Usar StorageGRID

StorageGRID software

NetApp
December 03, 2025

Índice

Use locatários e clientes do StorageGRID

Use uma conta de inquilino

Use uma conta de inquilino

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

O que é uma conta de inquilino?

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

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 corporativo:** Se o sistema StorageGRID estiver sendo usado dentro de uma empresa, o armazenamento de objetos da grade pode ser segregado pelos diferentes departamentos da organização. Por exemplo, pode haver contas de inquilinos para o departamento de Marketing, o departamento de Suporte ao Cliente, o departamento de Recursos Humanos e assim por diante.

  > Se você usar o protocolo de cliente S3, também poderá usar buckets e políticas de bucket do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa criar contas de inquilino separadas. Veja as instruções para implementação"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 armazenamento de objetos da grade poderá ser segregado pelas diferentes entidades que alugam o armazenamento. Por exemplo, pode haver contas de inquilinos para a Empresa A, Empresa B, Empresa C e assim por diante.

Como criar uma conta de inquilino

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

- Informações básicas, incluindo nome do locatário, tipo de cliente (S3) e cota de armazenamento opcional.
- Permissões para a conta do locatário, como se a conta do locatário pode usar os serviços da plataforma S3, configurar sua própria fonte de identidade, usar o S3 Select ou usar uma conexão de federação de grade.
- O acesso root inicial para o locatário, com base no uso de grupos e usuários locais pelo sistema StorageGRID , federação de identidade ou logon único (SSO).

Além disso, os administradores de grade podem habilitar a configuração de Bloqueio de Objeto S3 para o sistema StorageGRID se as contas de locatário S3 precisarem estar em conformidade com os requisitos regulatórios. Quando o Bloqueio de Objeto S3 está habilitado, todas as contas de locatário S3 podem criar e gerenciar buckets compatíveis.

Configurar locatários do S3

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

- Configurar federação de identidade (a menos que a fonte de identidade seja compartilhada com a grade)
- Gerenciar grupos e usuários
- Use a federação de grade para clonagem de conta e replicação entre grades
- Gerenciar chaves de acesso S3
- Criar e gerenciar buckets S3
- Use os serviços da plataforma S3
- Use o S3 Select
- Monitorar o uso do armazenamento

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

Como entrar e sair

Sign in no Gerenciador de Inquilinos

Você acessa o Tenant Manager inserindo a URL do inquilino na barra de endereço de um"navegador da web compatível" .

Antes de começar

- Você tem suas credenciais de login.
- Você tem uma URL para acessar o Gerenciador de Tenants, fornecida pelo administrador da sua grade. 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 nome de domínio totalmente qualificado (FQDN), o endereço IP de um nó administrativo ou o endereço IP virtual de um grupo HA de nós administrativos. Também pode incluir um número de porta, o ID da conta do locatário de 20 dígitos ou ambos.

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

Passos

1. Lançar um"navegador da web compatível" .

2. Na barra de endereço do navegador, digite o 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. Sign in no Gerenciador de Inquilinos.

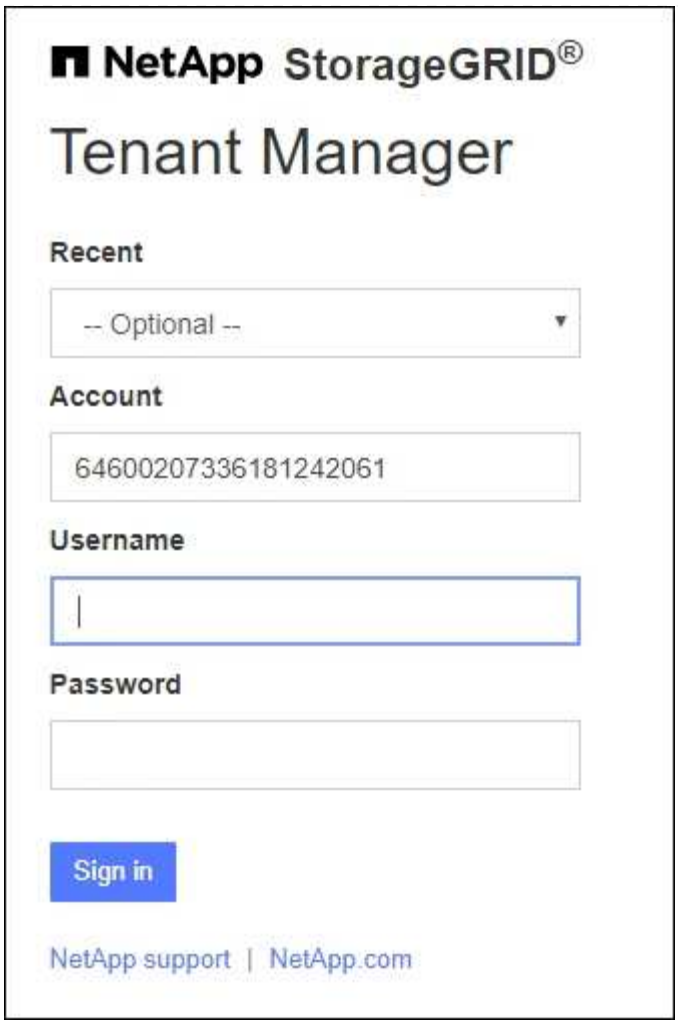
   A tela de login exibida depende do URL inserido e se o logon único (SSO) foi configurado para o StorageGRID.

Não usar SSO

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

- Página de login do Grid Manager. Selecione o link **Login do locatário**.

- Página de login do Gerenciador de inquilinos. O campo **Conta** pode já estar preenchido, conforme mostrado abaixo.



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

ii. Digite seu nome de usuário e senha.

iii. Selecione * Sign in*.

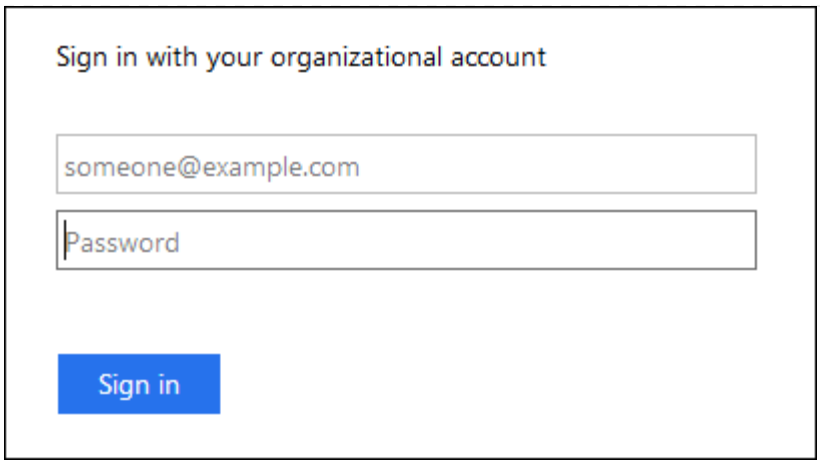
O painel do Gerenciador de inquilinos é exibido.

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

Usando SSO

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

◦ Página SSO da sua organização. Por exemplo:



Insira suas credenciais SSO padrão e selecione * Sign in*.

- Página de login do Tenant Manager SSO.

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

ii. Selecione * Sign in*.

iii. Sign in com suas credenciais SSO padrão na página de login SSO da sua organização.

O painel do Gerenciador de inquilinos é exibido.

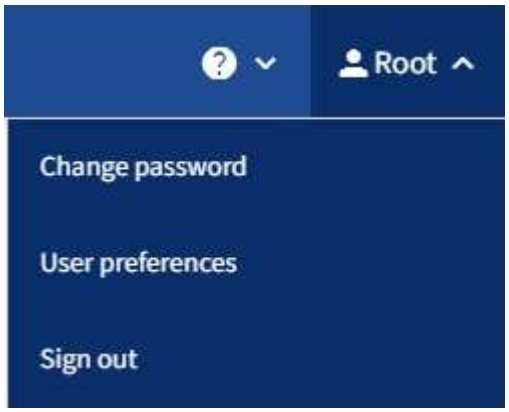
Sair do Gerenciador de Inquilinos

Quando terminar de trabalhar com o Tenant Manager, você deverá sair para garantir que usuários não autorizados não possam acessar o sistema StorageGRID . Fechar o

navegador pode não desconectar você do sistema, com base nas configurações de cookies do navegador.

Passos

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



2. Selecione o nome de usuário e depois selecione **Sair**.

   - Se o SSO não estiver em uso:

     Você está desconectado do nó de administração. A página de login do Gerenciador de inquilinos é exibida.

     Se você tiver entrado em mais de um nó de administração, será necessário sair de cada nó.

   - Se o SSO estiver habilitado:

     Você está desconectado de todos os nós de administração que estava acessando. A página de Sign in do StorageGRID é exibida. O nome da conta do locatário que você acabou de acessar é listado como padrão no menu suspenso **Contas recentes**, e o **ID da conta** do locatário é exibido.

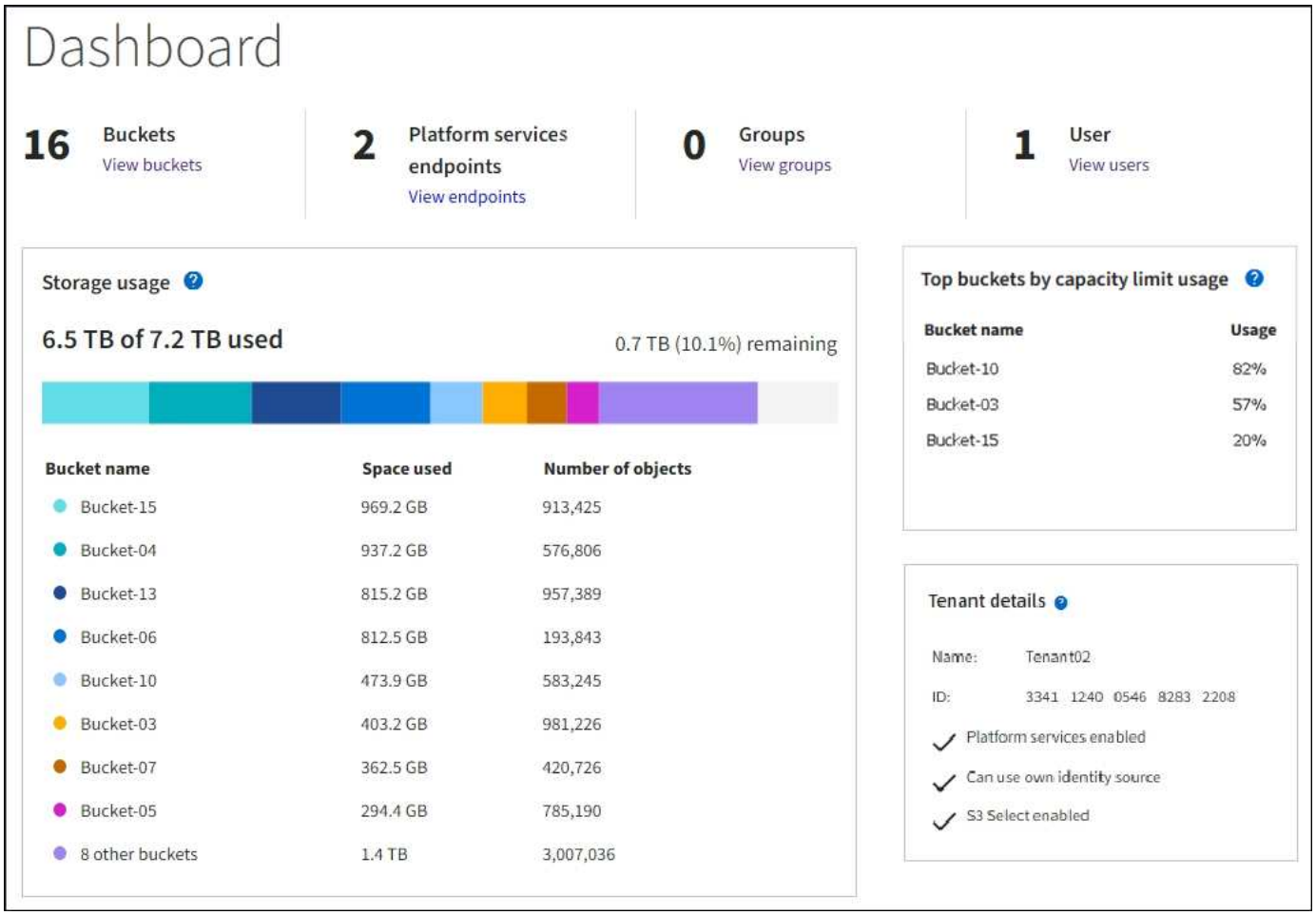
     Se o SSO estiver habilitado e você também estiver conectado ao Grid Manager, você também deverá sair do Grid Manager para sair do SSO.

Entenda o painel do Tenant Manager

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

Os valores do Espaço utilizado são estimativas. Essas estimativas são afetadas pelo tempo de ingestão, pela conectividade de rede e pelo status do nó.

Quando os objetos são carregados, o painel fica como no exemplo a seguir:



Informações da conta do inquilino

A parte superior do painel exibe o número de buckets ou contêineres, grupos e usuários configurados. Ele também exibe o número de pontos de extremidade de serviços de plataforma, se algum tiver sido configurado. Selecione os links para ver os detalhes.

Dependendo do"permissões de gerenciamento de inquilinos" você tem e as opções que você configurou, o restante do painel exibe várias combinações de diretrizes, uso de armazenamento, informações de objeto e detalhes do locatário.

Armazenamento e uso de cota

O painel de uso de armazenamento contém as seguintes informações:

- A quantidade de dados de objeto 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, a quantidade total de espaço disponível para dados de objeto e a quantidade e a porcentagem de espaço restante. A cota limita a quantidade de dados de objetos que podem ser ingeridos.

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

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

  Você pode colocar o cursor sobre qualquer um dos segmentos do gráfico para visualizar o espaço total consumido por aquele bucket ou contêiner.

- Para corresponder ao gráfico de barras, uma lista dos maiores buckets ou contêineres, incluindo a quantidade total de dados do objeto e o número de objetos para 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 baldes ou contêineres, todos os outros baldes ou contêineres serão combinados em uma única entrada na parte inferior da lista.

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

Alertas de uso de cota

Se os alertas de uso de cota tiverem sido habilitados no Grid Manager, esses alertas aparecerão no Tenant Manager quando a cota estiver baixa ou for excedida, da seguinte forma:

- Se 90% ou mais da cota de um locatário tiver sido usada, o alerta **Uso alto da cota do locatário** será acionado.

