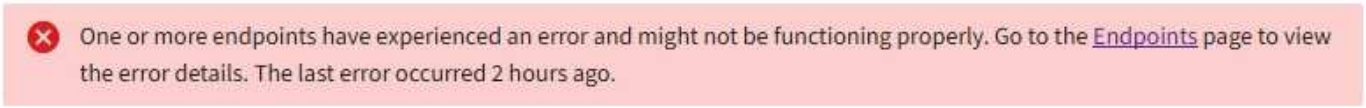
Uso do limite de capacidade

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

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

Erros de endpoint

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



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

API de gerenciamento de inquilinos

Saiba mais sobre a StorageGRID Tenant Management API

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

A Tenant Management API:

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

Para acessar a documentação Swagger da Tenant Management API:

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

Operações de API

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

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

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

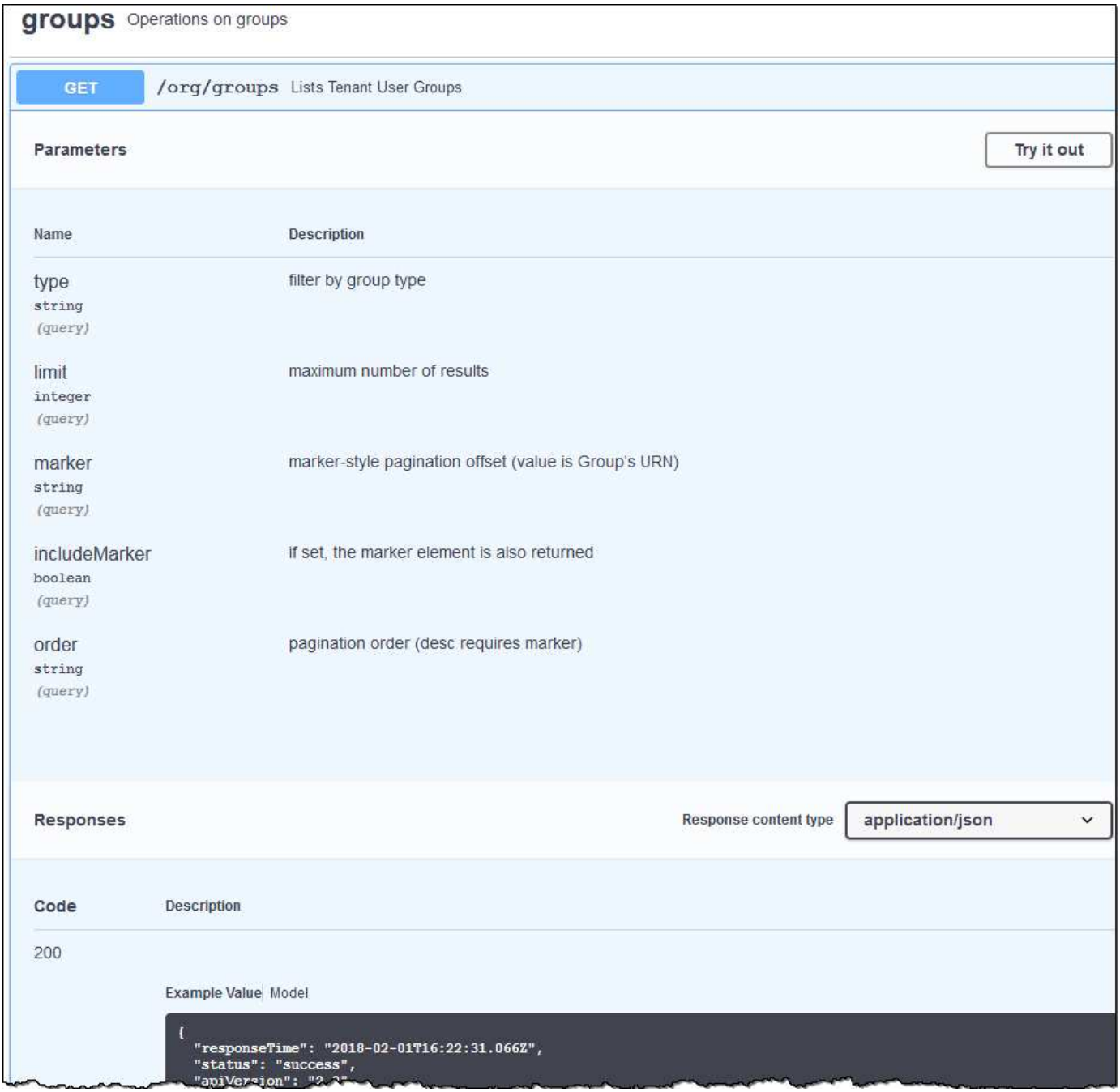
  Para obter informações sobre como melhorar a segurança de autenticação, consulte "Proteja contra falsificação de solicitação entre sites".

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

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

Detalhes da operação

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



Emitir solicitações de API

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

Passos

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

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

StorageGRID Versionamento da API de gerenciamento de locatários do StorageGRID

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

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

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

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

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

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

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

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

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

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

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

Determine quais versões da API são compatíveis na versão atual

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

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

Especifique uma versão da API para uma solicitação

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Use conexões de federação de grid

Clonar grupos de locatários e usuários em StorageGRID

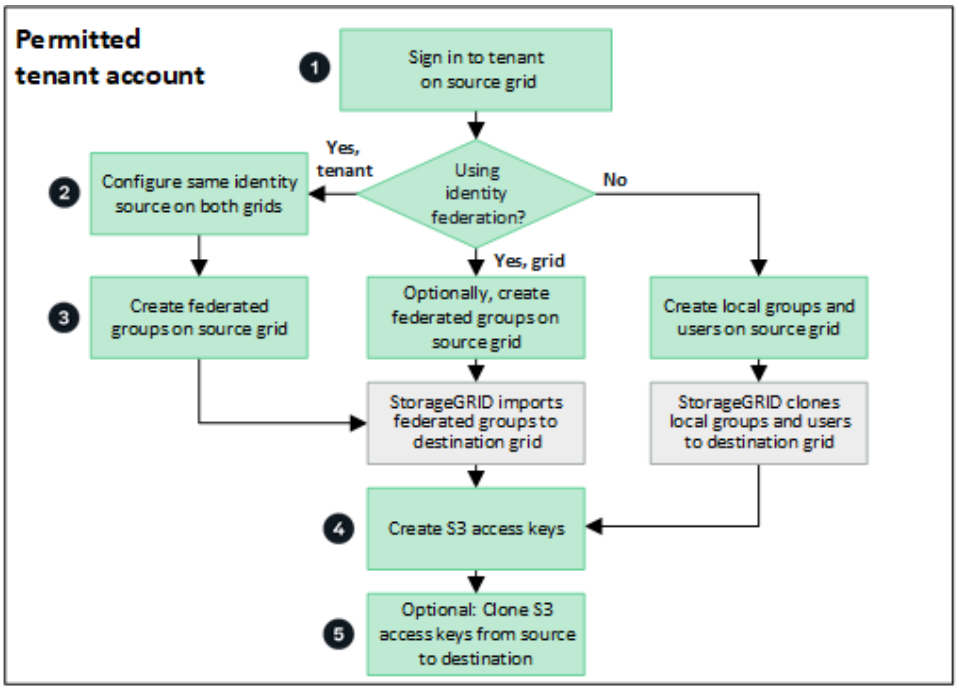
Se um locatário foi criado ou editado para usar uma conexão de federação de grid, esse locatário é replicado de um sistema StorageGRID (o locatário de origem) para outro sistema StorageGRID (o locatário de réplica). Após o locatário ser replicado, todos os grupos e usuários adicionados ao locatário de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

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

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

Fluxo de trabalho do locatário para clonagem de conta

Se a sua conta de locatário tiver a permissão **Usar conexão de federação de grid**, revise o diagrama de fluxo de trabalho para ver as etapas que você executará para clonar grupos, usuários e chaves de acesso S3.



Estas são as etapas principais do fluxo de trabalho:

Faça login no tenant

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

Opcionalmente, configure a federação de identidades

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

Criar grupos e usuários

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

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

4 Criar chaves de acesso S3

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

5 Opcionalmente, clone as chaves de acesso S3

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

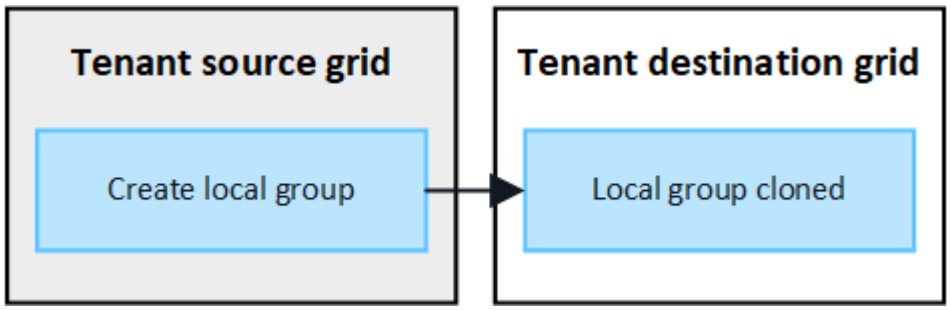
Como são clonados os grupos, usuários e chaves de acesso S3?

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

Os grupos locais criados na grade de origem são clonados

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

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

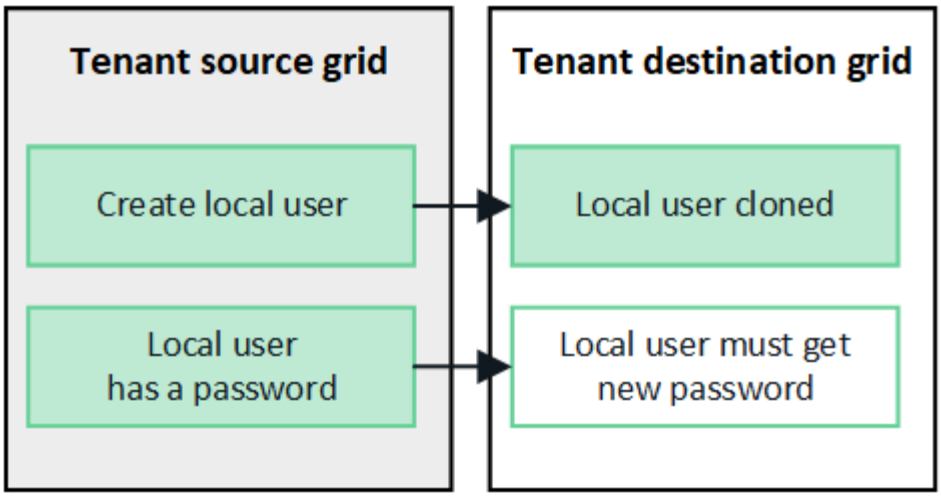


Os usuários que você selecionar ao criar um grupo local na grid de origem não serão incluídos quando o grupo for clonado para a grid de destino. Por esse motivo, não selecione usuários ao criar o grupo. Em vez disso, selecione o grupo ao criar os usuários.