  Considere pedir ao administrador da sua rede para aumentar a cota.

- Se você exceder sua cota, uma notificação informará que você não poderá carregar novos objetos.

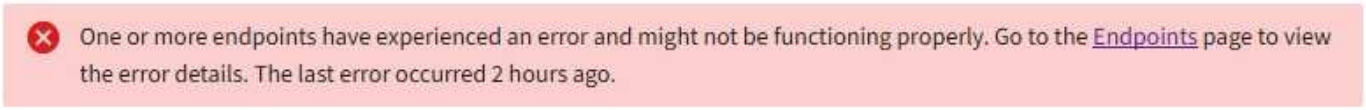
Uso do limite de capacidade

Se você definiu um limite de capacidade para seus buckets, o painel do Gerenciador de Tenants exibirá uma lista dos principais buckets por uso de 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 total de armazenamento e essa cota for atingida, você não poderá ingerir mais objetos, independentemente do limite de capacidade restante em um bucket.

Erros de endpoint

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



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

API de gerenciamento de inquilinos

Entenda a API de gerenciamento de locatários

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

API de gerenciamento de inquilinos:

- Utiliza a plataforma de API de código aberto Swagger. O Swagger fornece 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 de API.
- Usos"controle de versão para oferecer suporte a atualizações não disruptivas" .

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

1. Sign in no Gerenciador de Inquilinos.
2. Na parte superior do Gerenciador de Tenants, selecione o ícone de ajuda e selecione **Documentação da API**.

Operações de API

A API de gerenciamento de locatários organiza as operações de API disponíveis nas seguintes seções:

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

  A API de gerenciamento de locatários oferece suporte ao esquema de autenticação de token de portador. Para um login de locatário, você fornece um nome de usuário, senha e accountId no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com sucesso, um token de segurança será retornado. Este token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("Autorização: Token do portador").

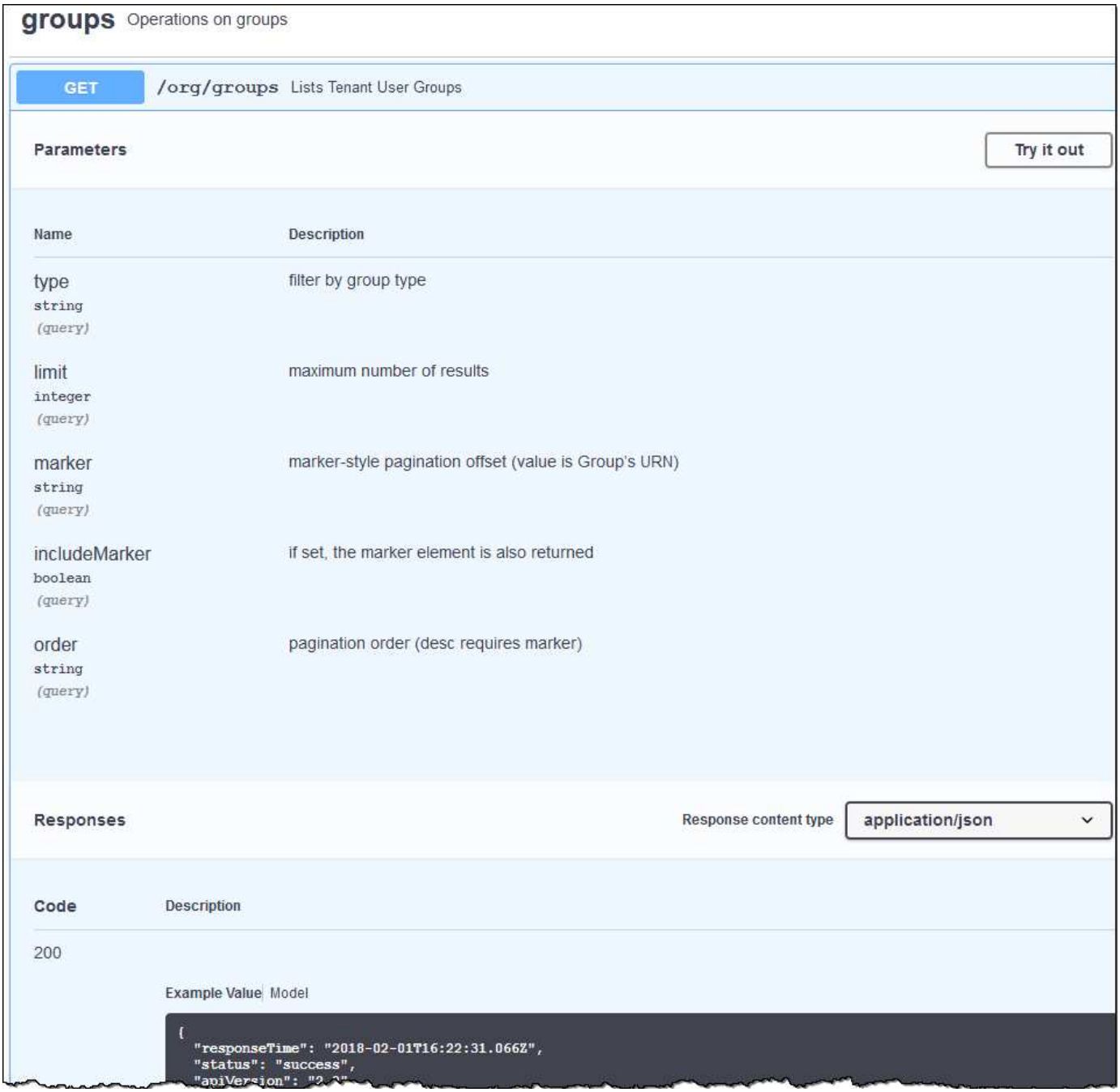
  Para obter informações sobre como melhorar a segurança da autenticação, consulte"Proteja-se contra falsificação de solicitação entre sites" .

  > ⓘ Se o logon único (SSO) estiver habilitado para o sistema StorageGRID , você deverá executar etapas diferentes para autenticar. Veja o"instruções para usar a API de gerenciamento de grade" .

- **config**: Operações relacionadas ao lançamento do produto e versões da API de gerenciamento de locatários. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **contêineres**: Operações em buckets S3 ou contêineres Swift.
- **deactivated-features**: Operações para visualizar recursos que podem ter sido desativados.
- **endpoints**: Operações para gerenciar um endpoint. Os endpoints permitem que um bucket S3 use um serviço externo para replicação, notificações ou integração de pesquisa do StorageGRID CloudMirror.
- **grid-federation-connections**: Operações em conexões de federação de rede e replicação entre redes.
- **grupos**: Operações para gerenciar grupos de inquilinos locais e recuperar grupos de inquilinos federados de uma fonte de identidade externa.
- **identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupos federados e usuários.
- **ilm**: Operações em configurações de gerenciamento do ciclo de vida da informação (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 objeto S3, usadas para dar suporte à conformidade regulatória.
- **usuários**: Operações para visualizar e gerenciar usuários locatários.

Detalhes da operação

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



Emitir solicitações de API

Todas as operações de API que você realiza usando a página de documentação da API são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Passos

1. Selecione a ação HTTP para ver os detalhes da solicitação.
2. Determine se a solicitação requer parâmetros adicionais, como um ID de grupo ou usuário. Então, obtenha esses valores. Talvez seja necessário emitir uma solicitação de API diferente primeiro para obter as informações necessárias.
3. Determine se você precisa modificar o corpo da solicitação de exemplo. Se sim, você pode selecionar **Modelo** para saber os requisitos de cada campo.

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

Controle de versão da API de gerenciamento de locatários

A API de gerenciamento de locatários usa controle de versão para oferecer suporte a atualizações sem interrupções.

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 alterada quando são feitas alterações que *não são compatíveis* com versões mais antigas. A versão secundária da API é alterada quando são feitas alterações que *são compatíveis* com versões mais antigas. Alterações compatíveis incluem a adição de novos pontos de extremidade ou novas propriedades.

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

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

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

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

Solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Obsoleto: verdadeiro"
- O corpo da resposta JSON inclui "deprecated": true
- Um aviso obsoleto foi adicionado ao nms.log. Por exemplo:

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

Determinar quais versões de API são suportadas na versão atual

Use o `GET /versions` Solicitação de API para retornar uma lista das principais versões de API suportadas. Esta solicitação está localizada na seção **config** da documentação da API do 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 de 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 substituirá o valor do caminho.

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

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

Proteja-se contra falsificação de solicitação entre sites (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra o StorageGRID usando tokens CSRF para aprimorar a autenticação que usa 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 efetuar login.

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

O StorageGRID ajuda a proteger contra ataques CSRF usando tokens CSRF. Quando ativado, o conteúdo de um cookie específico deve corresponder ao conteúdo de um cabeçalho específico ou de um parâmetro de corpo POST específico.

Para habilitar o recurso, defina o `csrfToken` parâmetro para `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 `GridCsrfToken` O cookie é definido com um valor aleatório para logins no Grid Manager e o `AccountCsrfToken` O cookie é definido com um valor aleatório para logins 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 terminais que aceitam um corpo codificado em formulário: A `csrfToken` parâmetro do corpo da solicitação codificado em formulário.

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

> Solicitações que tenham um cookie de token CSRF definido também aplicarão o cabeçalho "Content-Type: application/json" para qualquer solicitação que espere um corpo de solicitação JSON como proteção adicional contra ataques CSRF.

Usar conexões de federação de grade

Clonar grupos de locatários e usuários

Se um locatário foi criado ou editado para usar uma conexão de federação de grade, esse locatário é replicado de um sistema StorageGRID (o locatário de origem) para outro sistema StorageGRID (o locatário de réplica). Após o locatário ser replicado, todos os grupos e usuários adicionados ao locatário de origem são clonados no locatário de réplica.

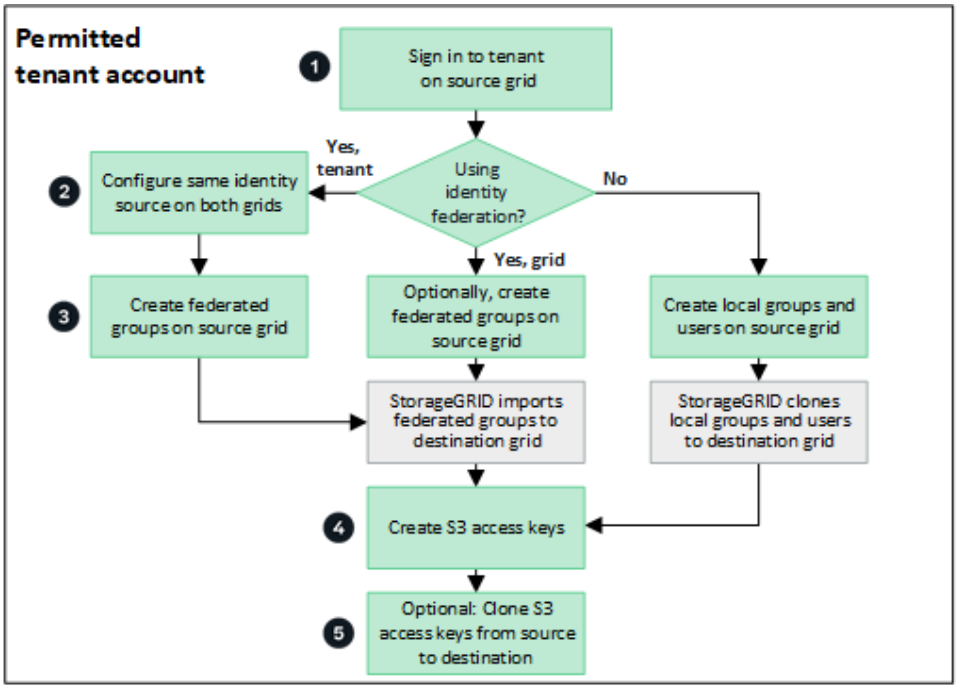
O sistema StorageGRID onde o locatário é criado originalmente é a *grade de origem* do locatário. O sistema StorageGRID onde o locatário é replicado é a *grade de destino* do locatário. Ambas as contas de locatário têm o mesmo ID de conta, nome, descrição, cota de armazenamento e permissões atribuídas,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

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

Fluxo de trabalho do locatário para clonagem de conta

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

S3.



Estas são as principais etapas do fluxo de trabalho:

1 Sign in como inquilino

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

2 Opcionalmente, configure a federação de identidade

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

3 Criar grupos e usuários

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

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

4 Criar chaves de acesso S3

Você pode"crie suas próprias chaves de acesso" ou para"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 use a API do Tenant Manager para cloná-las manualmente na grade de destino. Para obter instruções, consulte"Clonar chaves de acesso S3 usando a API" .

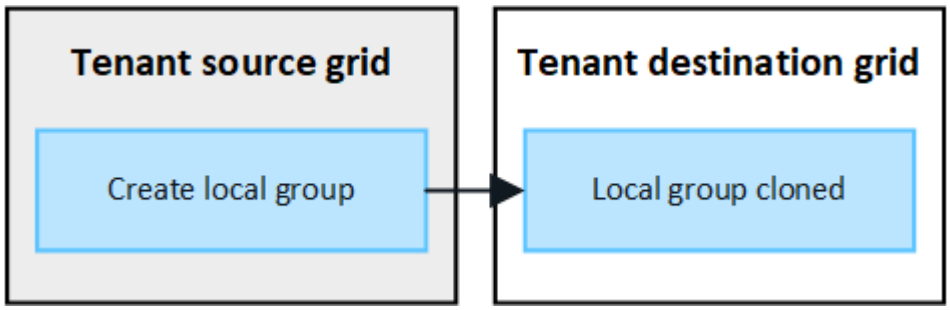
Como grupos, usuários e chaves de acesso do S3 são clonados?

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

Grupos locais criados na grade de origem são clonados

Depois que uma conta de locatário é criada e replicada para a grade de destino, o StorageGRID clona automaticamente todos os grupos locais que você adiciona à grade de origem do locatário para a grade de destino do locatário.

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

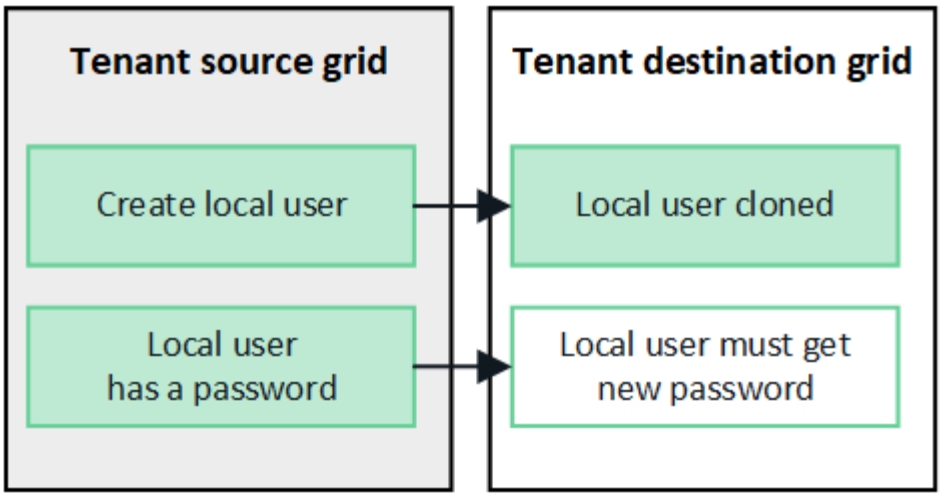


Qualquer usuário selecionado ao criar um grupo local na grade de origem não será incluído quando o grupo for clonado na grade de destino. Por esse motivo, não selecione usuários ao criar o grupo. Em vez disso, selecione o grupo ao criar os usuários.

Usuários locais criados na grade de origem são clonados

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

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

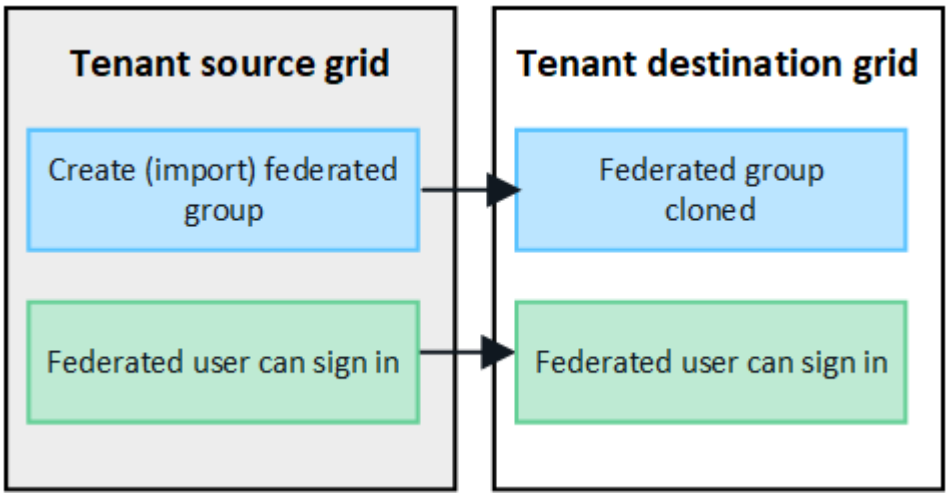


Os grupos federados criados na grade de origem são clonados

Assumindo os requisitos para usar o clone de conta com"login único" e"federação de identidade" foram atendidos, os grupos federados que você cria (importa) para o locatário na grade de origem são clonados automaticamente para o locatário na grade de destino.

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

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

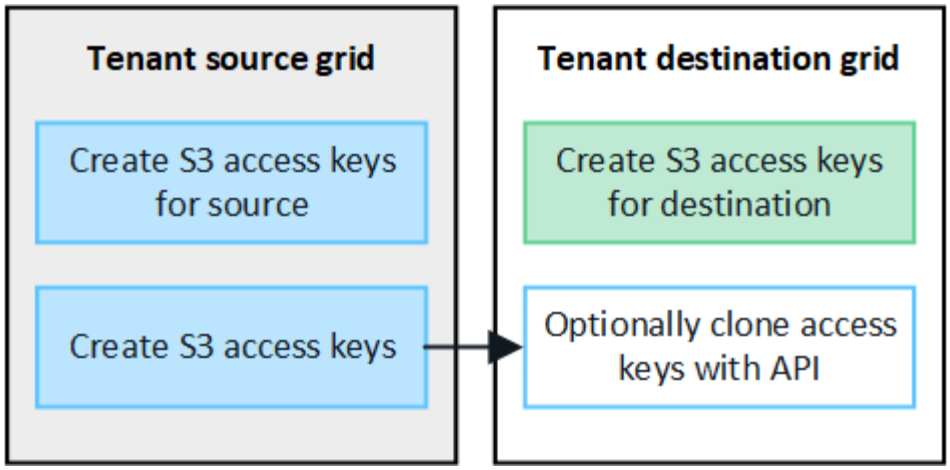


As chaves de acesso S3 podem ser clonadas manualmente

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

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

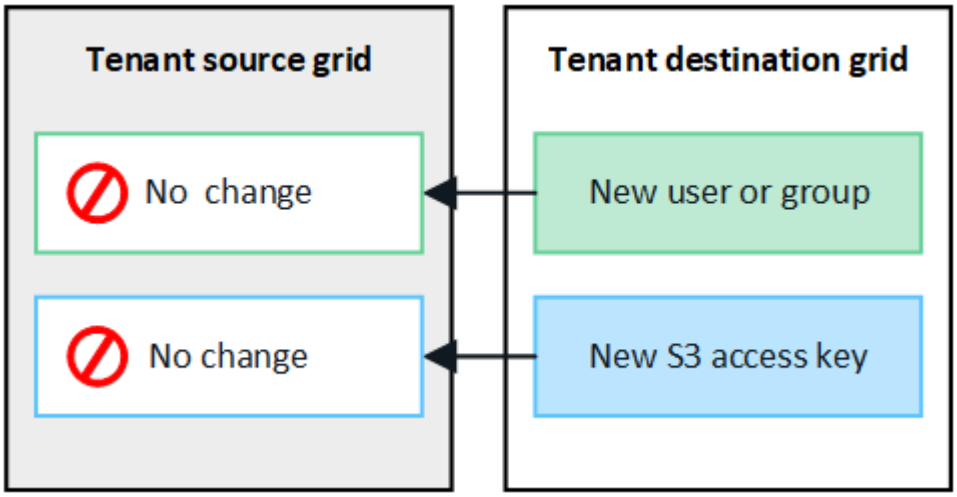
- Se você não precisa usar as mesmas chaves para cada grade, você pode"crie suas próprias chaves de acesso" ou"criar chaves de acesso de outro usuário" em cada grade.
- Se você precisar usar as mesmas chaves em ambas as grades, você pode criar chaves na grade de origem e então usar a API do Tenant Manager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



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

Grupos e usuários adicionados à grade de destino não são clonados

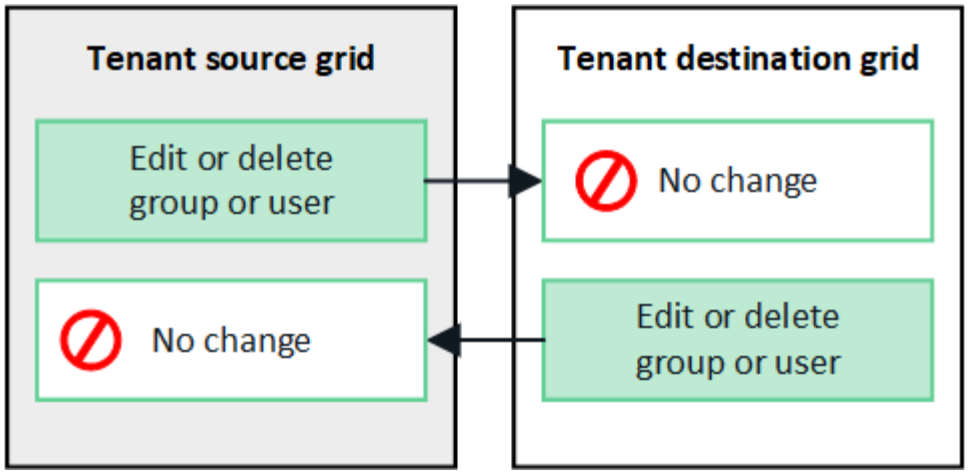
A clonagem ocorre somente da grade de origem do locatário para a grade de destino do locatário. Se você criar ou importar grupos e usuários na grade de destino do locatário, o StorageGRID não clonará esses itens de volta para a grade de origem do locatário.



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 grade, suas alterações não serão clonadas na outra grade.



Clonar chaves de acesso S3 usando a API

Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, você poderá usar a API de gerenciamento de locatários para clonar manualmente as chaves de acesso do S3 do locatário na grade de origem para o locatário na grade de destino.

Antes de começar

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

> Quando você clona chaves de acesso S3 para um usuário federado, tanto o usuário quanto as chaves de acesso S3 são adicionadas ao locatário de destino.