Usuários locais criados na grade de origem são clonados

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

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

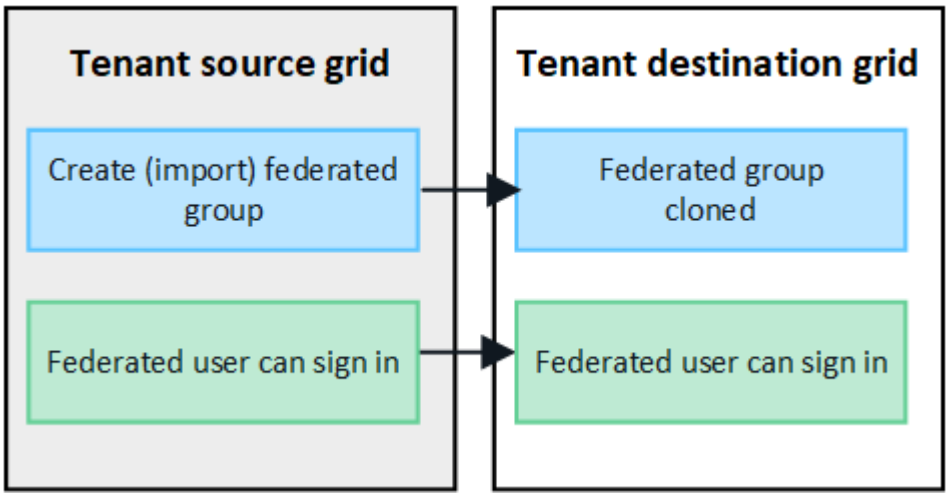


Grupos federados criados na grade de origem são clonados

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

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

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

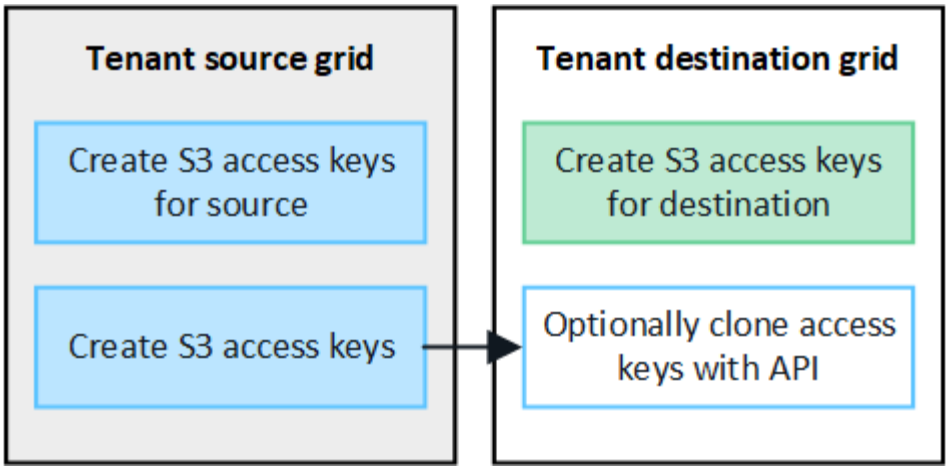


As chaves de acesso S3 podem ser clonadas manualmente

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

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

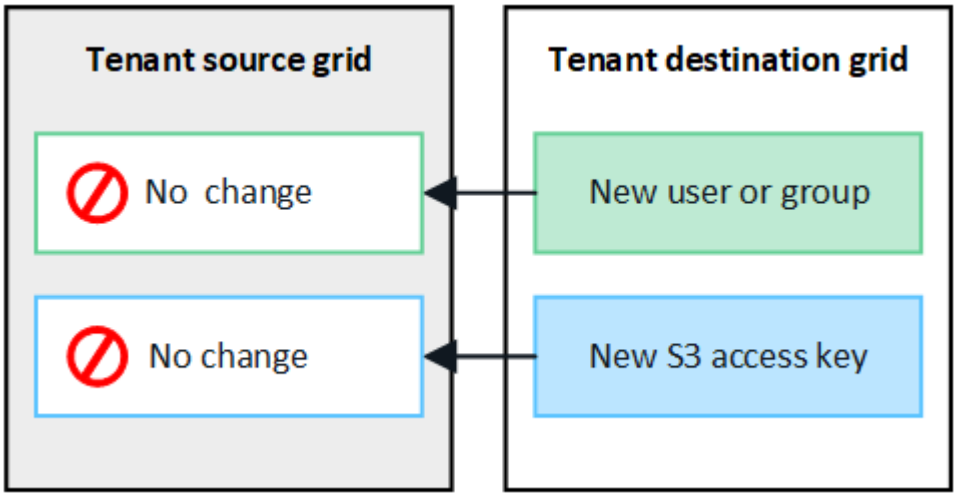
- Se você não precisar usar as mesmas chaves para cada grid, você pode "Crie suas próprias chaves de acesso" ou "Criar chaves de acesso de outro usuário" em cada grid.
- Se você precisar usar as mesmas chaves em ambas as grades, poderá criar chaves na grade de origem e, em seguida, usar a API do Gerenciador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



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

Grupos e usuários adicionados ao grid de destino não são clonados

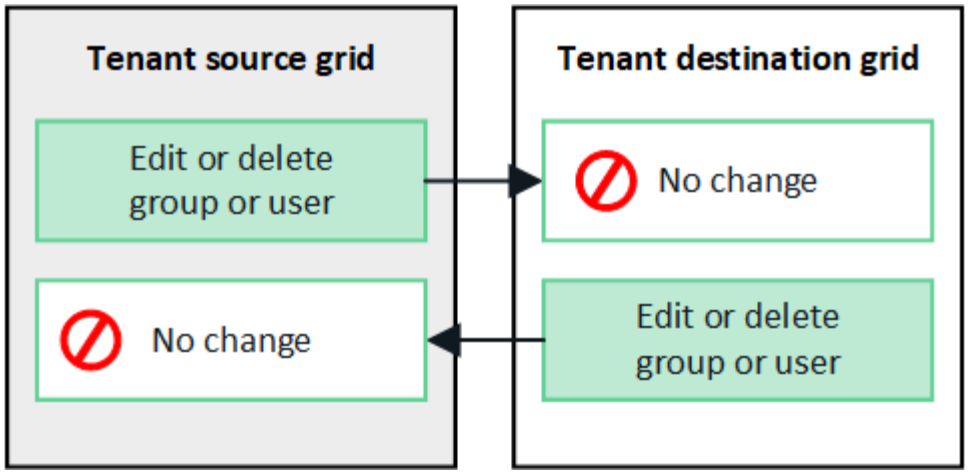
A clonagem ocorre somente da grade de origem do locatário para a grade de destino do locatário. Se você criar ou importar grupos e usuários na grade de destino do locatário, StorageGRID não clonará esses itens de volta para a grade de origem do locatário.



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

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

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



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

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

Antes de começar

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

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

Clone suas próprias chaves de acesso

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

Passos

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

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

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

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

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

Clonar as chaves de acesso de outro usuário

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

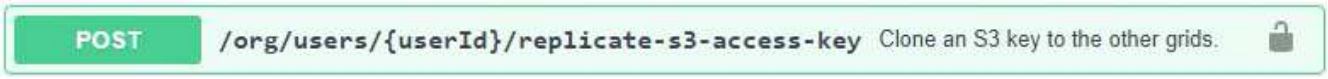
Passos

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

      `GET /org/users`

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

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



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

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

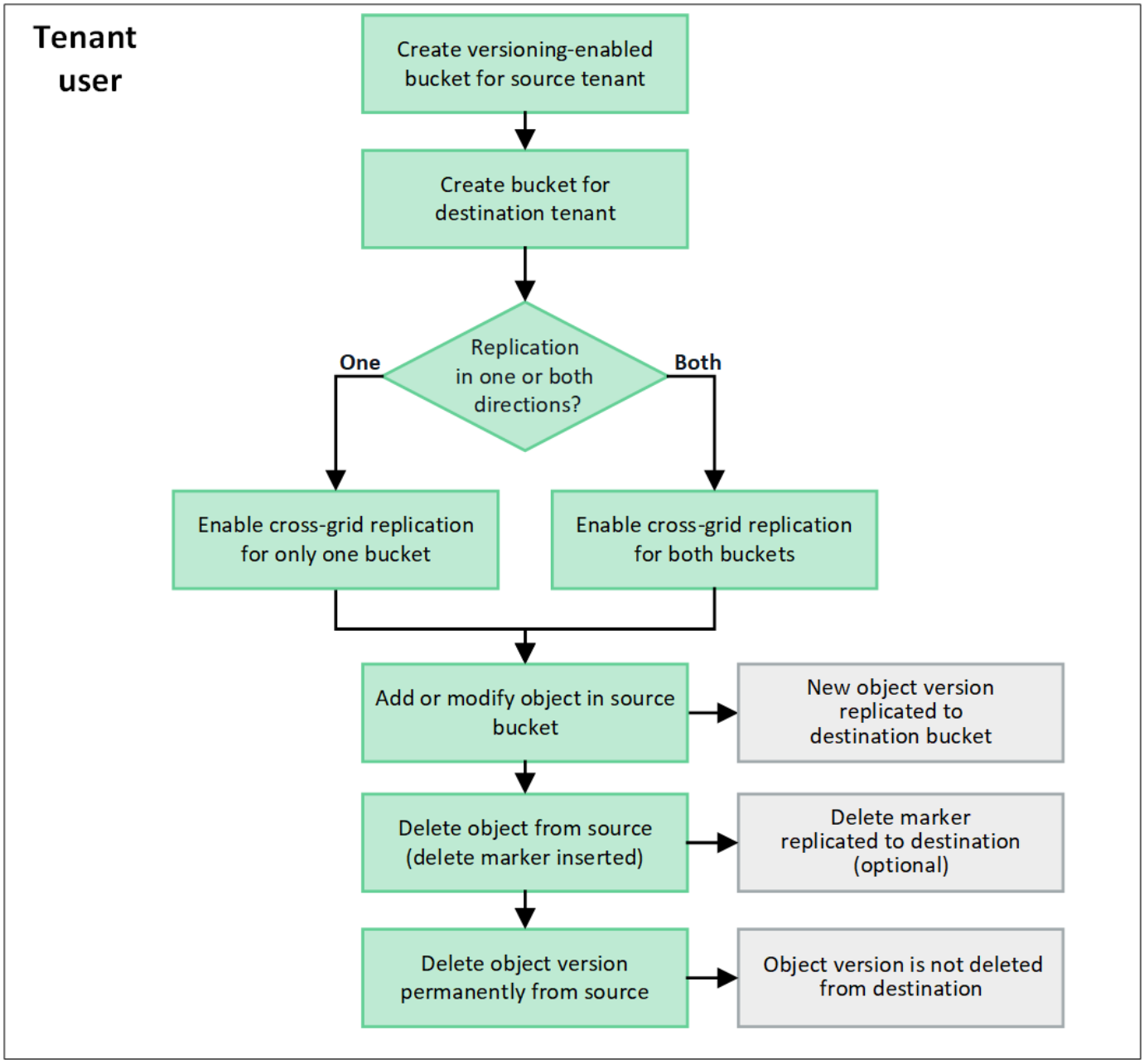
8. Se a chave expirar, substitua a entrada de exemplo para **expires** pela data e hora de expiração como uma string no formato de data e hora ISO 8601 (por exemplo, `2023-02-28T22:46:33-08:00`). Se a chave não expirar, insira **null** como o valor para a entrada **expires** (ou remova a linha **Expires**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