Clone suas próprias chaves de acesso

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

Passos

1. Usando o Tenant Manager na grade de origem,"crie suas próprias chaves de acesso" e baixe o `.csv` arquivo.
2. Na parte superior do Gerenciador de Tenants, selecione o ícone de ajuda e selecione **Documentação da API**.
3. Na seção **s3**, selecione o seguinte ponto de extremidade:

```
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 sequência de caracteres 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 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 a grade de destino.

Clonar as chaves de acesso de outro usuário

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

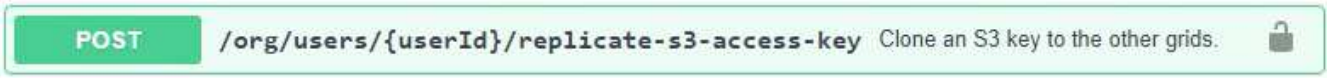
Passos

1. Usando o Tenant Manager na grade de origem,"crie as chaves de acesso S3 do outro usuário" e baixe o `.csv` arquivo.
2. Na parte superior do Gerenciador de Tenants, selecione o ícone de ajuda e selecione **Documentação da API**.
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. Encontre o usuário cujas chaves você deseja clonar e copie o número no campo **id**.
4. Na seção **s3**, selecione o seguinte ponto de extremidade:

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



5. Selecione **Experimentar**.
6. Na caixa de texto **userId**, cole o ID do usuário que você copiou.
7. Na caixa de texto **corpo**, substitua as entradas de exemplo para **chave de acesso de exemplo** e **chave de acesso secreta** pelos valores do arquivo **.csv** desse usuário.

   Certifique-se de manter as aspas duplas ao redor da string.

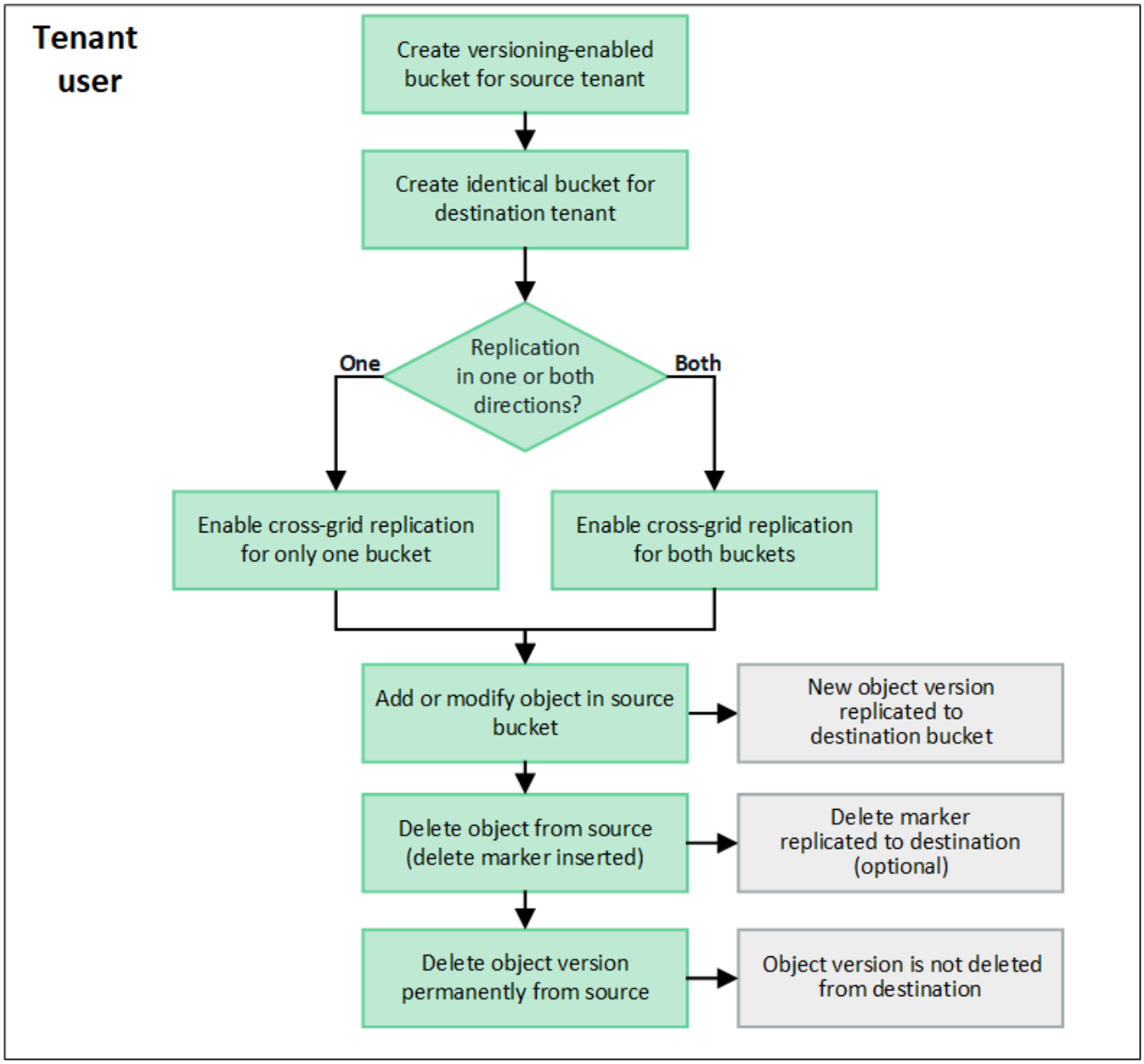
8. Se a chave expirar, substitua a entrada de exemplo para **expires** pela data e hora de expiração como uma sequência de caracteres no formato de data e hora ISO 8601 (por exemplo, `2023-02-28T22:46:33-08:00`). Se a chave não expirar, insira **null** como valor para a entrada **expires** (ou remova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

Gerenciar replicação entre redes

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

Fluxo de trabalho para replicação entre grades

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



Configurar replicação entre grades

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

Antes de começar

- Você revisou os requisitos para replicação entre redes. Ver "O que é replicação entre grades" .
- Você está usando um"navegador da web compatível" .
- A conta do locatário tem a permissão **Usar conexão de federação de grade** e contas de locatário idênticas existem em ambas as grades. Ver "Gerenciar os inquilinos permitidos para conexão de federação de rede" .
- O usuário locatário com o qual você fará login já existe em ambas as grades e pertence a um grupo de usuários que tem o"Permissão de acesso root" .

- Se você for efetuar login na 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 idênticos

Como primeiro passo, faça login nas contas de locatários correspondentes em cada grade e crie buckets idênticos.

Passos

1. A partir de qualquer grade na conexão de federação de grade, crie um novo bucket:
   a. Sign in na conta do locatário usando as credenciais de um usuário locatário que exista em ambas as grades.

      Se você não conseguir fazer login na grade de destino do locatário como um 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" .
   c. Na guia **Gerenciar configurações de objeto**, selecione **Ativar controle de versão de objeto**.
   d. Se o S3 Object Lock estiver habilitado para seu sistema StorageGRID , não habilite o S3 Object Lock para o bucket.
   e. Selecione **Criar bucket**.
   f. Selecione **Concluir**.
2. Repita essas etapas para criar um bucket idêntico para a mesma conta de locatário na outra grade na conexão de federação da grade.

   Conforme necessário, cada bucket pode usar uma região diferente.

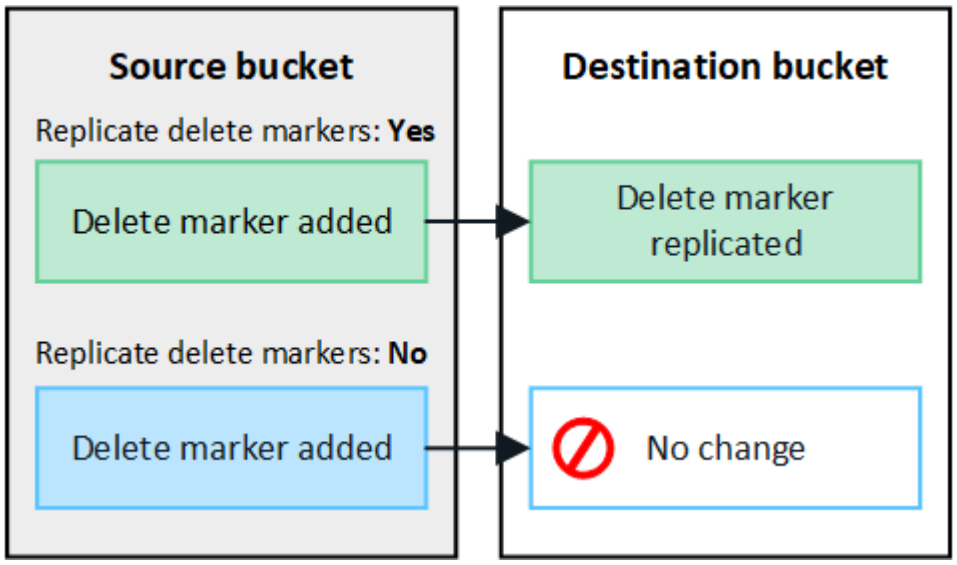
Habilitar replicação entre redes

Você deve executar estas etapas antes de adicionar qualquer objeto a qualquer um dos buckets.

Passos

1. A partir de uma grade cujos objetos você deseja replicar, habilite"replicação entre grades em uma direção" :
   a. Sign in na conta do locatário do bucket.
   b. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3)** > **Buckets**.
   c. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
   d. Selecione a aba **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 rede que você deseja usar.
   g. Opcionalmente, altere a configuração de **Replicar marcadores de exclusão** para determinar o que acontece na grade de destino se um cliente S3 emitir uma solicitação de exclusão para a grade de origem que não inclua um ID de versão:

- **Sim** (padrão): Um marcador de exclusão é adicionado ao bucket de origem e replicado no bucket de destino.
- **Não**: Um marcador de exclusão é adicionado ao bucket de origem, mas não é replicado no bucket de destino.



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

Ver"O que é replicação entre grades" para mais detalhes.

a. Opcionalmente, altere a configuração da categoria de auditoria **Replicação entre grades** para gerenciar o volume de mensagens de auditoria:
   - **Erro** (padrão): Somente solicitações de replicação entre grades 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 serão replicados automaticamente para a outra grade. **A replicação entre grades** é mostrada como um recurso habilitado na página de detalhes do bucket.

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

Replicação de teste entre grades

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

Antes de começar

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

Passos

1. Sign in na conta do locatário do bucket.
2. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3)** > **Buckets**.
3. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
4. Selecione a aba **Replicação entre grades**.
5. Selecione **Testar conexão**.

   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 grade podem usar para resolver o problema. Para obter detalhes, consulte "Solucionar erros de federação de grade" .

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

Desabilitar replicação entre grades

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

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

- Desabilitar 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 serão removidos se você desabilitar a replicação entre grades para esse bucket. Se você quiser excluir esses objetos, deverá 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 poderá 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 a replicar objetos de `my-bucket` na Grade 2 para `my-bucket` na Grade 1.
- Você deve desabilitar a replicação entre redes antes de poder remover a permissão de um locatário para usar a conexão de federação de rede. Ver "Gerenciar inquilinos permitidos" .
- Se você desabilitar a replicação entre grades para um bucket que contém objetos, não será possível habilitá-la novamente, a menos que você exclua todos os objetos dos buckets de origem e de destino.

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

Antes de começar

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

Passos

1. A partir da grade cujos objetos você não deseja mais replicar, interrompa a replicação entre grades para o bucket:

a. Sign in na conta do locatário do bucket.
b. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3)** > **Buckets**.
c. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
d. Selecione a aba **Replicação entre grades**.
e. Selecione **Desativar replicação**.
f. Se você tiver certeza de que deseja desabilitar a replicação entre grades para este bucket, digite **Sim** na caixa de texto e selecione **Desabilitar**.

   Após alguns instantes, uma mensagem de sucesso é exibida. Novos objetos adicionados a este bucket não podem mais ser replicados automaticamente para a outra grade. **A replicação entre grades** não é mais exibida como um recurso Habilitado na página Buckets.

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

Ver conexões de federação de grade

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

Antes de começar

- A conta do locatário tem a permissão **Usar conexão de federação de grade**.
- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Permissão de acesso root" .

Passos

1. Selecione **ARMAZENAMENTO (S3)** > **Conexões de federação de rede**.

   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 da federação de grade que este locatário tem permissão para usar.
Buckets com replicação entre grades	Para cada conexão de federação de grade, os buckets de locatários que têm replicação entre grades habilitada. Os objetos adicionados a esses buckets serão replicados para a outra grade na conexão.
Último erro	Para cada conexão de federação de grade, o erro mais recente ocorrido, se houver, quando os dados estavam sendo replicados para a outra grade. Ver Limpe 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 destes 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 tem o controle de versão suspenso.
- O bucket de destino foi recriado pela mesma conta, mas agora não tem versão.

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

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 grades estava em um estado inválido, possivelmente porque o controle de versão foi suspenso ou o bloqueio de objeto do S3 estava habilitado.

2. Execute todas as ações recomendadas. Por exemplo, se o controle de versão foi suspenso no bucket de destino para replicação entre grades, reative o controle de versão 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. Espere de 5 a 6 minutos e então ingira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.

   Para garantir que a mensagem de erro seja apagada, aguarde pelo menos 5 minutos após o registro de data e hora na mensagem antes de ingerir um novo objeto.

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

Gerenciar grupos e usuários

Usar federação de identidade

O uso da federação de identidades agiliza a configuração de grupos de locatários e usuários e permite que usuários locatários efetuem login na conta do locatário usando credenciais conhecidas.

Configurar federação de identidade para o Tenant Manager

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

Antes de começar

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

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

- Se você planeja usar o OpenLDAP, deverá configurar o servidor OpenLDAP. Ver 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 usar o TLS 1.2 ou 1.3. Ver "Cifras suportadas para conexões TLS de saída" .

Sobre esta tarefa

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

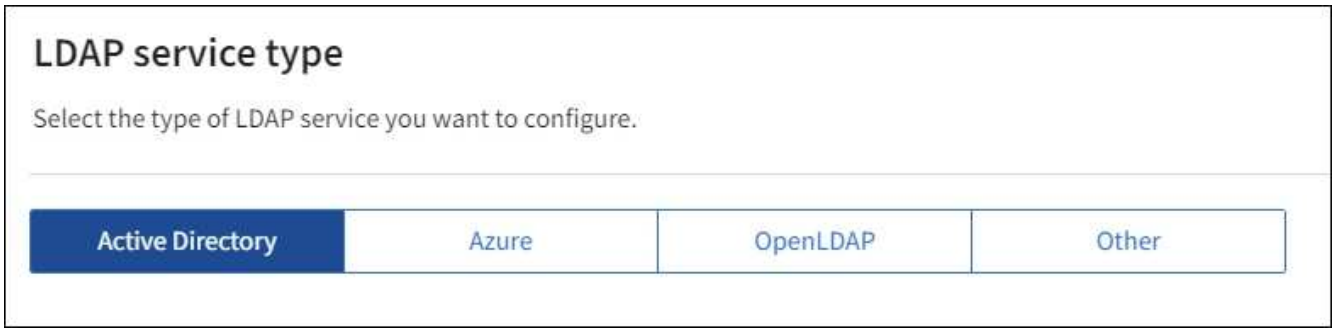
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Insira a configuração

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

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **Federação de identidade**.
2. Selecione **Ativar federação de identidade**.
3. Na seção Tipo de serviço LDAP, selecione o tipo de serviço LDAP que você deseja configurar.



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

4. Se você selecionou **Outro**, preencha os campos na seção Atributos LDAP. Caso contrário, vá para a próxima etapa.
   - **Nome exclusivo do usuário**: O nome do atributo que contém o identificador exclusivo de um usuário LDAP. Este atributo é equivalente a `sAMAccountName` para o 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 exclusivo permanente de um usuário LDAP. Este atributo é equivalente a `objectGUID` para o Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando o 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 hifens são ignorados.
   - **Nome exclusivo do grupo**: O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente a `sAMAccountName` para o Active Directory e `cn` para OpenLDAP. Se você estiver configurando o Oracle Directory Server, insira `cn` .
   - **UUID do grupo**: O nome do atributo que contém o identificador exclusivo permanente de um grupo LDAP. Este atributo é equivalente a `objectGUID` para o Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando o 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 hifens 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 nome de 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 distinto (DN) do usuário que se conectará ao servidor LDAP.

     Para o Active Directory, você também pode especificar o Nome de logon de nível inferior ou o Nome principal do usuário.

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

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

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

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

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

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

> Os valores de **Nome exclusivo do grupo** devem ser exclusivos dentro do **DN base do grupo** ao qual pertencem.

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

> Os valores de **Nome exclusivo do usuário** devem ser exclusivos dentro do **DN base do usuário** ao qual pertencem.

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

É recomendável fornecer o **formato de nome de usuário de associação** porque ele pode permitir que os usuários efetuem login caso o StorageGRID não consiga se associar à conta de serviço.

Insira um destes padrões:

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

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

6. Na seção Segurança da Camada de Transporte (TLS), selecione uma configuração de segurança.
   ◦ **Use 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 suportada pelo Azure.
   ◦ **Usar LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar esta opção para o Azure.
   ◦ **Não use TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido. Esta opção não é suportada pelo Azure.

O uso da opção **Não usar TLS** não é suportado se o seu servidor Active Directory impõe 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 conexões.
   - **Usar certificado CA personalizado**: Use um certificado de segurança personalizado.

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

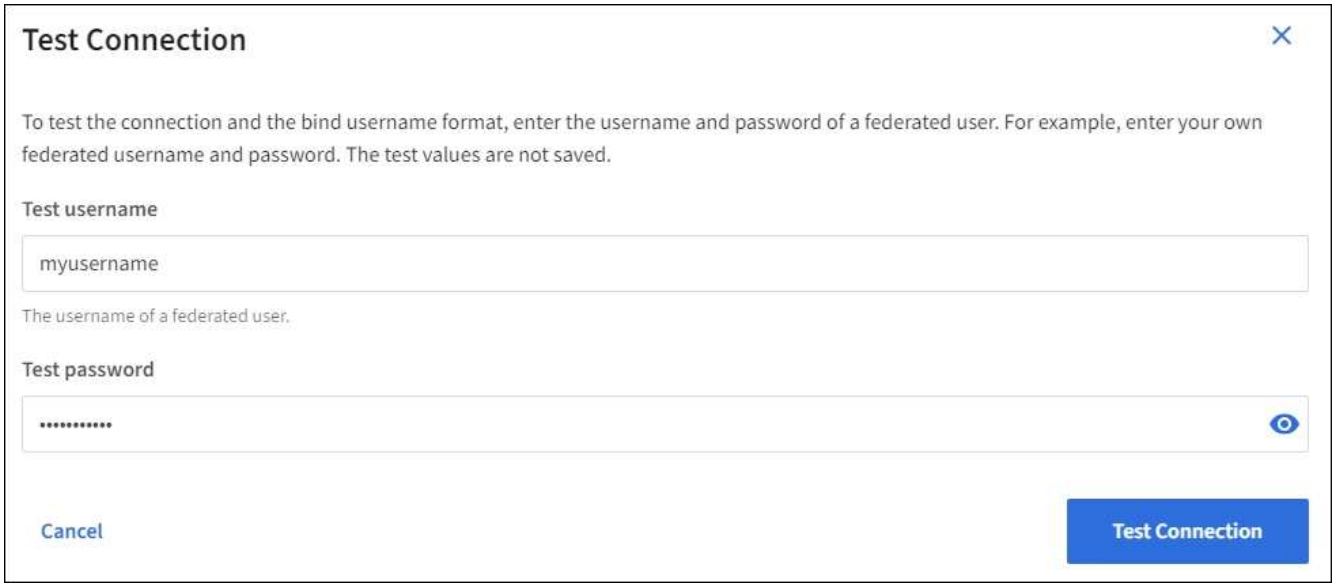
Teste a conexão e salve a configuração

Depois de inserir todos os valores, você deve testar a conexão antes de salvar a configuração. O StorageGRID verifica as configurações de conexão do servidor LDAP e o formato do nome de usuário de vinculação, se você forneceu um.

Passos

1. Selecione **Testar conexão**.
2. Se você não forneceu um formato de nome de usuário de vinculação:
   - A mensagem "Teste de conexão bem-sucedido" será exibida se as configurações de conexão forem válidas. Selecione **Salvar** para salvar a configuração.
   - A mensagem "não foi possível estabelecer a conexão de teste" aparece 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 vinculado, insira o nome de usuário e a senha de um usuário federado válido.

   Por exemplo, digite seu próprio nome de usuário e senha. Não inclua nenhum caractere especial no nome de usuário, como @ ou /.



   - A mensagem "Teste de conexão bem-sucedido" será 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 a 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 federados e usuários da fonte de identidade. Você pode forçar o início da sincronização se quiser habilitar ou restringir as permissões do usuário o mais rápido possível.

Passos

1. Acesse a página da Federação de Identidade.
2. Selecione **Servidor de sincronização** no topo da página.

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

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

Desabilitar federação de identidade

Você pode desabilitar temporária ou permanentemente a federação de identidade para grupos e usuários. Quando a federação de identidade está desabilitada, não há comunicação entre o StorageGRID e a origem da identidade. No entanto, todas as configurações que você definiu serão mantidas, permitindo que você reative facilmente a federação de identidades no futuro.

Sobre esta tarefa

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

- Usuários federados não poderão fazer login.
- Usuários federados que estão conectados no momento manterão acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.
- A sincronização entre o sistema StorageGRID e a fonte de identidade não ocorrerá, e alertas não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Habilitar federação de identidade** será desabilitada se o logon único (SSO) estiver definido como **Habilitado** ou **Modo Sandbox**. O status do SSO na página de logon único deve ser **Desativado** antes que você possa desabilitar a federação de identidades. Ver "Desativar logon único" .

Passos

1. Acesse a página da Federação de Identidade.
2. Desmarque a caixa de seleção **Ativar federação de identidade**.

Diretrizes para configurar o servidor OpenLDAP

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

Para fontes de identidade que não sejam ActiveDirectory ou Azure, o StorageGRID não bloqueará automaticamente o acesso ao S3 para usuários desabilitados externamente. Para bloquear o acesso ao S3, exclua todas as chaves S3 do usuário ou remova o usuário de todos os grupos.

Sobreposições de membro e reintegração

As sobreposições memberof e refint devem ser habilitadas. Para obter mais informações, consulte as instruções para manutenção de associação de grupo reverso nohttp://www.openldap.org/doc/admin24/index.html["Documentação do OpenLDAP: Guia do Administrador da Versão 2.4"^] .

Indexação

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

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

Além disso, certifique-se de que os campos mencionados na ajuda para Nome de usuário sejam indexados para desempenho ideal.

Veja as informações sobre manutenção de associação de grupo reverso nohttp://www.openldap.org/doc/admin24/index.html["Documentação do OpenLDAP: Guia do Administrador da Versão 2.4"^] .

Gerenciar grupos de inquilinos

Criar grupos para um locatário S3

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem 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 sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, você revisou o fluxo de trabalho e as considerações para"clonagem de grupos de inquilinos e usuários" , e você está conectado à grade de origem do locatário.

Acesse o assistente Criar grupo

Como primeiro passo, acesse o assistente Criar grupo.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **Grupos**.
2. Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, confirme se um banner azul aparece, indicando que novos grupos criados nesta grade serão clonados para o mesmo locatário na outra grade na conexão. Se este banner não aparecer, você pode estar conectado à grade de destino do locatário.

3. Selecione **Criar grupo**.

Escolha um tipo de grupo

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

Passos

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

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

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

   - **Grupo federado**: Insira o nome exclusivo. Para o 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 **Continuar**.

Gerenciar permissões de grupo

As permissões de grupo controlam quais tarefas os usuários podem executar no Tenant Manager e na Tenant Management API.

Passos

1. Para **Modo de acesso**, selecione uma das seguintes opções:
   - **Leitura e gravação** (padrão): os usuários podem fazer login no Tenant Manager e gerenciar a configuração do locatário.
   - **Somente leitura**: os usuários podem apenas visualizar configurações e recursos. Eles não podem fazer nenhuma alteração ou executar nenhuma operação no Tenant Manager ou na Tenant Management API. Usuários locais somente leitura podem alterar suas próprias senhas.

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

2. Selecione uma ou mais permissões para este grupo.

   Ver "Permissões de gerenciamento de inquilinos" .

3. Selecione **Continuar**.

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 S3	Padrão. Os usuários neste grupo não têm acesso aos recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar esta opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
Acesso somente leitura	Os usuários neste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários neste grupo podem listar objetos e ler dados de objetos, metadados e tags. Quando você seleciona esta opção, a string JSON para uma política de grupo somente leitura aparece na caixa de texto. Você não pode editar esta sequência.
Acesso total	Os usuários neste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona esta opção, a string JSON para uma política de grupo de acesso total aparece na caixa de texto. Você não pode editar esta sequência.

Política de grupo	Descrição
Mitigação de Ransomware	Esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários neste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que tenham o controle de versão de objetos habilitado. Usuários do Tenant Manager que têm a permissão **Gerenciar todos os buckets** podem substituir esta política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação Multifator (MFA) quando disponível.
Personalizado	Os usuários do grupo recebem as permissões que você especifica 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 válida no formato JSON.

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

3. Se você estiver criando um grupo local, selecione **Continuar**. Se você 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 sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, todos os usuários selecionados ao criar um grupo local na grade de origem não serão incluídos quando o grupo for clonado na grade 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 sua conta de locatário tiver a permissão **Usar conexão de federação de grade** e você estiver na grade de origem do locatário, o novo grupo será clonado na grade de destino do locatário. **Sucesso** aparece como **Status de clonagem** na seção Visão geral da página de detalhes do grupo.

Criar grupos para um locatário Swift

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

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem 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.

Acesse o assistente Criar grupo

Passos

Como primeiro passo, acesse o assistente Criar grupo.

1. Selecione **GERENCIAMENTO DE ACESSO** > **Grupos**.
2. Selecione **Criar grupo**.

Escolha um tipo de grupo

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

Passos

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

   Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID , os usuários pertencentes a grupos locais não poderão fazer logon no Gerenciador de locatários, embora possam usar aplicativos cliente para gerenciar os recursos do locatário, com base nas permissões do 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 mais tarde.
   - **Grupo federado**: Insira o nome exclusivo. Para o 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 **Continuar**.

Gerenciar permissões de grupo

As permissões de grupo controlam quais tarefas os usuários podem executar no Tenant Manager e na Tenant Management API.

Passos

1. Para **Modo de acesso**, selecione uma das seguintes opções:
   - **Leitura e gravação** (padrão): os usuários podem fazer login no Tenant Manager e gerenciar a configuração do locatário.
   - **Somente leitura**: os usuários podem apenas visualizar configurações e recursos. Eles não podem fazer nenhuma alteração ou executar nenhuma operação no Tenant Manager ou na Tenant Management API. Usuários locais somente leitura podem alterar suas próprias senhas.

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

2. Selecione a caixa de seleção **Acesso root** se os usuários do grupo precisarem fazer login no Gerenciador de Tenants ou na API de Gerenciamento de Tenants.
3. Selecione **Continuar**.

Definir política de grupo Swift

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

1. Selecione a caixa de seleção **Administrador Swift** se os usuários do grupo precisarem usar a API REST do Swift para gerenciar contêineres e objetos.
2. Se você estiver criando um grupo local, selecione **Continuar**. Se você 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.

Passos

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

   Se você ainda não criou usuários locais, pode adicionar este grupo ao usuário na página Usuários. Ver "Gerenciar usuários locais" .

2. Selecione **Criar grupo** e **Concluir**.

   O grupo que você criou aparece na lista de grupos.

Permissões de gerenciamento de inquilinos

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 Gerenciador de Locatários ou a API de Gerenciamento de Locatários. Um usuário pode pertencer a um ou mais grupos. As permissões são cumulativas se um usuário pertencer a vários grupos.

Para fazer login no Tenant Manager ou usar a API de gerenciamento de locatários, os usuários devem pertencer a um grupo que tenha pelo menos uma permissão. Todos os usuários que podem fazer login podem executar as seguintes tarefas:

- Ver o painel
- Alterar sua própria senha (para usuários locais)

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

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

Você pode atribuir as seguintes permissões a um grupo. Observe que os locatários do S3 e do Swift têm permissões de grupo diferentes.

Permissão	Descrição	Detalhes
Acesso root	Fornece acesso total ao Gerenciador de Inquilinos e à API de Gerenciamento de Inquilinos.	Os usuários do Swift devem ter permissão de acesso Root para fazer login na conta do locatário.
Administrador	Somente inquilinos do Swift. Fornece acesso total aos contêineres e objetos Swift para esta conta de locatário	Os usuários do Swift devem ter permissão de administrador do Swift para executar qualquer operação com a API REST do Swift.
Gerencie suas próprias credenciais S3	Permite que os usuários criem e removam suas próprias chaves de acesso S3.	Usuários que não têm essa permissão não veem a opção de menu **ARMAZENAMENTO (S3)** > **Minhas chaves de acesso S3**.
Ver todos os baldes	**Locatários S3**: Permite que os usuários visualizem todos os buckets e configurações de buckets. **Inquilinos Swift**: Permite que usuários Swift visualizem todos os contêineres e configurações de contêineres usando a API de gerenciamento de inquilinos.	Usuários que não têm a permissão Exibir todos os buckets ou Gerenciar todos os buckets não veem a opção de menu **Buckets**. Esta permissão é substituída pela permissão Gerenciar todos os buckets. Não afeta as políticas de grupo ou bucket do S3 usadas pelos clientes do S3 ou pelo Console do S3. Você só pode atribuir essa permissão a grupos Swift da API de gerenciamento de locatários. Você não pode atribuir essa permissão a grupos Swift usando o Gerenciador de Tenants.

Permissão	Descrição	Detalhes
Gerenciar todos os buckets	**Locatários S3**: permite que os usuários usem o Gerenciador de Locatários e a API de Gerenciamento de Locatários para criar e excluir buckets S3 e gerenciar as configurações de todos os buckets S3 na conta do locatário, independentemente das políticas de grupo ou bucket S3. **Inquilinos Swift**: Permite que usuários Swift controlem a consistência dos contêineres Swift usando a API de gerenciamento de inquilinos.	Usuários que não têm a permissão Exibir todos os buckets ou Gerenciar todos os buckets não veem a opção de menu **Buckets**. Esta permissão substitui a permissão Exibir todos os buckets. Não afeta as políticas de grupo ou bucket do S3 usadas pelos clientes do S3 ou pelo Console do S3. Você só pode atribuir essa permissão a grupos Swift da API de gerenciamento de locatários. Você não pode atribuir essa permissão a grupos Swift usando o Gerenciador de Tenants.
Gerenciar endpoints	Permite que os usuários usem o Tenant Manager ou a Tenant Management API para criar ou editar pontos de extremidade de serviço da plataforma, que são usados como destino para os serviços da plataforma StorageGRID .	Usuários que não têm essa permissão não veem a opção de menu **Pontos de extremidade de serviços da plataforma**.
Usar a guia Console do S3	Quando combinado com a permissão Exibir todos os buckets ou Gerenciar todos os buckets, permite que os usuários visualizem e gerenciem objetos na guia Console do S3 na página de detalhes de um bucket.	

Gerenciar grupos

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Permissão de acesso root" .

Ver ou editar grupo

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

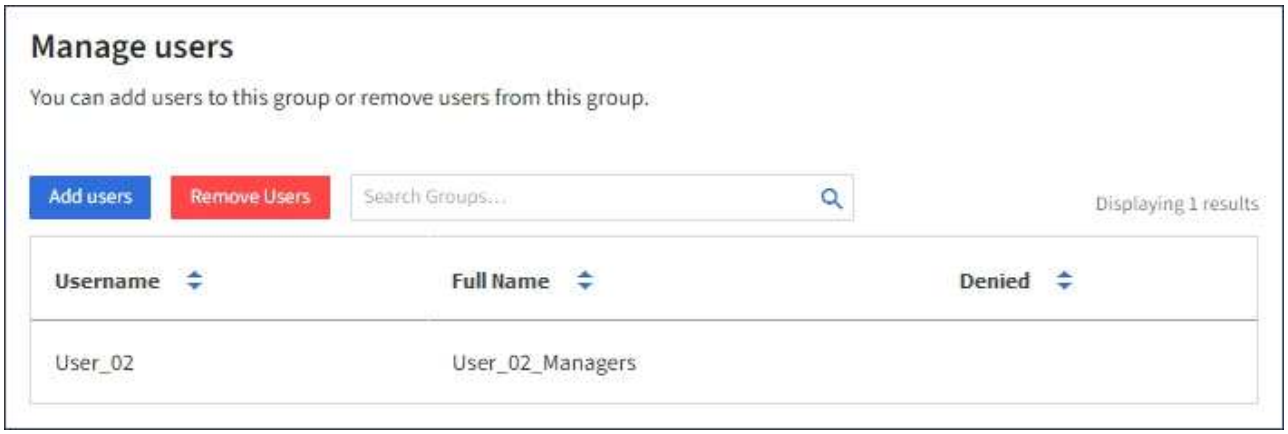
Passos

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

   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 de banner indica que se você editar ou remover um grupo, suas alterações não serão sincronizadas com a outra grade.
- Conforme necessário, uma mensagem de banner indica se os grupos não foram clonados para o locatário na grade de destino. Você podetentar novamente um clone de grupo que falhou.

3. Se você quiser alterar o nome do grupo:
   a. Marque a caixa de seleção do grupo.
   b. Selecione **Ações** > **Editar nome do grupo**.
   c. Digite o novo nome.
   d. Selecione **Salvar alterações.**
4. Se quiser ver mais detalhes ou fazer edições adicionais, faça um dos seguintes:
   - Selecione o nome do grupo.
   - Marque a caixa de seleção do grupo e selecione **Ações** > **Exibir detalhes do grupo**.
5. Revise a seção Visão geral, que mostra 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 grade** e você estiver visualizando o grupo na grade de origem do locatário:
     - Status de clonagem, **Sucesso** ou **Falha**
     - Um banner azul indicando que se você editar ou excluir este grupo, suas alterações não serão sincronizadas com a outra grade.
6. Edite as configurações do grupo conforme necessário. Ver"Criar grupos para um locatário S3" e"Criar grupos para um locatário Swift" 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 aba **Permissões do grupo**, atualize as permissões e selecione **Salvar alterações**.
   c. Na aba **Política de grupo**, faça as alterações e selecione **Salvar alterações**.
      - Se você estiver editando um grupo S3, opcionalmente selecione uma política de grupo S3 diferente ou insira a string JSON para uma política personalizada, conforme necessário.
      - Se você estiver editando um grupo Swift, opcionalmente, selecione ou desmarque a caixa de seleção **Administrador Swift**.
7. Para adicionar um ou mais usuários locais existentes ao grupo:
   a. Selecione a aba 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 aba Usuários.

b. Selecione **Remover usuários**.

c. Selecione os usuários que deseja remover e selecione **Remover usuários**.

Uma mensagem de sucesso aparece no canto superior direito.

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

Grupo duplicado

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

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