Gerencie a replicação entre grids no StorageGRID

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

Fluxo de trabalho para replicação entre grids

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



Configurar replicação entre grids

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

Antes de começar

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

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

Crie dois buckets

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

Passos

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

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

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

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

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

   Conforme necessário, cada bucket pode usar uma região diferente.

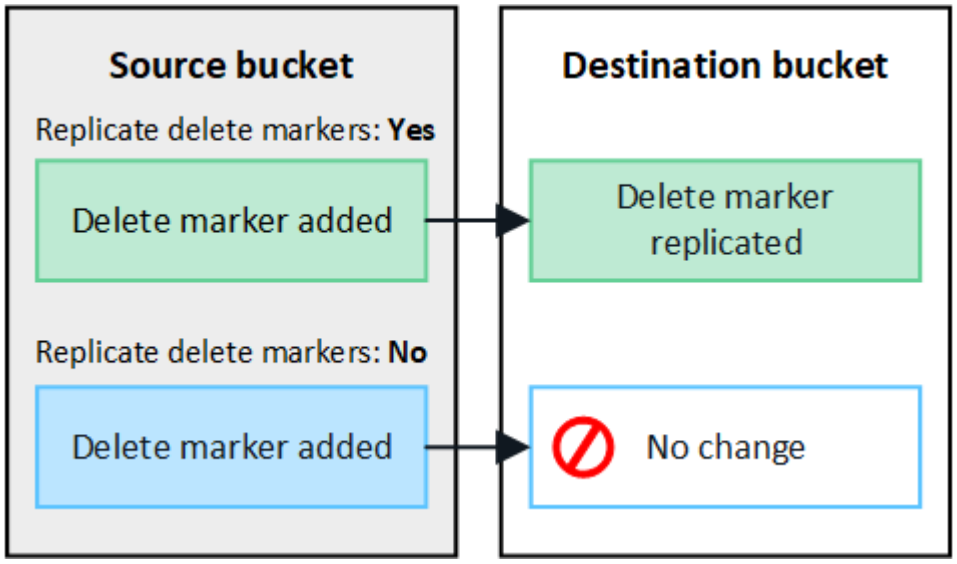
Habilitar replicação entre grids

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

Passos

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

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



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

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

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

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

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

Testar a replicação entre grids

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

Antes de começar

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

Passos

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

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

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

Desativar replicação entre grades

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

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

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

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

Antes de começar

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

Passos

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

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

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

Visualizar conexões de federação de grid no StorageGRID

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

Antes de começar

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

Passos

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

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

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

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

Limpar o último erro

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

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

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

Passos

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

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

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

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

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

Gerenciar grupos e usuários

Use a federação de identidades no StorageGRID

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

Configurar a federação de identidades para o Tenant Manager

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

Antes de começar

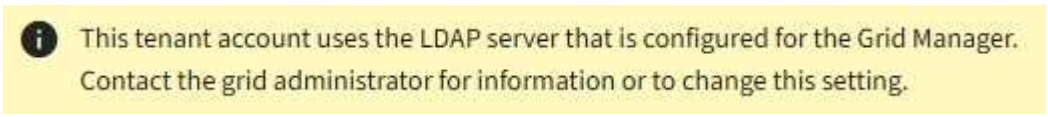
- Você está conectado ao Gerenciador de Inquilinos usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui o "Permissão de acesso root".
- Você está usando Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server como provedor de identidade.

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

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

Sobre esta tarefa

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

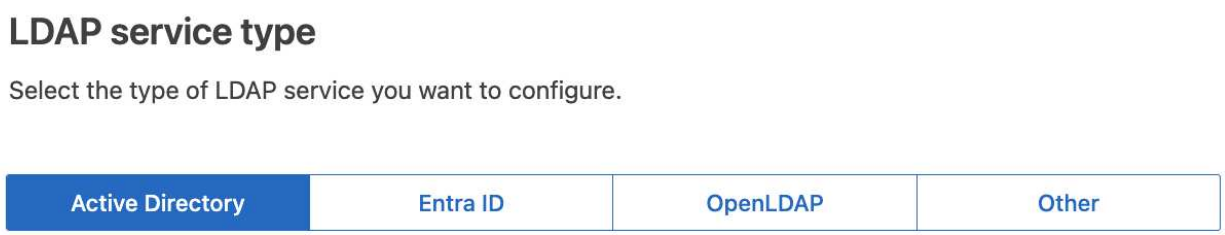


Insira a configuração

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

Passos

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Insira um destes padrões:

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

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

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

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

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

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

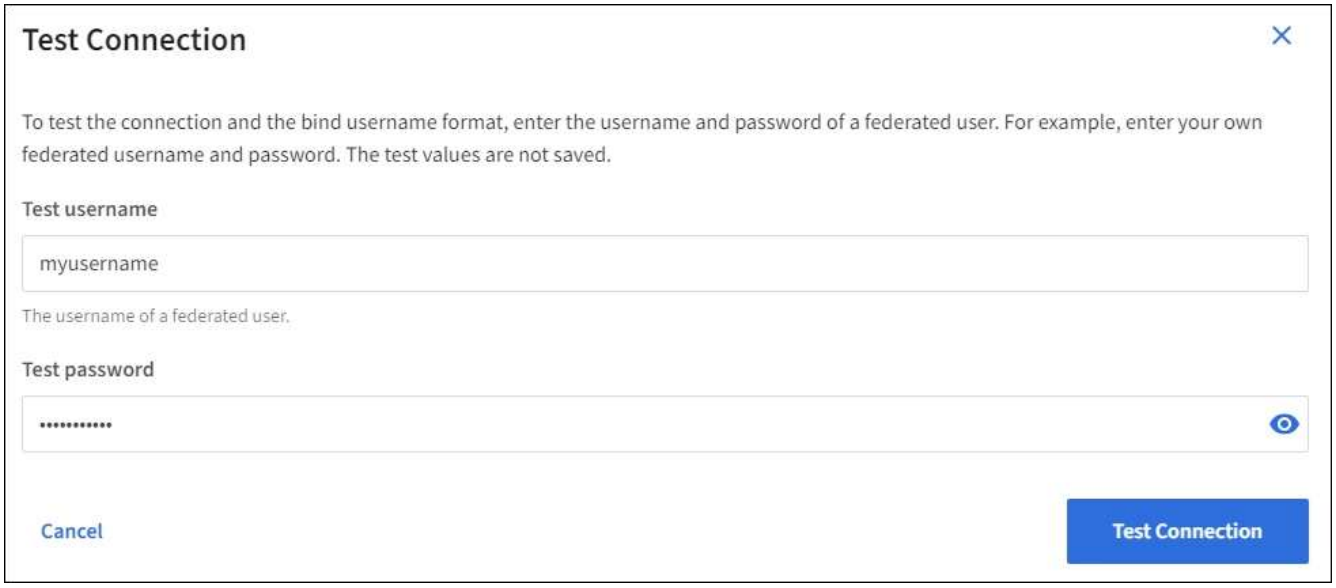
Teste a conexão e salve a configuração

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

Passos

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

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



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

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

Forçar sincronização com a fonte de identidade

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

Passos

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

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

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

Desativar federação de identidade

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

Sobre esta tarefa

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

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

Passos

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

Diretrizes para configurar o servidor OpenLDAP

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

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

Memberof e sobreposições refint

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

Indexação

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

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

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

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

Gerenciar grupos de locatários

Crie grupos para um locatário S3 no StorageGRID

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

Antes de começar

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

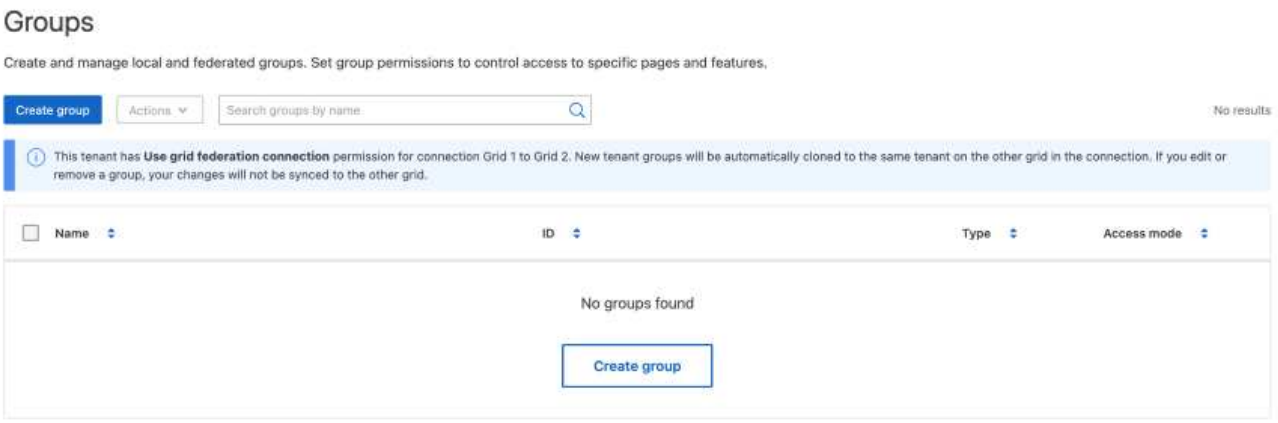
Acesse o assistente de criação de grupo

Como primeiro passo, acesse o assistente Create group.