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **Grupos**.
2. Marque a caixa de seleção do grupo que você deseja duplicar.
3. Selecione **Ações** > **Duplicar grupo**.
4. Ver"Criar grupos para um locatário S3" ou"Criar grupos para um locatário Swift" para obter detalhes sobre o que inserir.
5. Selecione **Criar grupo**.

Clone do grupo de repetição

Para tentar novamente um clone que falhou:

1. Selecione cada grupo que indica *(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 locatários e usuários" .

Excluir um ou mais grupos

Você pode excluir um ou mais grupos. Qualquer usuário que pertença apenas a um grupo excluído não poderá mais fazer login no Gerenciador de Locatários nem usar a conta do locatário.

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

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **Grupos**.
2. Marque a caixa de seleção de 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**.

Gerenciar usuários locais

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

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Permissão de acesso root" .
- Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, você revisou o fluxo de trabalho e as considerações para"clonagem de grupos de inquilinos e usuários" , e você está conectado à grade 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 ou 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.

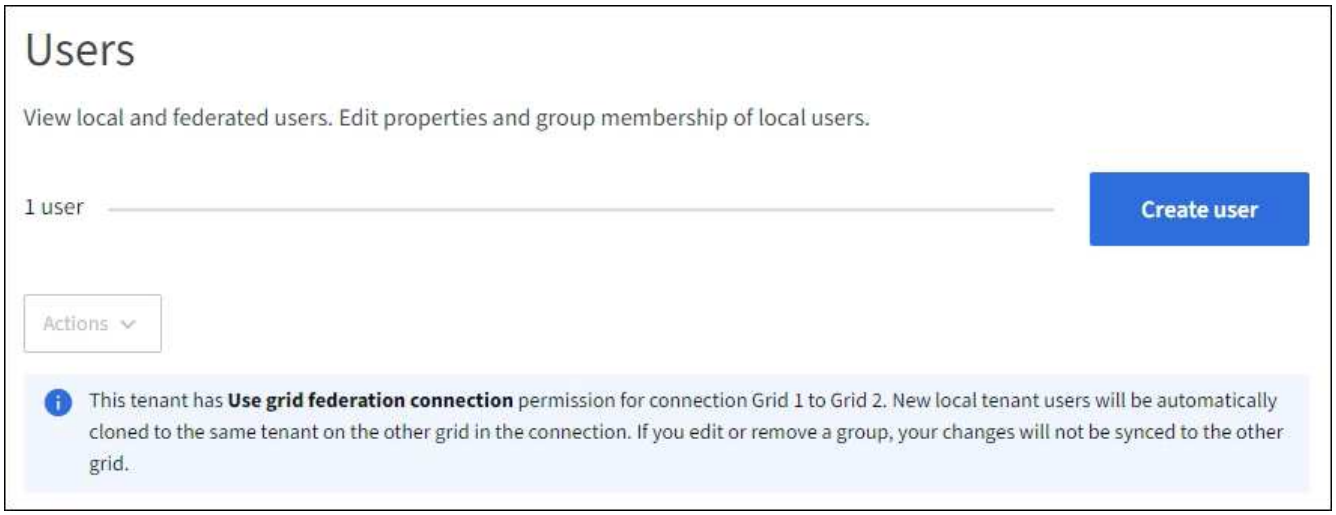
Usuários do Swift que não pertencem a nenhum grupo não têm permissões de gerenciamento ou acesso ao contêiner do Swift.

Acesse o assistente Criar usuário

Passos

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

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



2. Selecione **Criar usuário**.

Insira as credenciais

Passos

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

Campo	Descrição
Nome completo	O nome completo deste usuário, por exemplo, o nome e o 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 exclusivos e não podem ser alterados. **Observação**: se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, ocorrerá um erro de clonagem se o mesmo **Nome de usuário** já existir para o locatário na grade de destino.
Senha e Confirmar senha	A senha que o usuário usará inicialmente ao fazer login.

Campo	Descrição
Negar acesso	Selecione **Sim** para impedir que este usuário faça login na conta do locatário, mesmo que ele ainda pertença a um ou mais grupos. Por exemplo, selecione **Sim** para suspender temporariamente a capacidade de um usuário fazer login.

2. Selecione **Continuar**.

Atribuir a grupos

Passos

1. Atribua o usuário a um ou mais grupos locais para determinar quais tarefas 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. Os usuários terão todas as permissões para todos os grupos aos quais pertencem. Ver "Permissões de gerenciamento de inquilinos" .

2. Selecione **Criar usuário**.

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

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

Ver ou editar usuário local

Passos

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

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

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

- Selecione o nome de usuário.
- Marque a caixa de seleção do usuário e selecione **Ações** > **Exibir detalhes do usuário**.

5. Revise a seção Visão geral, que mostra as seguintes informações para cada usuário:
   - Nome completo
   - Nome de usuário
   - Tipo de usuário
   - Acesso negado
   - Modo de acesso
   - Associação ao grupo
   - Campos adicionais se a conta do locatário tiver a permissão **Usar conexão de federação de grade** e você estiver visualizando o usuário na grade de origem do locatário:
     - Status de clonagem, **Sucesso** ou **Falha**
     - Um banner azul indicando que se você editar este usuário, suas alterações não serão sincronizadas com a outra grade.
6. Edite as configurações do usuário conforme necessário. VerCriar usuário local para obter 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 aba **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 aba **Chaves de acesso**, selecione **Criar chave** e siga as instruções para"criando chaves de acesso S3 de outro usuário" .
   e. Na guia **Grupos**, selecione **Editar grupos** para adicionar o usuário aos grupos ou removê-lo dos grupos. Em seguida, selecione **Salvar alterações**.
7. Confirme se você selecionou **Salvar alterações** para cada seção alterada.

Usuário local duplicado

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

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

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **Usuários**.
2. Marque a caixa de seleção do usuário que você deseja duplicar.
3. Selecione **Ações** > **Duplicar usuário**.
4. VerCriar usuário local para obter detalhes sobre o que inserir.
5. Selecione **Criar usuário**.

Repetir clonagem do usuário

Para tentar novamente um clone que falhou:

1. Selecione cada usuário que indica *(Falha na clonagem)* abaixo do nome do 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 locatários 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 sua conta de locatário tiver a permissão **Usar conexão de federação de grade** e você excluir um usuário local, o StorageGRID não excluirá o usuário correspondente na outra grade. Se você precisar manter essas informações sincronizadas, deverá excluir o mesmo usuário de ambas as grades.

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

Passos

1. Selecione **GERENCIAMENTO DE ACESSO** > **Usuários**.
2. Marque 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

Gerenciar chaves de acesso S3

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

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

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

O StorageGRID suporta autenticação Signature versão 2 e Signature versão 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

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Gerencie suas próprias credenciais S3 ou permissão de acesso Root" .

Sobre esta tarefa

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

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

- Defina um tempo de expiração para suas chaves para limitar seu acesso a um determinado período de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco caso seu ID de chave de acesso e sua chave de acesso secreta sejam acidentalmente expostos. Chaves expiradas são removidas automaticamente.
- Se o risco de segurança no seu ambiente for baixo e você não precisar criar novas chaves periodicamente, não será necessário definir um tempo de expiração para suas chaves. Se você decidir criar novas chaves posteriormente, 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 exibidas para sua conta no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com 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 **ARMAZENAMENTO (S3)** > **Minhas chaves de acesso**.

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

2. Selecione **Criar chave**.
3. Faça um dos seguintes:
   - Selecione **Não definir um tempo de expiração** para criar uma chave que não irá expirar. (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 expiração pode ser de no mínimo um minuto a partir da hora atual.

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

A caixa de diálogo Baixar chave de acesso é exibida, listando seu ID de chave de acesso e sua 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 ter copiado ou baixado estas informações. Não é possível copiar ou baixar chaves depois que a caixa de diálogo for fechada.

6. Selecione **Concluir**.

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

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

Visualize suas chaves de acesso S3

Se você estiver usando um locatário S3 e tiver o"permissão apropriada" , você pode visualizar uma lista de suas chaves de acesso S3. Você pode classificar a lista por tempo de expiração para determinar quais chaves expirarão em breve. Conforme necessário, você pode"criar novas chaves" ou"teclas de exclusão" que você não está mais usando.

> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidas para sua conta no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com 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 Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que possui o recurso Gerenciar suas próprias credenciais do S3"permissão" .

Passos

1. Selecione **ARMAZENAMENTO (S3)** > **Minhas chaves de acesso**.
2. Na página Minhas chaves de acesso, classifique todas as chaves de acesso existentes por **Tempo de expiração** ou **ID da chave de acesso**.
3. Conforme necessário, crie novas chaves ou exclua aquelas que você não estiver mais usando.

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

   Chaves expiradas são removidas automaticamente.

Exclua suas próprias chaves de acesso S3

Se você estiver usando um locatário S3 e tiver a permissão apropriada, poderá excluir suas próprias chaves de acesso S3. Depois que uma chave de acesso é excluída, ela

não pode mais ser usada para acessar os objetos e buckets na conta do locatário.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você tem o"Permissão para gerenciar suas próprias credenciais do S3" .

> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidas para sua conta no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com 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 **ARMAZENAMENTO (S3)** > **Minhas chaves de acesso**.
2. Na página Minhas chaves de acesso, marque a caixa de seleção de cada chave de acesso que deseja remover.
3. Selecione **tecla Delete**.
4. Na caixa de diálogo de confirmação, selecione **Tecla Delete**.

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

Crie chaves de acesso S3 de outro usuário

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem 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 suas contas de locatário. Depois de criar uma nova chave de acesso, atualize o aplicativo com o novo ID da chave de acesso e a nova chave de acesso secreta. 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 chave antes que a antiga expire e, em seguida, exclua-a.

Cada chave pode ter um tempo de expiração específico ou não ter 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 de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco se o ID da chave de acesso e a chave de acesso secreta forem expostos acidentalmente. Chaves expiradas são removidas automaticamente.
- Se o risco de segurança no seu ambiente for baixo e você não precisar criar novas chaves periodicamente, não será necessário definir um tempo de expiração para as chaves. Se você decidir criar novas chaves posteriormente, 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 exibidas para esse usuário no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com 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 S3 você deseja gerenciar.

   A página de detalhes do usuário é exibida.

3. Selecione **Teclas de acesso** e depois selecione **Criar chave**.
4. Faça um dos seguintes:
   - 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 expiração pode ser de no mínimo um minuto a partir da hora 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 ter copiado ou baixado estas informações. Não é possível copiar ou baixar chaves depois que a caixa de diálogo for fechada.

7. Selecione **Concluir**.

   A nova chave é listada na guia Chaves de acesso da página de detalhes do usuário.

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

Ver as chaves de acesso S3 de outro usuário

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da 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 exibidas para esse usuário no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com 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 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 estão 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.

   Chaves expiradas são removidas automaticamente.

Informações relacionadas

- "Crie chaves de acesso S3 de outro usuário"
- "Excluir chaves de acesso S3 de outro usuário"

Excluir chaves de acesso S3 de outro usuário

Se você estiver usando um locatário S3 e tiver permissões apropriadas, poderá excluir as chaves de acesso 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 locatário.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da 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 exibidas para esse usuário no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com 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 S3 você deseja gerenciar.
3. Na página Detalhes do usuário, selecione **Chaves de acesso** e marque a caixa de seleção de cada chave de acesso que deseja excluir.
4. Selecione **Ações** > **Excluir chave selecionada**.
5. Na caixa de diálogo de confirmação, selecione **Tecla Delete**.

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

Gerenciar buckets S3

Criar um bucket S3

Você pode usar o Tenant Manager para criar buckets do S3 para dados de objetos.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem acesso Root ou Gerenciar todos os buckets"permissão" . Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

> Permissões para definir ou modificar propriedades de bloqueio de objeto 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 de grade habilitou a configuração global S3 Object Lock para o sistema StorageGRID , e você revisou os requisitos para buckets e objetos do S3 Object Lock.
- Se cada locatário tiver 5.000 buckets, cada nó de armazenamento na grade terá no mínimo 64 GB de RAM.

> Cada grade pode ter no máximo 100.000 buckets.

Acesse o assistente

Passos

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

Insira os detalhes

Passos

1. Insira detalhes do bucket.

Campo	Descrição
Nome do balde	Um nome para o bucket que esteja em conformidade com estas regras: • Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário). • Deve ser compatível com DNS. • Deve conter no mínimo 3 e no máximo 63 caracteres. • Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hifens. • Não deve conter pontos em solicitações de estilo de hospedagem virtual. Os períodos causarão problemas com a verificação do certificado curinga do servidor. Para mais informações, consulte o "Documentação da Amazon Web Services (AWS) sobre regras de nomenclatura de buckets" . **Observação**: você não pode alterar o nome do bucket depois de criá-lo.
Região	A região do balde. 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 no `us-east-1` região. **Observação**: você não pode alterar a região depois de criar o bucket.

2. Selecione **Continuar**.

Gerenciar configurações

Passos

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

   Habilite o controle de versão de objetos se quiser armazenar todas as versões de cada objeto neste bucket. Você pode então recuperar versões anteriores de um objeto conforme necessário. Você deve habilitar o controle de versão de objetos se o bucket for usado para replicação entre grades.

2. Se a configuração global do S3 Object Lock estiver habilitada, opcionalmente habilite o S3 Object Lock para que o bucket armazene objetos usando um modelo WORM (gravar uma vez e ler várias vezes).

   Habilite o Bloqueio de Objetos S3 para um bucket somente se você precisar manter objetos por um período fixo de tempo, por exemplo, para atender a determinados requisitos regulatórios. O Bloqueio de Objetos do S3 é uma configuração permanente que ajuda a evitar que objetos sejam excluídos ou substituídos por um período fixo de tempo ou indefinidamente.