Passos

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

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



3. Selecione **Criar grupo**.

Escolha um tipo de grupo

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

Passos

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

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

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

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

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

Gerenciar permissões de grupo

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

Passos

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

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

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

2. Selecione uma ou mais permissões para este grupo.

   Consulte "Permissões de gerenciamento de tenant".

3. Selecione **Continue**.

Definir política de grupo S3

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

Passos

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

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

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

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

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

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

Adicionar usuários (somente grupos locais)

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

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

Passos

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

   O grupo que você criou aparece na lista de grupos.

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

Permissões de gerenciamento de locatários do StorageGRID

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

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

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

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

relacionados.

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

Você pode atribuir as seguintes permissões a um grupo.

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

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

Gerenciar grupos de locatários do StorageGRID

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

Antes de começar

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

Ver ou editar grupo

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

Passos

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

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

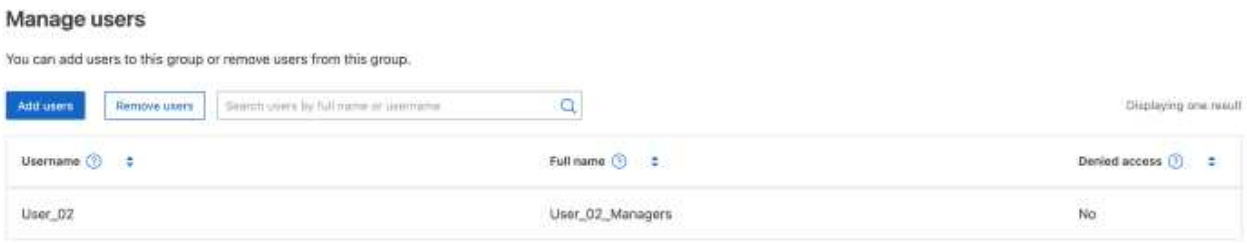
   - Uma mensagem no banner indica que, se você editar ou remover um grupo, suas alterações não serão sincronizadas com a outra grid.
   - Conforme necessário, uma mensagem em destaque indica se os grupos não foram clonados para o locatário na grade de destino. Você pode tentar novamente um clone de grupo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

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

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

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

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



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

      Uma mensagem de sucesso aparece no canto superior direito.

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

      Uma mensagem de sucesso aparece no canto superior direito.

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

Grupo duplicado

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

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

Passos

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

Tentar novamente clonagem de grupo

Para tentar novamente uma clonagem que falhou:

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

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

Excluir um ou mais grupos

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

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

Passos

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

   Uma caixa de diálogo de confirmação é exibida.

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

Configurar AssumeRole

Antes de começar

Você precisa ser um administrador para configurar AssumeRole.

Sobre esta tarefa

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

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

Passos

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

Exemplo de uma AssumeRole política de confiança S3

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

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

Gerenciar usuários de locatários do StorageGRID

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

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

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

Antes de começar

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

Criar um usuário local

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

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

Acesse o assistente de criação de usuário

Passos

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

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

2. Selecione **Criar usuário**.

Insira as credenciais

Passos

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

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

2. Selecione **Continue**.

Atribuir a grupos

Passos

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

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

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

2. Selecione **Criar usuário**.

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

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

Visualizar ou editar usuário local

Passos

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

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

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

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

      Você não pode alterar o nome de usuário.

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

Importar usuários federados

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

Passos

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

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

4. Selecione **Import**.

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

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

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

Usuário local duplicado

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

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

Passos

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

Tentar novamente clonar usuário

Para tentar novamente uma clonagem que falhou:

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

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

Excluir um ou mais usuários locais

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

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

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

Passos

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

   Uma caixa de diálogo de confirmação é exibida.

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

Gerenciar chaves de acesso S3

Gerencie as chaves de acesso S3 no StorageGRID

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

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

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

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

Crie suas próprias chaves de acesso S3 no StorageGRID

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

Antes de começar

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

permissão de acesso root".

Sobre esta tarefa

Você pode criar uma ou mais chaves de acesso S3 que permitem criar e gerenciar buckets para sua conta de tenant. Após criar uma nova chave de acesso, atualize o aplicativo com seu novo ID da chave de acesso e chave de acesso secreta. Por segurança, não crie mais chaves do que você precisa e exclua as chaves que não estiver usando. Se você tiver apenas uma chave e ela estiver prestes a expirar, crie uma nova antes que a antiga expire e depois exclua a antiga.

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

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

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

Passos

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

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

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

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

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

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

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

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

6. Selecione **Concluir**.

A nova chave está listada na página My access keys.

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

Visualize suas chaves de acesso S3 no StorageGRID

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

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

Antes de começar

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

Passos

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

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

   As chaves expiradas são removidas automaticamente.

Exclua suas próprias chaves de acesso S3 no StorageGRID

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

Antes de começar

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

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

Passos

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

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

Crie chaves de acesso S3 de outro usuário no StorageGRID

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

Antes de começar

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

Sobre esta tarefa

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

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

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

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

Passos

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

   A página de detalhes do usuário aparece.

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

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

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

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

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

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

7. Selecione **Concluir**.

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

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

Visualizar as chaves de acesso S3 de outro usuário no StorageGRID

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

Antes de começar

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

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

Passos

1. Selecione **Gerenciamento de Acesso** > **Usuários**.
2. Na página Usuários, selecione o usuário cujas chaves de acesso ao S3 você deseja visualizar.
3. Na página Detalhes do usuário, selecione **Chaves de acesso**.
4. Classifique as chaves por **Tempo de expiração** ou **ID da chave de acesso**.
5. Conforme necessário, crie novas chaves e exclua manualmente as chaves que não estiverem mais em uso.

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

   As chaves expiradas são removidas automaticamente.

Informações relacionadas

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

Excluir as chaves de acesso S3 de outro usuário no StorageGRID

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

Antes de começar

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

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

Passos

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

5. Na caixa de diálogo de confirmação, selecione **Delete key**.

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

Gerenciar buckets do S3

Crie um bucket S3 do StorageGRID

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

Antes de começar

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

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

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

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

Acesse o assistente

Passos

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

Insira os detalhes

Passos

1. Insira os detalhes do bucket.

Campo	Descrição
Nome do bucket	Um nome para o bucket que esteja em conformidade com estas regras: • Deve ser único em cada sistema StorageGRID (e não apenas único dentro da conta do locatário). • Deve ser compatível com DNS. • Deve conter no mínimo 3 e no máximo 63 caracteres. • Cada etiqueta deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens. • Não devem constar pontos em solicitações no estilo de hospedagem virtual. Pontos podem causar problemas na verificação do certificado curinga do servidor. Para obter mais informações, consulte o "Documentação da Amazon Web Services (AWS) sobre regras de nomenclatura de buckets". **Observação**: Não é possível alterar o nome do bucket depois de criar o bucket.
Região	A região do bucket. O administrador do StorageGRID gerencia as regiões disponíveis. A região de um bucket pode afetar a política de proteção de dados aplicada aos objetos. Por padrão, todos os buckets são criados na região `us-east-1`. Se a região padrão estiver configurada para uma região diferente de `us-east-1`, essa outra região será selecionada inicialmente na lista suspensa. **Observação**: Não é possível alterar a região depois de criar o bucket.

2. Selecione **Continue**.

Gerenciar configurações

Passos

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

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

   Você deve habilitar o versionamento de objetos se:

   ◦ O bucket será usado para replicação entre grids.

   ◦ Você deseja criar um "bucket de branch" a partir deste bucket.

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

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

período fixo ou indefinidamente.

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

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

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

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

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

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

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

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

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

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

do grid para aumentar ou diminuir o período de retenção máximo.

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

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

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

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

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

6. Selecione **Create bucket**.

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

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

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

Veja os detalhes do bucket S3 no StorageGRID

Você pode visualizar os buckets na sua conta de locatário.

Antes de começar

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

Passos

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

   A página Buckets é exibida.

2. Analise a tabela de resumo para cada bucket.

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

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

   Nome

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

Recursos ativados

Lista de funcionalidades habilitadas para o bucket.

Bloqueio de objeto S3

Indica se o S3 Object Lock está ativado para o bucket.

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

Região

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

Contagem de objetos

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

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

Espaço utilizado

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

Esse valor pode levar até 10 minutos para ser atualizado.

Uso

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

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

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

Capacidade

Se definido, o limite de capacidade do bucket.

Data de criação

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

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

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

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

d. Visualize ou altere as configurações do bucket em cada uma das abas, conforme necessário.

- **Console S3**: Visualize os objetos do bucket. Para obter mais informações, consulte "Use o console S3".
- **Opções do bucket**: visualize ou altere as configurações de opções. Algumas configurações, como S3 Object Lock, não podem ser alteradas após a criação do bucket.
  - "Gerencie a consistência do bucket"
  - "Atualizações do último tempo de acesso"
  - "Limite de capacidade"
  - "Limite de contagem de objetos"
  - "Versionamento de objetos"
  - "Bloqueio de objeto S3"
  - "Retenção padrão do bucket"
  - "Gerencie a replicação entre grades" (se permitido ao inquilino)
- **Serviços de plataforma**: "Gerenciar serviços de plataforma" (se permitido para o locatário)
- **Acesso ao bucket**: visualize ou altere as configurações de opções. Você precisa ter permissões de acesso específicas.
  - Configure "CORS para buckets e objetos" para que o bucket e os objetos nele contidos fiquem acessíveis a aplicativos web em outros domínios.
  - "Controlar o acesso do usuário" para um bucket S3 e os objetos contidos nesse bucket.
- **Ramos**: Veja a lista de buckets de ramos para o bucket. "Criar um novo bucket de branch ou gerenciar buckets de branch".

Saiba mais sobre os buckets de ramificação do StorageGRID

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

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

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

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

Observe as seguintes características dos buckets de branch:

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

Exemplos de utilização de buckets de ramificação

- Você pode usar um bucket de ramificação para remover objetos corrompidos criando um bucket de ramificação a partir de um ponto no tempo anterior à ocorrência da corrupção e, em seguida, direcionando os aplicativos para o bucket de ramificação em vez do bucket base que contém objetos corrompidos.
- Você está salvando dados em um bucket versionado. Ocorreu uma vulnerabilidade acidental que causou a ingestão de muitos objetos indesejados após o tempo *T*. Você pode criar um bucket de ramificação para o valor de tempo Antes, *T*, e redirecionar as operações do cliente para esse bucket de ramificação. Assim, somente os objetos ingeridos antes do tempo Antes, *T*, são expostos aos clientes.