   Depois que a configuração de bloqueio de objeto do S3 é habilitada para um bucket, ela não pode ser desabilitada. Qualquer pessoa com as permissões corretas pode adicionar objetos a este bucket que não podem ser alterados. Talvez você não consiga excluir esses objetos ou o próprio bucket.

Se você habilitar o S3 Object Lock para um bucket, o controle de versão do bucket será habilitado automaticamente.

3. Se você selecionou **Ativar bloqueio de objeto S3**, opcionalmente ative **Retenção padrão** para este bucket.

   O administrador da sua rede deve dar-lhe permissão para"usar recursos específicos do S3 Object Lock" .

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

   a. Se **Retenção padrão** estiver habilitado, especifique um **Modo de retenção padrão** para o bucket.

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

   b. Se **Retenção padrão** estiver habilitado, especifique o **Período de retenção padrão** para o bucket.

      O **Período de retenção padrão** indica por quanto tempo 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 do locatário, conforme definido pelo administrador da grade.

   Um período de retenção *máximo*, que pode ser um valor de 1 dia a 100 anos, é definido quando o administrador da grade cria o locatário. Quando você define um período de retenção *padrão*, ele não pode exceder o valor definido para o período máximo de retenção. Se necessário, peça ao administrador da sua rede para aumentar ou diminuir o período máximo de retenção.

4. Opcionalmente, selecione **Ativar limite 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 no disco).

Se nenhum limite for definido, a capacidade deste bucket será ilimitada. Consulte "Limite de utilização da capacidade" para maiores informações.

5. Selecione **Criar bucket**.

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

6. Opcionalmente, selecione **Ir para a página de detalhes do bucket** para"ver detalhes do bucket" e executar configurações adicionais.

Ver detalhes do bucket

Você pode visualizar os buckets na sua conta de locatário.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Permissão de acesso root, gerenciar todos os buckets ou visualizar todos os buckets" . Essas permissões substituem as configurações de permissão em políticas de grupo ou bucket.

Passos

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

   A página Buckets é exibida.

2. Revise a tabela de resumo para cada bucket.

   Conforme necessário, você pode classificar as informações por qualquer coluna ou pode avançar e voltar na lista.

   > Os valores de Contagem de Objetos, Espaço Usado e Uso exibidos são estimativas. Essas estimativas são afetadas pelo tempo de ingestão, pela conectividade de rede e pelo status do nó. Se os buckets tiverem o controle de versão habilitado, as versões de objetos excluídas serão incluídas na contagem de objetos.

   Nome
   Nome exclusivo do bucket, que não pode ser alterado.

   Recursos habilitados
   A lista de recursos habilitados para o bucket.

   Bloqueio de Objeto S3
   Se o bloqueio de objeto S3 está habilitado para o bucket.

   Esta coluna aparece somente se o Bloqueio de Objeto S3 estiver habilitado para a grade. Esta coluna também mostra informações para quaisquer buckets compatíveis legados.

   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 os buckets tiverem o controle de versão habilitado, versões de

objetos não atuais serão 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 codificadas para eliminação ou para metadados de objetos.

Este valor pode levar até 10 minutos para ser atualizado.

Uso

A porcentagem utilizada do limite de capacidade do bucket, se um tiver sido definido.

O valor de uso é baseado em estimativas internas e pode ser excedido em alguns casos. Por exemplo, o StorageGRID verifica o limite de capacidade (se definido) quando um locatário começa a carregar objetos e rejeita novas ingestões para esse bucket se o locatário tiver excedido o limite de capacidade. No entanto, o StorageGRID não leva em consideração o tamanho do upload atual ao determinar se o limite de capacidade foi excedido. Se os objetos forem excluídos, um locatário poderá ser temporariamente impedido de carregar novos objetos neste 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

Data e hora em que o bucket foi criado. Esta coluna está oculta por padrão.

3. Para visualizar detalhes de um bucket específico, selecione o nome do bucket na tabela.
   a. Veja as informações resumidas na parte superior da página da web para confirmar os detalhes do bucket, como região e contagem de objetos.
   b. Veja a barra de uso do limite de capacidade. Se o uso for de 100% ou próximo de 100%, considere aumentar o limite ou excluir alguns objetos.
   c. Conforme necessário, selecione **Excluir objetos no bucket** e **Excluir bucket**.

> Preste muita atenção aos avisos que aparecem quando você seleciona cada uma dessas opções. Para mais informações, consulte:
>
> - "Excluir todos os objetos em um bucket"
> - "Excluir um bucket"(o balde deve estar vazio)

   d. Visualize ou altere as configurações do bucket em cada uma das guias, conforme necessário.
      - **Console S3**: visualize os objetos do bucket. Para mais informações, consulte "Usar o console S3" .
      - **Opções de bucket**: visualize ou altere as configurações de opções. Algumas configurações, como o S3 Object Lock, não podem ser alteradas após a criação do bucket.
        - "Gerenciar consistência de bucket"
        - "Últimas atualizações de tempo de acesso"

        - "Limite de capacidade"
        - "Controle de versão de objetos"
        - "Bloqueio de Objeto S3"
        - "Retenção de bucket padrão"
        - "Gerenciar replicação entre redes"(se permitido para o inquilino)
    - **Serviços de plataforma**:"Gerenciar serviços de plataforma" (se permitido para o inquilino)
    - **Acesso ao bucket**: visualize ou altere as configurações de opções. Você deve ter permissões de acesso específicas.
        - Configurar"Compartilhamento de Recursos de Origem Cruzada (CORS)" para que o bucket e os objetos no bucket sejam acessíveis a aplicativos web em outros domínios.
        - "Controlar o acesso do usuário"para um bucket S3 e objetos nesse bucket.

Aplicar uma tag de política ILM a um bucket

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

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

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Permissão de acesso root, gerenciar todos os buckets ou visualizar todos os buckets" . Essas permissões substituem as configurações de permissão em políticas de grupo ou bucket.

Passos

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

   A página Buckets é exibida. Conforme necessário, você pode classificar as informações por qualquer coluna ou pode avançar e voltar na lista.

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

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

   > Os valores de Contagem de Objetos e Espaço Usado exibidos são estimativas. Essas estimativas são afetadas pelo tempo de ingestão, pela conectividade de rede e pelo status do nó. Se os buckets tiverem o controle de versão habilitado, as versões de objetos excluídas serão incluídas na contagem de objetos.

3. Na guia Opções de bucket, expanda o acordeão de tags de política do ILM. Este acordeão só aparece se o administrador da grade tiver habilitado o uso de tags de política personalizadas.

4. Leia a descrição de cada tag de política para determinar qual tag deve ser aplicada ao bucket.

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

5. Selecione o botão de opção para a 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 de política do ILM.

> Certifique-se de que seus aplicativos S3 não substituam ou excluam acidentalmente a nova tag de bucket. Se esta tag for omitida ao aplicar um novo TagSet ao bucket, os objetos no bucket voltarão a ser avaliados em relação à política ILM padrão.

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

> Alterar a tag de política atribuída a um bucket tem um impacto temporário no desempenho enquanto os objetos estão sendo reavaliados usando a nova política do ILM.

Gerenciar política de bucket

Você pode controlar o acesso do usuário a um bucket do S3 e aos objetos nesse bucket.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Permissão de acesso root" . As permissões Exibir todos os buckets e Gerenciar todos os buckets permitem apenas a visualização.
- Você verificou se o número necessário de nós de armazenamento e sites está disponível. Se dois ou mais nós de armazenamento não estiverem disponíveis em nenhum site, ou se um site não estiver disponível, as alterações nessas configurações poderão 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:
   - Insira uma política de bucket marcando 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 sequência de caracteres.
   - Desabilite uma política desmarcando **Habilitar política**.

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

Gerenciar consistência de bucket

Os valores de consistência podem ser usados para especificar a disponibilidade de alterações nas configurações do bucket, bem como para fornecer um equilíbrio entre a disponibilidade dos objetos dentro de um bucket e a consistência desses objetos em diferentes nós de armazenamento e sites. Você pode alterar os valores de consistência para que sejam diferentes dos valores padrão para que os aplicativos clientes possam atender às suas necessidades operacionais.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Gerenciar todos os buckets ou permissão de acesso root" . Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

Diretrizes de consistência de bucket

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

Alterar consistência do bucket

Se a consistência **Leitura após nova gravação** não atender aos requisitos do aplicativo cliente, você poderá alterar a consistência definindo a consistência do bucket ou usando o `Consistency-Control` cabeçalho. O `Consistency-Control` O cabeçalho substitui a consistência do bucket.

> Quando você altera a consistência de um bucket, somente os objetos ingeridos após a alteração têm a garantia de atender à configuração revisada.

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (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 operações executadas nos objetos neste 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 de clientes em todos os sites.
   - **Strong-site**: Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.
   - **Leitura após nova gravação** (padrão): fornece consistência de leitura após gravação para novos objetos e consistência eventual para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
   - **Disponível**: Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que raramente são lidos ou para operações HEAD ou GET em chaves que não existem). Não

suportado para buckets do S3 FabricPool .

5. Selecione **Salvar alterações**.

O que acontece quando você altera as configurações do bucket

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

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

- "Exclusão de bucket vazio em segundo plano"
- "Último horário de acesso"
- "Ciclo de vida do bucket"
- "Política de balde"
- "Etiquetagem de balde"
- "Controle de versão de bucket"
- "Bloqueio de Objeto S3"
- "Criptografia de bucket"

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

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

- "Configuração de serviços de plataforma: integração de notificação, replicação ou pesquisa"
- "Configuração CORS"
- Alterar consistência do bucket

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

Habilitar ou desabilitar atualizações do último horário de acesso

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

Estas instruções se aplicam somente a sistemas StorageGRID que incluem pelo menos uma regra ILM que usa a opção **Último horário de acesso** como um filtro avançado ou como um horário de referência. Você pode ignorar essas instruções se o seu sistema StorageGRID não incluir essa regra. Ver"Usar a hora do último acesso nas regras do ILM" para mais detalhes.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Gerenciar todos os buckets ou permissão de acesso root" . Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

Sobre esta tarefa

Último horário de acesso é uma das opções disponíveis para a instrução de posicionamento **Horário de referência** para uma regra ILM. Definir o Tempo de referência para uma regra como Hora do último acesso permite que os administradores da grade 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 objetos visualizados recentemente permaneçam em um armazenamento mais rápido, um administrador de grade pode criar uma regra ILM especificando o seguinte:

- Objetos recuperados no mês passado devem permanecer nos nós de armazenamento locais.
- Objetos que não foram recuperados no último mês devem ser movidos para um local externo.

Por padrão, as atualizações do último horário de acesso são desabilitadas. Se o seu sistema StorageGRID incluir uma regra ILM que usa a opção **Último horário de acesso** e você quiser que essa opção se aplique a objetos neste bucket, você deverá habilitar atualizações para o último horário de acesso para os buckets do S3 especificados nessa regra.

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

Um impacto no desempenho ocorre com as atualizações do último horário de acesso porque o StorageGRID deve executar estas etapas adicionais sempre que os objetos são recuperados:

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

A tabela resume o comportamento aplicado a todos os objetos no bucket quando o último horário de acesso é desabilitado ou habilitado.

Tipo de solicitação	Comportamento se o último horário de acesso estiver desabilitado (padrão)		Comportamento se o último horário de acesso estiver habilitado	
	Último horário de acesso atualizado?	Objeto adicionado à fila de avaliação do ILM?	Último horário de acesso atualizado?	Objeto adicionado à fila de avaliação do ILM?
Solicitação para recuperar um objeto, sua lista de controle de acesso ou seus metadados	Não	Não	Sim	Sim

Solicitação para atualizar os metadados de um objeto	Sim	Sim	Sim	Sim
Solicitação para listar objetos ou versões de objetos	Não	Não	Não	Não
Solicitação para copiar um objeto de um bucket para outro	• Não, para a cópia de origem • Sim, para a cópia de destino	• Não, para a cópia de origem • 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 multiparte	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 **ARMAZENAMENTO (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 **Atualizações de hora do último acesso**.
4. Habilitar ou desabilitar atualizações de horário do último acesso.
5. Selecione **Salvar alterações**.

Alterar o controle de versão do objeto para um bucket

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Gerenciar todos os buckets ou permissão de acesso root" . Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Você verificou se o número necessário de nós de armazenamento e sites está disponível. Se dois ou mais nós de armazenamento não estiverem disponíveis em nenhum site, ou se um site não estiver disponível, as alterações nessas configurações poderão não estar disponíveis.

Sobre esta tarefa

Você pode habilitar ou suspender o controle de versão de objetos para um bucket. Depois de habilitar o controle de versão para um bucket, ele não poderá retornar a um estado sem versão. No entanto, você pode suspender o controle de versão do bucket.