Operações em objetos em buckets de branch

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

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

Operação	Alvo	Resultado	Visibilidade do objeto no bucket base	Visibilidade do objeto no bucket de branch
Excluir com ID de versão	Bucket de branch	A versão específica do objeto é excluída apenas para bucket de ramificação	HEAD/GET retorna uma versão específica do objeto (o objeto do bucket base não é afetado)	HEAD/GET retorna "Versão do objeto não existe"

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

Gerenciar buckets de ramificação do StorageGRID

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

Antes de começar

- Você fez login no Tenant Manager usando um "navegador web compatível".
- Você pertence a um grupo de usuários que possui acesso Root ou "Gerenciar todas as permissões de buckets". Essas permissões substituem as configurações de permissões nas políticas de grupo ou bucket.
- O bucket base a partir do qual você deseja criar uma ramificação tem "versionamento ativado".
- Você é o proprietário do bucket base.

Sobre esta tarefa

Observe as seguintes informações para os buckets de ramificação:

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

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

Criar bucket de ramificação

Passos

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

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

Insira os detalhes

Passos

1. Insira os detalhes do bucket da filial.

Campo	Descrição
Nome do bucket da filial	Um nome para o bucket da branch que esteja em conformidade com estas regras: • Deve ser único em cada sistema StorageGRID (e não apenas único dentro da conta do locatário). • Deve ser compatível com DNS. • Deve conter no mínimo 3 e no máximo 63 caracteres. • Cada etiqueta deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens. • Não devem constar pontos em solicitações no estilo de hospedagem virtual. Pontos podem causar problemas na verificação do certificado curinga do servidor. Para obter mais informações, consulte o "Documentação da Amazon Web Services (AWS) sobre regras de nomenclatura de buckets". **Observação**: Você não pode alterar o nome depois de criar o bucket da branch.
Região (não pode ser modificada para buckets de ramificação)	A região do bucket do branch. A região do bucket de ramificação deve corresponder à região do bucket base, portanto, esse campo está desativado para buckets de ramificação.
Antes do tempo	O horário limite para que as versões de objetos criadas no bucket base sejam acessíveis a partir do bucket de ramificação. O bucket de ramificação fornece acesso às versões de objetos criadas antes do horário Before. O termo "antes" deve se referir a uma data e hora que já passaram. Não pode ser uma data futura.
Tipo de bucket de branch	• **Leitura e gravação**: Você pode adicionar ou excluir objetos ou versões de objetos no bucket de ramificação. • **Somente leitura**: Você não pode modificar objetos no bucket de ramificação. **Nota**: Você pode definir o tipo de bucket de branch como somente leitura apenas se o bucket de branch estiver vazio. Se o tipo de um bucket de branch existente estiver definido como leitura e gravação e você não tiver gravado nele, você pode alterar o tipo para somente leitura.

2. Selecione **Continue**.

Gerenciar configurações de objetos (opcional)

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

Passos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Selecione **Create bucket**.

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

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

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

Aplicar uma tag de política ILM a um bucket do StorageGRID

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

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

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

Antes de começar

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

Passos

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

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

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

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

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

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

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

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

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

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

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

Gerenciar política de bucket do StorageGRID

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

nesse bucket.

Antes de começar

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

Passos

1. Selecione **Buckets** e, em seguida, selecione o bucket que você deseja gerenciar.
2. Na página de detalhes do bucket, selecione **Acesso ao bucket** > **Política do bucket**.
3. Faça um dos seguintes procedimentos:
   - Defina uma política de bucket selecionando a caixa de seleção **Ativar política**. Em seguida, insira uma string válida no formato JSON.

     Cada política de bucket tem um limite de tamanho de 20.480 bytes.
   - Modifique uma política existente editando a string.
   - Desative uma política desmarcando a opção **Ativar política**.

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

Gerenciar a consistência dos buckets do StorageGRID

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

Antes de começar

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

Diretrizes de consistência de bucket

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

Alterar a consistência do bucket

Se a consistência **Read-after-new-write** não atender aos requisitos do aplicativo cliente, você pode alterá-la

definindo a consistência do bucket ou usando o `Consistency-Control` cabeçalho. O `Consistency-Control` cabeçalho substitui a consistência do bucket.

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

Passos

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

   A página de detalhes do bucket é exibida.

3. Na aba **Opções do bucket**, selecione o ** acordeão.
4. Selecione uma consistência para as operações realizadas nos objetos deste bucket.
   - **Todos**: Oferece o mais alto nível de consistência. Todos os nós recebem os dados imediatamente ou a solicitação falhará.
   - **Strong-global**: Garante consistência de leitura após gravação para todas as solicitações do cliente em todos os sites.
   - **Site forte**: Garante a consistência de leitura após gravação para todas as solicitações do cliente dentro de um site.
   - **Leitura após nova gravação** (padrão): Oferece consistência de leitura após gravação para novos objetos e consistência eventual para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
   - **Disponível**: Oferece consistência eventual tanto para novos objetos quanto para atualizações de objetos. Para buckets do S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que são lidos raramente ou para operações HEAD ou GET em chaves que não existem). Não é compatível com buckets do S3 FabricPool.
5. Selecione **Save changes**.

O que acontece quando você altera as configurações do bucket

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

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

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

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

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

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

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

Ativar ou desativar atualizações de tempo de acesso no StorageGRID

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

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

Antes de começar

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

Sobre esta tarefa

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

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

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

Por padrão, as atualizações do tempo de acesso estão desativadas. Se o seu StorageGRID incluir uma regra de gerenciamento do ciclo de vida das informações (ILM) que use a opção **Último tempo de acesso** e você

quiser que essa opção se aplique aos objetos neste bucket, será necessário ativar as atualizações do tempo de acesso para os buckets S3 especificados nessa regra.

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

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

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

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

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

Solicitação para concluir um upload multipart	Sim, para o objeto montado	Sim, para o objeto montado	Sim, para o objeto montado	Sim, para o objeto montado

Passos

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

   A página de detalhes do bucket é exibida.

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

Alterar o versionamento de objeto para um bucket S3 no StorageGRID

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

Antes de começar

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

Sobre esta tarefa

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

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

Para obter mais informações, consulte o seguinte:

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

Passos

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

A página de detalhes do bucket é exibida.

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

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

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

5. Selecione **Save changes**.

Use S3 Object Lock para reter objetos no StorageGRID

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

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

O que é o bloqueio de objeto S3?

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

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

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

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

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

Na prática, todos os objetos recém-ingeridos têm configurações de retenção quando a retenção padrão está

configurada. Os objetos existentes sem configurações de retenção permanecem inalterados.

Modos de retenção

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

- No modo de conformidade:
  - O objeto não pode ser excluído até que sua retain-until-date seja atingida.
  - A data de retenção do objeto pode ser aumentada, mas não pode ser diminuída.
  - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- Em modo de governança:
  - Usuários com permissão especial podem usar um cabeçalho de bypass em solicitações para modificar determinadas configurações de retenção.
  - Esses usuários podem excluir uma versão de objeto antes que a data de retenção seja atingida.
  - Esses usuários podem aumentar, diminuir ou remover a retain-until-date de um objeto.

Configurações de retenção para versões de objetos

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

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

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

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

Configuração padrão de retenção para buckets

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

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

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

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

Tarefas de bloqueio de objetos S3

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

Administrador de grid

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

Usuário locatário

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

Requisitos para buckets com S3 Object Lock ativado

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

Requisitos para objetos em buckets com S3 Object Lock ativado

- Para proteger uma versão de objeto, você pode especificar configurações de retenção padrão para o bucket ou pode especificar configurações de retenção para cada versão de objeto. As configurações de retenção em nível de objeto podem ser especificadas usando o aplicativo cliente S3 ou a API REST.
- As configurações de retenção se aplicam a versões individuais de objetos. Uma versão de objeto pode ter tanto uma configuração de data de retenção quanto de guarda legal, uma delas, mas não a outra, ou nenhuma das duas. Especificar uma data de retenção ou uma configuração de guarda legal para um objeto protege apenas a versão especificada na solicitação. Você pode criar novas versões do objeto, enquanto a versão anterior do objeto permanece bloqueada.

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

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

1. **Ingestão de objeto**

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

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

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

2. **Retenção e exclusão de objetos**

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

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

Ainda posso gerenciar buckets legados compatíveis?

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

Atualizar retenção padrão do S3 Object Lock no StorageGRID

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

Antes de começar

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

Passos

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

   A página de detalhes do bucket é exibida.

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

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

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

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

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

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

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

7. Selecione **Save changes**.

Configure CORS para buckets S3 no StorageGRID

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

Antes de começar

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

Sobre esta tarefa

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

Habilite o CORS para um bucket

Passos

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

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

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

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

   A página de detalhes do bucket é exibida.

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

Modificar configuração CORS

Passos

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

Desativar a configuração CORS

Passos

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

Informações relacionadas

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

Excluir objetos de um bucket S3 do StorageGRID

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

Considerações e requisitos

Antes de executar esses passos, observe o seguinte:

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

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

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

Antes de começar

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

Passos

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

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

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

Menu de ações

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

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

Página de detalhes

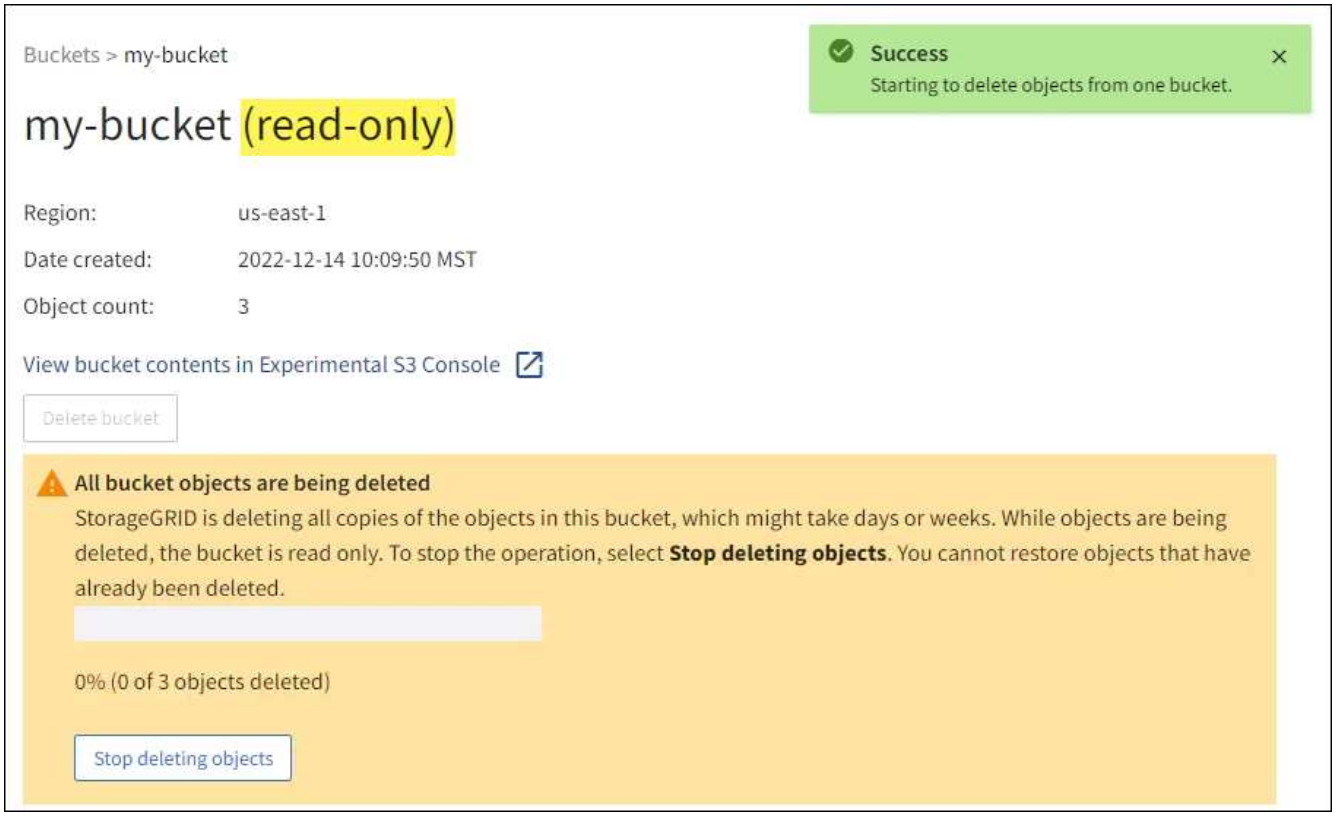
a. Selecione o nome do bucket para exibir seus detalhes.

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

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

Após alguns minutos:

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



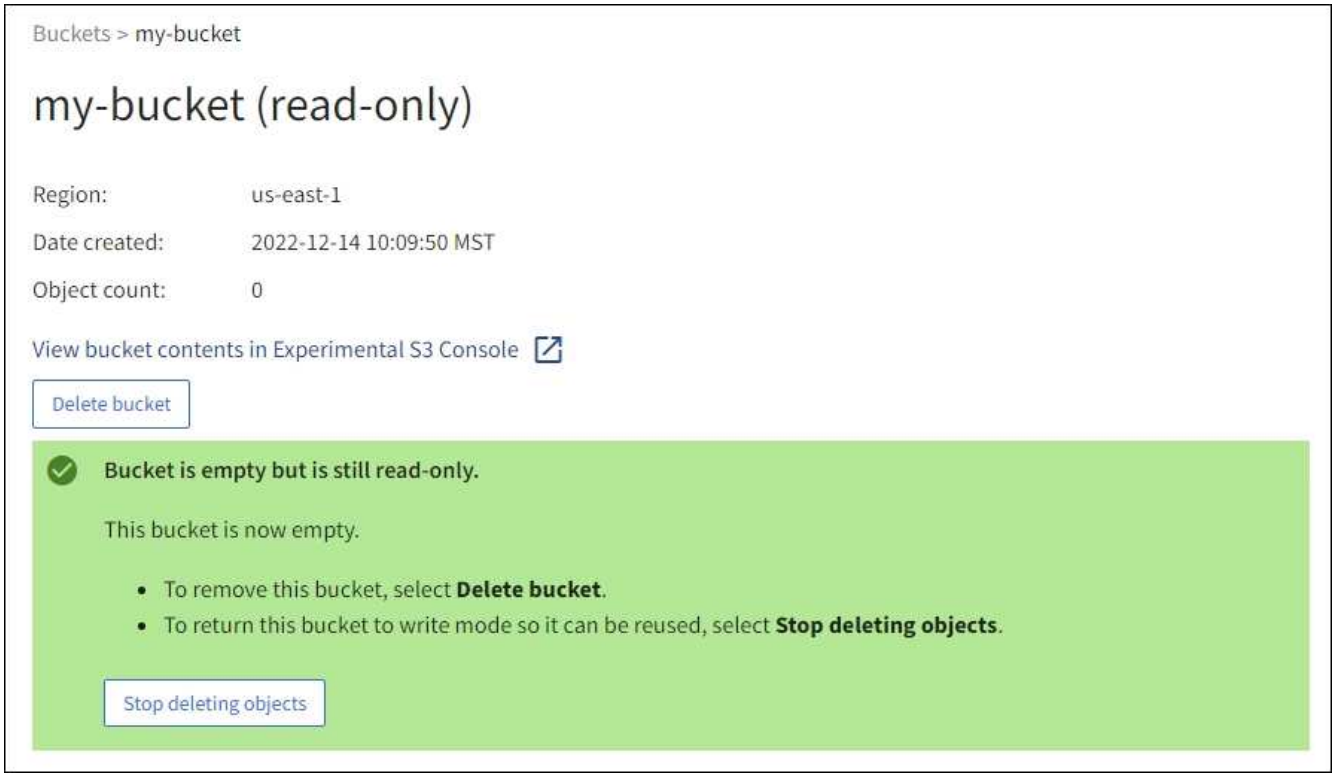
5. Se necessário, durante a execução da operação, selecione **Parar exclusão de objetos** para interromper o processo. Em seguida, opcionalmente, selecione **Excluir objetos no bucket** para retomar o processo.

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

pode acessar ou restaurar nenhum objeto que tenha sido excluído.

6. Aguarde a conclusão da operação.

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



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

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

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

Excluir um bucket S3 do StorageGRID

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

Antes de começar

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

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

Sobre esta tarefa

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

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

Passos

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

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

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

   Menu de ações

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

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

   Página de detalhes

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

   b. Selecione **Excluir bucket**.

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

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

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

Use o S3 Console no StorageGRID

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

O S3 Console permite que você:

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

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

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

Antes de começar

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

Passos

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

Informações adicionais

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

Gerenciar serviços da plataforma S3

Serviços da plataforma S3

Saiba mais sobre os serviços de plataforma para StorageGRID

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

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

Visão geral dos serviços da plataforma

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

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

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

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

Como os serviços da plataforma são configurados

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

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

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

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

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

plataforma StorageGRID:

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

Considerações sobre o uso de serviços de plataforma

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

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

Considerações sobre o uso do serviço de replicação CloudMirror

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

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

Saiba mais sobre o serviço de replicação StorageGRID CloudMirror

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

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

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

CloudMirror e ILM

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

CloudMirror e replicação entre grades

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

CloudMirror e buckets S3

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

Buckets existentes

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

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

Vários buckets de destino

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

Buckets versionados ou não versionados

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

Exclusão, loops de replicação e eventos

Comportamento de exclusão

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

bucket de destino nem exclui o objeto de destino.

Proteção contra loops de replicação

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

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

Eventos no bucket de destino

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

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

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

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

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

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

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

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

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

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

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

Saiba mais sobre o serviço de integração de pesquisa do StorageGRID

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

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

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

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

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

Integração de pesquisa e buckets S3

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

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

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

Notificações de pesquisa

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

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

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

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

Serviço de integração de pesquisa e Elasticsearch

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

Gerenciar endpoints de serviços de plataforma

Configure os endpoints dos serviços da plataforma no StorageGRID

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

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

O que é um endpoint de serviços de plataforma?

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

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

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

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

Pontos finais para replicação CloudMirror

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

Pontos de extremidade para notificações

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

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

Pontos de extremidade para o serviço de integração de pesquisa

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

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

Informações relacionadas

"Administrar StorageGRID"

Especifique um URN para um endpoint de serviços de plataforma StorageGRID

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

único.

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

Elementos URN

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

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

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

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

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

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

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

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

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

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

URNs para serviços hospedados na AWS e no GCP

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

- CloudMirror replicação:

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

- Notificações:

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

- Integração de pesquisa:

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

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

URNs para serviços hospedados localmente

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

- CloudMirror replicação:

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

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

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

- Notificações:

  Especifique um endpoint do Amazon Simple Notification Service:

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

  Especifique um endpoint do Kafka:

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

  Especifique um endpoint de webhook:

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

- Integração de pesquisa:

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

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

Crie um endpoint de serviços da plataforma StorageGRID

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

Antes de começar

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

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

- Nome único de recurso (URN)

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

- Credenciais de autenticação (se necessário):

  Pontos de extremidade de integração de pesquisa

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

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

  CloudMirror endpoints de replicação

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

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

  Pontos de extremidade do Amazon SNS

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

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

  Pontos de extremidade do Kafka

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

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

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

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

Passos

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

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

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

   Utilize um dos seguintes formatos:

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

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

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

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

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

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

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

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

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

   > Se o endpoint for usado para o serviço de replicação CloudMirror, não inclua o nome do bucket no URI. Inclua o nome do bucket no campo **URN**.

5. Insira o Nome Único do Recurso (URN) para o endpoint.

   > Não é possível alterar o URN de um endpoint depois que ele foi criado.

6. Selecione **Continue**.
7. Selecione um valor para **Tipo de autenticação**.

   > Se você deseja autenticação para endpoints de webhook, configure Mutual Transport Layer Security (mTLS) em Etapa 9.

Pontos de extremidade de integração de pesquisa

Insira ou carregue as credenciais para um endpoint de integração de pesquisa.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints com segurança desativada.	Sem autenticação.
Chave de acesso	Utiliza credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta
HTTP básico	Utiliza um nome de usuário e senha para autenticar conexões com o destino.	• Nome de usuário • Senha

CloudMirror endpoints de replicação

Insira ou carregue as credenciais para um ponto de extremidade de replicação CloudMirror.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints com segurança desativada.	Sem autenticação.
Chave de acesso	Utiliza credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta
CAP (Portal de Acesso C2S)	Utiliza certificados e chaves para autenticar conexões com o destino.	• URL de credenciais temporárias • Certificado CA do servidor (upload de arquivo PEM) • Certificado do cliente (upload de arquivo PEM) • Chave privada do cliente (upload de arquivo PEM, formato criptografado OpenSSL ou formato de chave privada não criptografada) • Senha da chave privada do cliente (opcional)

Pontos de extremidade do Amazon SNS

Insira ou carregue as credenciais para um endpoint do Amazon SNS.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints com segurança desativada.	Sem autenticação.
Chave de acesso	Utiliza credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta

Pontos de extremidade do Kafka

Insira ou carregue as credenciais para um endpoint do Kafka.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints com segurança desativada.	Sem autenticação.
SASL/PLAIN	Utiliza um nome de usuário e senha em texto simples para autenticar conexões com o destino.	• Nome de usuário • Senha
SASL/SCRAM-SHA-256	Utiliza um nome de usuário e senha usando um protocolo de desafio-resposta e hash SHA-256 para autenticar conexões com o destino.	• Nome de usuário • Senha
SASL/SCRAM-SHA-512	Utiliza um nome de usuário e senha usando um protocolo de desafio-resposta e hash SHA-512 para autenticar conexões com o destino.	• Nome de usuário • Senha

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

8. Selecione **Continue**.
9. Selecione um botão de opção para **Verificar certificados** para escolher como a conexão TLS com o endpoint é verificada.

A maioria dos endpoints

Verifique a conexão TLS para integração de pesquisa, CloudMirror replication, Amazon SNS ou endpoints Kafka.

Tipo de verificação de certificado	Descrição
TLS	Valida o certificado do servidor para conexões TLS com o recurso de endpoint.
Desabilitado	A verificação de certificado está desativada. Esta opção não é segura.
Use um certificado CA personalizado	O certificado CA personalizado é usado para verificar a identidade do servidor ao conectar-se ao endpoint.
Use o certificado CA do sistema operacional	Utilize o certificado padrão da Autoridade de Certificação (CA) do Grid instalado no sistema operacional para proteger as conexões.

Apenas endpoints de webhook

Verifique a conexão TLS para os endpoints do webhook.

Tipo de verificação de certificado	Descrição
TLS	Valida o certificado do servidor para conexões TLS com o recurso de endpoint.
mTLS	Valida os certificados do cliente e do servidor para conexões TLS mútuas com o recurso de endpoint.
Desabilitado	A verificação de certificado está desativada. Esta opção não é segura.
Use um certificado CA personalizado	O certificado CA personalizado é usado para verificar a identidade do servidor ao conectar-se ao endpoint.

Ao selecionar **mTLS**, essas opções ficam disponíveis.

Tipo de verificação de certificado	Descrição
Não verificar o certificado do servidor	Desativa a verificação do certificado do servidor, o que significa que a identidade do servidor não é verificada. Esta opção não é segura.
Certificado do cliente	O certificado do cliente é usado para verificar a identidade do cliente ao se conectar ao endpoint.

Tipo de verificação de certificado	Descrição
Chave privada do cliente	A chave privada do certificado do cliente. Se criptografada, deve usar o formato tradicional PKCS #1 (o formato PKCS #8 não é suportado).
Senha da chave privada do cliente	A senha para descriptografar a chave privada do cliente. Se a chave privada não estiver criptografada, deixe este campo em branco.

10. Selecione **Test and create endpoint**.
    - Uma mensagem de sucesso é exibida se o endpoint puder ser acessado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada site.
    - Uma mensagem de erro aparece se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **Retornar aos detalhes do endpoint** e atualize as informações. Depois, selecione **Testar e criar endpoint**.

> ⓘ A criação do endpoint falha se os serviços da plataforma não estiverem habilitados para sua conta de locatário. Entre em contato com o administrador do StorageGRID.

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

Informações relacionadas

- "Especifique o URN para o endpoint dos serviços da plataforma"
- "Configurar a replicação CloudMirror"
- "Configurar notificações de eventos"
- "Configurar serviço de integração de pesquisa"

Teste a conexão para um endpoint de serviços de plataforma StorageGRID

Caso a conexão com um serviço da plataforma tenha sido alterada, você pode testar a conexão com o endpoint para validar se o recurso de destino existe e se pode ser acessado usando as credenciais que você especificou.

Antes de começar

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

Sobre esta tarefa

StorageGRID não valida se as credenciais possuem as permissões corretas.

Passos

1. Selecione **STORAGE (S3)** > **Pontos de extremidade de serviços da plataforma**.

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

2. Selecione o endpoint cuja conexão você deseja testar.

   A página de detalhes do endpoint é exibida.

3. Selecione **Test connection**.
   - Uma mensagem de sucesso é exibida se o endpoint puder ser acessado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada site.
   - Uma mensagem de erro é exibida se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **Configuração** e atualize as informações. Em seguida, selecione **Testar e salvar alterações**.

Editar um endpoint de serviços de plataforma no StorageGRID

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

Antes de começar

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

Passos

1. Selecione **STORAGE (S3)** > **Pontos de extremidade de serviços da plataforma**.

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

2. Selecione o endpoint que você deseja editar.

   A página de detalhes do endpoint é exibida.

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

   > Não é possível alterar o URN de um endpoint depois que ele foi criado.

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

> A chave privada do cliente deve estar no formato criptografado OpenSSL ou no formato de chave privada não criptografada.

d. Conforme necessário, altere o método para verificar certificados.

5. Selecione **Test and save changes**.
   - Uma mensagem de sucesso é exibida se o endpoint puder ser acessado usando as credenciais especificadas. A conexão com o endpoint é verificada a partir de um nó em cada site.
   - Uma mensagem de erro será exibida se a validação do endpoint falhar. Modifique o endpoint para corrigir o erro e, em seguida, selecione **Test and save changes**.

Excluir um endpoint de serviços da plataforma StorageGRID

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

Antes de começar

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

Passos

1. Selecione **STORAGE (S3)** > **Pontos de extremidade de serviços da plataforma**.

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

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

> Se você excluir um endpoint de serviços de plataforma que esteja em uso, o serviço de plataforma associado será desativado para qualquer bucket que use esse endpoint. Quaisquer solicitações que ainda não tenham sido concluídas serão descartadas. Novas solicitações continuarão sendo geradas até que você altere a configuração do seu bucket para não referenciar mais o URN excluído. StorageGRID reportará essas solicitações como erros irrecuperáveis.

3. Selecione **Ações** > **Excluir endpoint**.

   Uma mensagem de confirmação é exibida.

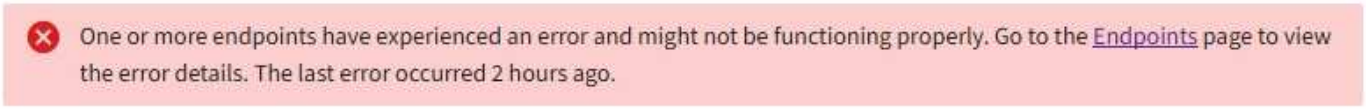
4. Selecione **Excluir endpoint**.

Solucione erros de endpoint dos serviços da plataforma StorageGRID

Se ocorrer um erro quando StorageGRID tentar se comunicar com um endpoint de serviços da plataforma, uma mensagem será exibida no painel. Na página Endpoints de serviços da plataforma, a coluna Último erro indica há quanto tempo o erro ocorreu. Nenhum erro é exibido se as permissões associadas às credenciais de um endpoint estiverem incorretas.

Determine se ocorreu algum erro

Se ocorrerem erros nos endpoints dos serviços da plataforma nos últimos 7 dias, o painel do Tenant Manager exibirá uma mensagem de alerta. Você pode acessar a página de endpoints dos serviços da plataforma para ver mais detalhes sobre o erro.



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

Passos

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

Verifique se o erro ainda persiste

Alguns erros podem continuar sendo exibidos na coluna **Último erro** mesmo após serem resolvidos. Para verificar se um erro ainda está ativo ou para forçar a remoção de um erro resolvido da tabela:

Passos

1. Selecione o endpoint.

   A página de detalhes do endpoint é exibida.

2. Selecione **Conexão** > **Testar conexão**.

Selecionar **Test connection** faz com que o StorageGRID valide se o endpoint dos serviços da plataforma existe e se pode ser acessado com as credenciais atuais. A conexão com o endpoint é validada a partir de um nó em cada site.

Resolver erros de endpoint

Você pode usar a mensagem **Último erro** na página de detalhes do endpoint para ajudar a determinar o que está causando o erro. Alguns erros podem exigir que você edite o endpoint para resolver o problema. Por exemplo, um erro CloudMirroring pode ocorrer se StorageGRID não conseguir acessar o bucket S3 de destino porque não possui as permissões de acesso corretas ou a chave de acesso expirou. A mensagem é "As credenciais do endpoint ou o acesso ao destino precisam ser atualizados" e os detalhes são "AccessDenied" ou "InvalidAccessKeyId".

Se você precisar editar o endpoint para corrigir um erro, selecionar **Testar e salvar alterações** fará com que o StorageGRID valide o endpoint atualizado e confirme que ele pode ser acessado com as credenciais atuais. A conexão com o endpoint é validada a partir de um nó em cada site.

Passos

1. Selecione o endpoint.
2. Na página de detalhes do endpoint, selecione **Configuration**.
3. Edite a configuração do endpoint conforme necessário.

4. Selecione **Conexão** > **Testar conexão**.

Credenciais de endpoint com permissões insuficientes

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

Informações relacionadas

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

Configure a replicação CloudMirror no StorageGRID

Para habilitar a replicação CloudMirror para um bucket, você cria e aplica um arquivo XML de configuração de replicação de bucket válido.

Antes de começar

- Os serviços da plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket para servir como fonte de replicação.
- O ponto de extremidade que você pretende usar como destino para CloudMirror replication já existe e você possui o seu URN.
- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Locatários.

Sobre esta tarefa

CloudMirror replica objetos de um bucket de origem para um bucket de destino especificado em um endpoint.

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

> ⓘ A replicação CloudMirror apresenta semelhanças e diferenças importantes em relação ao recurso de replicação entre grades. Para saber mais, consulte "Compare a replicação entre grades e a replicação CloudMirror".

Observe os seguintes requisitos e características ao configurar a replicação CloudMirror:

- Ao criar e aplicar um XML de configuração de replicação de bucket válido, é necessário usar o URN de um endpoint de bucket S3 para cada destino.
- A replicação não é compatível para buckets de origem ou destino com o S3 Object Lock ativado.
- Se você habilitar a replicação CloudMirror em um bucket que contém objetos, os novos objetos

adicionados ao bucket serão replicados, mas os objetos existentes no bucket não serão replicados. Você precisa atualizar os objetos existentes para acionar a replicação.

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

Passos

1. Ative a replicação para o seu bucket de origem:
   - Utilize um editor de texto para criar o XML de configuração de replicação necessário para habilitar a replicação, conforme especificado na API de replicação do S3.
   - Ao configurar o XML:
     - Observe que StorageGRID suporta apenas V1 da configuração de replicação. Isso significa que StorageGRID não suporta o uso do `Filter` elemento para regras e segue as convenções de V1 para exclusão de versões de objetos. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes.
     - Utilize o URN de um endpoint de bucket S3 como destino.
     - Opcionalmente, adicione o `<StorageClass>` elemento e especifique uma das seguintes opções:
       - `STANDARD`: A classe de armazenamento padrão. Se você não especificar uma classe de armazenamento ao carregar um objeto, a `STANDARD`classe de armazenamento padrão será usada.
       - `STANDARD_IA`: (Padrão - acesso pouco frequente.) Use esta classe de armazenamento para dados que são acessados com menos frequência, mas que ainda exigem acesso rápido quando necessário.
       - `REDUCED_REDUNDANCY`: Utilize esta classe de armazenamento para dados não críticos e reproduzíveis que podem ser armazenados com menos redundância do que a `STANDARD` classe de armazenamento.
     - Se você especificar um `Role` no XML de configuração, ele será ignorado. Esse valor não é usado pelo StorageGRID.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

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

A página de detalhes do bucket é exibida.

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

> Os serviços da plataforma devem ser ativados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a Grid Management API. Entre em contato com o administrador do StorageGRID se ocorrer um erro ao salvar o XML de configuração.

7. Verifique se a replicação está configurada corretamente:
   a. Adicione um objeto ao bucket de origem que atenda aos requisitos de replicação especificados na configuração de replicação.

      No exemplo mostrado anteriormente, os objetos que correspondem ao prefixo "2020" são replicados.

   b. Confirme se o objeto foi replicado para o bucket de destino.

      Para objetos pequenos, a replicação ocorre rapidamente.

Informações relacionadas

"Criar endpoint de serviços de plataforma"

Configure as notificações de eventos no StorageGRID

Você habilita as notificações para um bucket criando um arquivo XML de configuração de notificações e usando o Tenant Manager para aplicar o XML a um bucket.

Antes de começar

- Os serviços da plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket para servir como fonte de notificações.
- O endpoint que você pretende usar como destino para notificações de eventos já existe e você possui seu URN.
- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Locatários.

Sobre esta tarefa

Você configura as notificações de eventos associando um arquivo XML de configuração de notificações a um bucket de origem. O arquivo XML de configuração de notificações segue as convenções do S3 para configurar notificações de buckets, com o destino Amazon SNS topic, Kafka topic ou endpoint do webhook especificado como o URN de um endpoint.

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

Observe os seguintes requisitos e características ao configurar notificações de eventos para um bucket:

- Ao criar e aplicar um XML de configuração de notificação válido, é necessário usar o URN de um endpoint de notificações de eventos para cada destino.
- Embora seja possível configurar a notificação de eventos em um bucket com o S3 Object Lock ativado, os metadados do S3 Object Lock (incluindo Retain Until Date e o status de Legal Hold) dos objetos não serão incluídos nas mensagens de notificação.
- Após configurar as notificações de eventos, sempre que um evento específico ocorrer para um objeto no bucket de origem, uma notificação será gerada e enviada para o tópico Amazon SNS, tópico Kafka ou endpoint webhook usado como destino.
- Se você ativar as notificações de eventos para um bucket que contém objetos, as notificações serão enviadas apenas para ações realizadas após o salvamento da configuração de notificação.

Passos

1. Ative as notificações para seu bucket de origem:
   - Utilize um editor de texto para criar o XML de configuração de notificações necessário para habilitar as notificações de eventos, conforme especificado na API de notificações do S3.
   - Ao configurar o XML, utilize o URN de um endpoint de notificações de eventos como o tópico de destino.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. No Tenant Manager, selecione **STORAGE (S3)** > **Buckets**.
3. Selecione o nome do bucket de origem.

   A página de detalhes do bucket é exibida.

4. Selecione **Serviços da plataforma** > **Notificações de eventos**.
5. Selecione a caixa de seleção **Ativar notificações de eventos**.
6. Cole o XML de configuração de notificação na caixa de texto e selecione **Salvar alterações**.

Os serviços da plataforma devem ser ativados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a Grid Management API. Entre em contato com o administrador do StorageGRID se ocorrer um erro ao salvar o XML de configuração.

7. Verifique se as notificações de eventos estão configuradas corretamente:

   a. Execute uma ação em um objeto no bucket de origem que atenda aos requisitos para acionar uma notificação conforme configurado no XML de configuração.

      No exemplo, uma notificação de evento é enviada sempre que um objeto é criado com o `images/` prefixo.

   b. Confirme que uma notificação foi entregue ao destino Amazon SNS topic, Kafka topic ou endpoint do webhook.

      Por exemplo, se o seu tópico de destino estiver hospedado no Amazon SNS, você pode configurar o serviço para enviar um e-mail quando a notificação for entregue.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


+ Se a notificação for recebida no tópico de destino, você configurou com sucesso seu bucket de origem para notificações do StorageGRID.

Informações relacionadas

- "Entenda as notificações para buckets"
- "Utilize a API REST S3"
- "Criar endpoint de serviços de plataforma"

Configure o serviço de integração de pesquisa em StorageGRID

Você habilita a integração de pesquisa para um bucket criando um XML de integração de pesquisa e usando o Tenant Manager para aplicar o XML ao bucket.

Antes de começar

- Os serviços da plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você já criou um bucket S3 cujo conteúdo você deseja indexar.
- O endpoint que você pretende usar como destino para o serviço de integração de pesquisa já existe e você possui seu URN.
- Você pertence a um grupo de usuários que possui as "Gerenciar todos os buckets ou permissão de acesso à raiz". Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Locatários.

Sobre esta tarefa

Após configurar o serviço de integração de pesquisa para um bucket de origem, a criação de um objeto ou a atualização dos metadados ou tags de um objeto aciona o envio dos metadados do objeto para o endpoint de destino.

Se você ativar o serviço de integração de pesquisa para um bucket que já contém objetos, as notificações de metadados não serão enviadas automaticamente para os objetos existentes. Atualize esses objetos existentes para garantir que seus metadados sejam adicionados ao índice de pesquisa de destino.

Passos

1. Ativar a integração de pesquisa para um bucket:
   - Utilize um editor de texto para criar o XML de notificação de metadados necessário para habilitar a integração de pesquisa.
   - Ao configurar o XML, use o URN de um endpoint de integração de pesquisa como destino.

     Os objetos podem ser filtrados pelo prefixo do nome do objeto. Por exemplo, você pode enviar metadados para objetos com o prefixo `images` para um destino e metadados para objetos com o prefixo `videos` para outro. Configurações com prefixos sobrepostos não são válidas e são rejeitadas no momento do envio. Por exemplo, uma configuração que inclua uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não é permitida.

     Se necessário, consulte o exemplos para o XML de configuração de metadados.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

Elementos no XML de configuração da notificação de metadados:

Nome	Descrição	Obrigatório
MetadataNotificationConfiguration	Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos de Rule.	Sim
Regra	Etiqueta de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice específico. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
ID	Identificador único para a regra. Incluído no elemento Rule.	Não
Status	O status pode ser 'Ativado' ou 'Desativado'. Nenhuma ação é executada para regras desativadas. Incluído no elemento Rule.	Sim
Prefixo	Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento Rule.	Sim
Destino	Etiqueta de contêiner para o destino de uma regra. Incluído no elemento Rule.	Sim

Nome	Descrição	Obrigatório
Urna	URN do destino para onde os metadados do objeto são enviados. Deve ser o URN de um endpoint do StorageGRID com as seguintes propriedades: • `es`deve ser o terceiro elemento. • O URN deve terminar com o índice e o tipo onde os metadados estão armazenados, no formato `domain-name/myindex/mytype`. Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles têm o seguinte formato: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O endpoint deve ser configurado antes do envio do XML de configuração, ou a configuração falhará com um erro 404. O URN está incluído no elemento destino.	Sim

2. No Gerenciador de Locatários, selecione **ARMAZENAMENTO (S3)** > **Buckets**.
3. Selecione o nome do bucket de origem.

   A página de detalhes do bucket é exibida.

4. Selecione **Serviços da plataforma** > **Integração de pesquisa**
5. Selecione a caixa de seleção **Enable search integration**.
6. Cole a configuração de notificação de metadados na caixa de texto e selecione **Salvar alterações**.

   Os serviços da plataforma devem ser ativados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a Management API. Entre em contato com seu administrador do StorageGRID se ocorrer um erro ao salvar o XML de configuração.

7. Verifique se o serviço de integração de pesquisa está configurado corretamente:
   a. Adicione um objeto ao bucket de origem que atenda aos requisitos para acionar uma notificação de metadados, conforme especificado no XML de configuração.

      No exemplo mostrado anteriormente, todos os objetos adicionados ao bucket acionam uma notificação de metadados.

   b. Confirme se um documento JSON contendo os metadados e as tags do objeto foi adicionado ao índice de pesquisa especificado no endpoint.

Depois que você terminar

Se necessário, você pode desativar a integração de pesquisa para um bucket usando um dos seguintes métodos:

- Selecione **STORAGE (S3)** > **Buckets** e desmarque a caixa de seleção **Enable search integration**.
- Se você estiver usando a API S3 diretamente, use uma solicitação DELETE Bucket metadata notification. Veja as instruções para implementar aplicativos cliente S3.

Exemplo: configuração de notificação de metadados que se aplica a todos os objetos

Neste exemplo, os metadados dos objetos são enviados para o mesmo destino.

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

Exemplo: configuração de notificação de metadados com duas regras

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

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Formato de notificação de metadados

Ao ativar o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado para o endpoint de destino sempre que os metadados ou tags de um objeto são adicionados, atualizados ou excluídos.

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

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

Campos incluídos no documento JSON

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

Informações sobre buckets e objetos

`bucket`: Nome do bucket

`key`: nome da chave do objeto

`versionID`: Versão do objeto, para objetos em buckets versionados

`region`: Região do bucket, por exemplo `us-east-1`

Metadados do sistema

`size`: Tamanho do objeto (em bytes) conforme visível para um cliente HTTP

`md5`: hash de objeto

Metadados do usuário

`metadata`: Todos os metadados do usuário para o objeto, como pares de chave-valor

`key:value`

Tags

`tags`: Todas as tags de objeto definidas para o objeto, como pares chave-valor

```
key:value
```

Como visualizar resultados no Elasticsearch

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

Informações sobre direitos autorais

Informações sobre marcas comerciais