- Desativado: o controle de versão nunca foi habilitado

- Habilitado: o controle de versão está habilitado
- Suspenso: o controle de versão foi habilitado anteriormente e está suspenso

Para mais informações, consulte o seguinte:

- "Controle de versão 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 **ARMAZENAMENTO (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 do objeto**.
4. Selecione um estado de controle de versão para os objetos neste bucket.

   O controle de versão de objetos deve permanecer habilitado para um bucket usado para replicação entre grades. Se o bloqueio de objeto S3 ou a conformidade com o legado estiver habilitado, as opções de **Controle de versão do objeto** serão desabilitadas.

Opção	Descrição
Habilitar controle de versão	Habilite o controle de versão de objetos se quiser armazenar todas as versões de cada objeto neste bucket. Você pode então recuperar versões anteriores de um objeto conforme necessário. Objetos que já estavam no bucket serão versionados quando forem modificados por um usuário.
Suspender o controle de versão	Suspenda o controle de versão do objeto se não quiser mais que novas versões do objeto sejam criadas. Você ainda pode recuperar qualquer versão de objeto existente.

5. Selecione **Salvar alterações**.

Use o S3 Object Lock para reter objetos

Você pode usar o S3 Object Lock se os buckets e objetos precisarem estar em conformidade com os requisitos regulatórios de retenção.

> O administrador da grade deve lhe dar permissão para usar recursos específicos do S3 Object Lock.

O que é o S3 Object Lock?

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

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

Um bucket sem bloqueio de objeto S3 só pode ter objetos sem configurações de retenção especificadas. Nenhum objeto ingerido terá configurações de retenção.

Um bucket com bloqueio de objeto S3 pode ter objetos com e sem configurações de retenção especificadas por aplicativos cliente S3. Alguns objetos ingeridos terão configurações de retenção.

Um bucket com bloqueio de objeto S3 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, porque a configuração de retenção não foi configurada no nível do objeto.

Efetivamente, todos os objetos recém-ingeridos têm configurações de retenção quando a retenção padrão é configurada. Objetos existentes sem configurações de retenção de objetos 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 data de retenção seja atingida.
  - A data de retenção do objeto pode ser aumentada, mas não diminuída.
  - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- No 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 do objeto antes que sua data de retenção seja atingida.
  - Esses usuários podem aumentar, diminuir ou remover a data de retenção de um objeto.

Configurações de retenção para versões de objeto

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

- **Modo de retenção**: conformidade ou governança.
- **Reter-até-data**: Se a data de retenção de uma versão do objeto for no futuro, o objeto poderá ser recuperado, mas não poderá ser excluído.
- **Retenção legal**: Aplicar uma retenção legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar reter legalmente um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até ser explicitamente removida. As retenções legais são independentes da retenção até a data.

  > ⓘ Se um objeto estiver sob retenção legal, ninguém poderá excluí-lo, independentemente do seu modo de retenção.

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

bloqueio de objeto do S3" .

Configuração de retenção padrão para buckets

Se um bucket for criado com o S3 Object Lock habilitado, os usuários poderão, opcionalmente, especificar as seguintes configurações padrão para o bucket:

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

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

Ver"Criar um bucket S3" e"Atualizar retenção padrão do bloqueio de objeto S3" .

Tarefas de bloqueio de objeto S3

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

Administrador de rede

- Habilitar a configuração global de bloqueio de objeto S3 para todo o sistema StorageGRID .
- Garantir que as políticas de gestão do ciclo de vida da informação (ILM) sejam *compatíveis*; ou seja, que atendam aos"requisitos de buckets com bloqueio de objeto S3 habilitado" .
- Conforme necessário, permita que um locatário use Conformidade como modo de retenção. Caso contrário, somente o modo Governança é permitido.
- Conforme necessário, defina um período máximo de retenção para um locatário.

Usuário locatário

- Revise as considerações para buckets e objetos com o S3 Object Lock.
- Conforme necessário, entre em contato com o administrador da grade para habilitar a configuração global de bloqueio de objeto do S3 e definir permissões.
- Crie buckets com o S3 Object Lock habilitado.
- Opcionalmente, configure as definições de retenção padrão para um bucket:
  - Modo de retenção padrão: Governança ou Conformidade, se permitido pelo administrador da rede.
  - Período de retenção padrão: deve ser menor ou igual ao período máximo de retenção 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 rede.
  - Data de retenção: deve ser menor ou igual ao que é permitido pelo período máximo de retenção definido pelo administrador da grade.

Requisitos para buckets com bloqueio de objeto S3 habilitado

- Se a configuração global do S3 Object Lock estiver habilitada para o sistema StorageGRID , você poderá usar o Tenant Manager, a Tenant Management API ou a S3 REST API para criar buckets com o S3 Object

Lock habilitado.

- Se você planeja usar o S3 Object Lock, deverá habilitar o S3 Object Lock ao criar o bucket. Não é possível habilitar o S3 Object Lock para um bucket existente.
- Quando o S3 Object Lock é habilitado para um bucket, o StorageGRID habilita automaticamente o controle de versão para esse bucket. Não é possível desabilitar o bloqueio de objeto do S3 ou suspender o controle de versão do 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 retenção até a data para cada versão do objeto quando ele for carregado.
- A configuração do ciclo de vida do bucket é suportada para buckets com o S3 Object Lock habilitado.
- A replicação do CloudMirror não é suportada para buckets com S3 Object Lock habilitado.

Requisitos para objetos em buckets com bloqueio de objeto S3 habilitado

- Para proteger uma versão do objeto, você pode especificar configurações de retenção padrão para o bucket ou especificar configurações de retenção para cada versão do objeto. As configurações de retenção no nível do objeto podem ser especificadas usando o aplicativo cliente S3 ou a API REST do S3.
- As configurações de retenção se aplicam a versões de objetos individuais. Uma versão de objeto pode ter uma configuração de retenção até a data e uma configuração de retenção legal, uma mas não a outra, ou nenhuma delas. Especificar uma configuração de retenção até a data ou de retenção legal para um objeto protege apenas a versão especificada na solicitação. Você pode criar novas versões do objeto, enquanto a versão anterior do objeto permanece bloqueada.

Ciclo de vida de objetos em buckets com bloqueio de objeto S3 habilitado

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

1. **Ingestão de objetos**

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

   - Se as configurações de retenção forem especificadas para o objeto, as configurações no nível do objeto serão aplicadas. Todas as configurações de bucket padrão são ignoradas.
   - Se nenhuma configuração de retenção for especificada para o objeto, as configurações de bucket padrão serão aplicadas, se existirem.
   - Se nenhuma configuração de retenção for especificada para o objeto ou o bucket, o objeto não será protegido pelo S3 Object Lock.

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

2. **Retenção e exclusão de objetos**

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

   - Se um objeto estiver sob retenção legal, ninguém poderá excluí-lo, independentemente do seu modo

de retenção.

Ainda posso gerenciar buckets compatíveis legados?

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, poderá continuar a gerenciar as configurações desses buckets; no entanto, não poderá mais criar novos buckets compatíveis. Para obter instruções, consultehttps://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"^] .

Atualizar retenção padrão do bloqueio de objeto S3

Se você habilitou o Bloqueio de Objeto S3 ao criar o bucket, poderá editá-lo para alterar as configurações de retenção padrão. Você pode habilitar (ou desabilitar) a retenção padrão e definir um modo e um período de retenção padrão.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Gerenciar todos os buckets ou permissão de acesso root" . Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- O S3 Object Lock está habilitado globalmente para seu sistema StorageGRID , e você habilitou o S3 Object Lock quando criou o bucket. Ver "Use o S3 Object Lock para reter objetos" .

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (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 nessa configuração não se aplicam a objetos que já estão no bucket ou a quaisquer objetos que possam ter seus próprios períodos de retenção.

5. Se **Retenção padrão** estiver habilitado, especifique um **Modo de retenção padrão** para o bucket.

Modo de retenção padrão	Descrição
Governança	• Usuários com o `s3:BypassGovernanceRetention` permissão pode usar o `x-amz-bypass-governance-retention: true` cabeçalho de solicitação para ignorar as configurações de retenção. • Esses usuários podem excluir uma versão do objeto antes que sua data de retenção seja atingida. • Esses usuários podem aumentar, diminuir ou remover a data de retenção de um objeto.

Modo de retenção padrão	Descrição
Conformidade	• O objeto não pode ser excluído até que sua data de retenção seja atingida. • A data de retenção do objeto pode ser aumentada, mas não diminuída. • A data de retenção do objeto não pode ser removida até que essa data seja atingida. **Observação**: o administrador da sua rede deve permitir que você use o modo de conformidade.

6. Se **Retenção padrão** estiver habilitado, especifique o **Período de retenção padrão** para o bucket.

   O **Período de retenção padrão** indica por quanto tempo 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 do locatário, conforme definido pelo administrador da grade.

   Um período de retenção *máximo*, que pode ser um valor de 1 dia a 100 anos, é definido quando o administrador da grade cria o locatário. Quando você define um período de retenção *padrão*, ele não pode exceder o valor definido para o período máximo de retenção. Se necessário, peça ao administrador da sua rede para aumentar ou diminuir o período máximo de retenção.

7. Selecione **Salvar alterações**.

Configurar compartilhamento de recursos de origem cruzada (CORS)

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Para solicitações de configuração GET CORS, você pertence a um grupo de usuários que tem o"Permissão para gerenciar todos os buckets ou visualizar todos os buckets" . Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Para solicitações de configuração PUT CORS, você pertence a um grupo de usuários que tem o"Permissão para gerenciar todos os buckets" . Esta permissão substitui as configurações de permissões em políticas de grupo ou bucket.
- O"Permissão de acesso root" fornece acesso a todas as solicitações de configuração do CORS.

Sobre esta tarefa

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

Habilitar CORS para um bucket

Passos

1. Use um editor de texto para criar o XML necessário. Este exemplo mostra o XML usado para habilitar o CORS para um bucket S3. Especificamente:
   - Permite que qualquer domínio envie solicitações GET para o bucket
   - Permite apenas o `http://www.example.com` domínio para enviar 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 do CORS, consulte "Documentação da Amazon Web Services (AWS): Guia do usuário do Amazon Simple Storage Service" .

2. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (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 entre origens (CORS)**.
5. Marque a caixa de seleção **Ativar CORS**.
6. Cole o XML de configuração do CORS na caixa de texto.
7. Selecione **Salvar alterações**.

Modificar configuração CORS

Passos

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

Desabilitar configuração CORS

Passos

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

Excluir objetos no bucket

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

Considerações e requisitos

Antes de executar essas etapas, observe o seguinte:

- Quando você exclui os objetos em um bucket, o StorageGRID remove permanentemente todos os objetos e todas as versões de objetos em cada bucket selecionado de todos os nós e sites no seu sistema StorageGRID . O StorageGRID também remove quaisquer metadados de objetos relacionados. Você não poderá recuperar essas informações.
- A exclusão de 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 balde tiver"Bloqueio de objeto S3 habilitado" , ele pode permanecer no estado **Excluindo objetos: somente leitura** por *anos*.

> Um bucket que usa 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 retenções legais sejam removidas.

- 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 no estado somente leitura. Você pode fazer um dos seguintes:
  - Retorne o bucket ao modo de gravação e reutilize-o para novos objetos
  - Excluir o balde
  - Mantenha o bucket no modo somente leitura para reservar seu nome para uso futuro
- Se um bucket tiver o controle de versão de objeto habilitado, os marcadores de exclusão que foram criados no StorageGRID 11.8 ou posterior poderão ser removidos usando Excluir objetos nas operações do bucket.
- Se um bucket tiver o controle de versão de objeto habilitado, a operação de exclusão de objetos não removerá os marcadores de exclusão que foram criados no StorageGRID 11.7 ou anterior. Veja informações sobre como excluir objetos em um bucket em"Como objetos versionados do S3 são excluídos" .
- Se você usar"replicação entre grades" , observe o seguinte:
  - Usar esta opção não exclui nenhum objeto do bucket na outra grade.
  - Se você selecionar esta opção para o bucket de origem, o alerta **Falha de replicação entre grades** será acionado se você adicionar objetos ao bucket de destino na outra grade. Se você não puder garantir que ninguém adicionará objetos ao bucket na outra grade,"desabilitar replicação entre redes" para esse bucket antes de excluir todos os objetos do bucket.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Permissão de acesso root" . Esta permissão substitui as configurações de permissões em políticas de grupo ou bucket.

Passos

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

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

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

   Menu de ações

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

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

   Página de detalhes

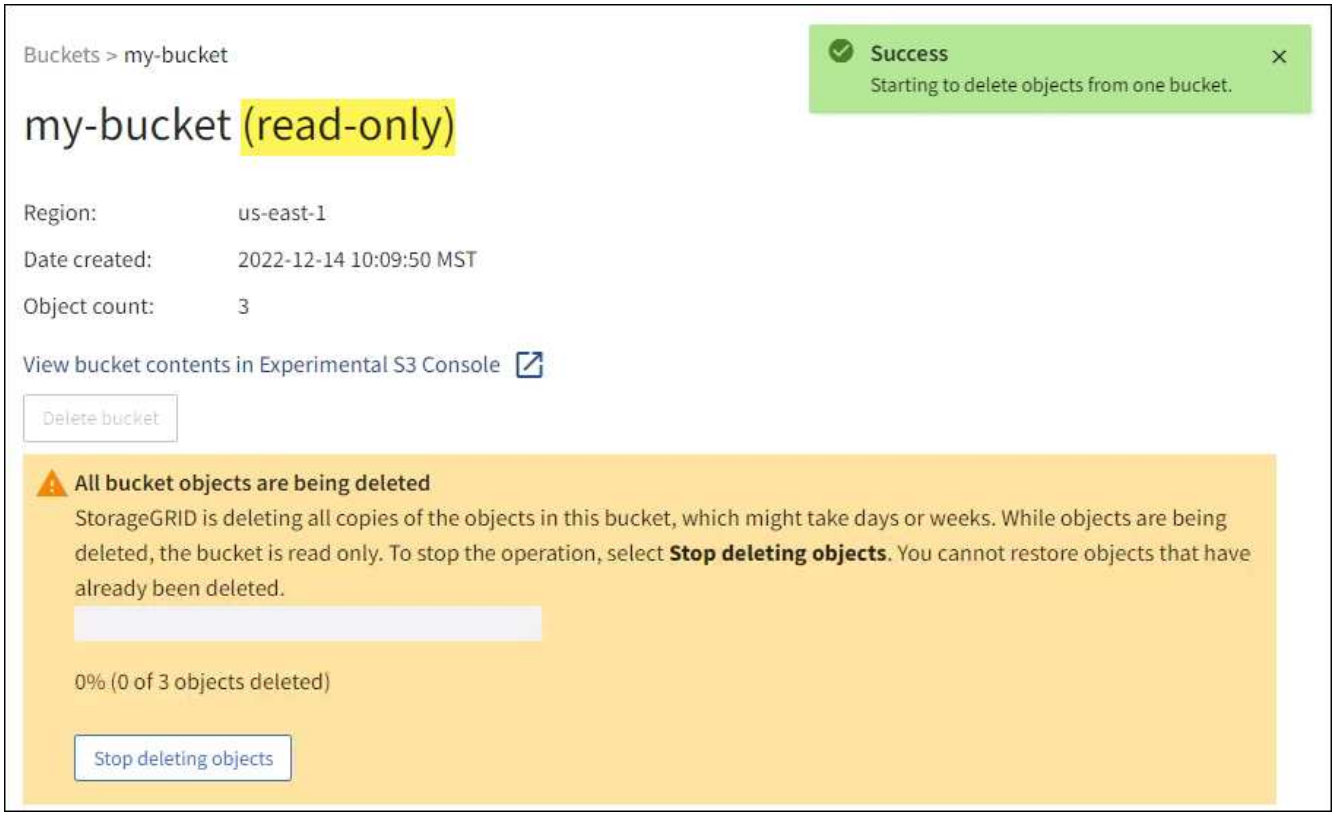
   a. Selecione um nome de bucket para exibir seus detalhes.

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

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

   Depois de alguns minutos:

   - Um banner de status amarelo aparece na página de detalhes do bucket. A barra de progresso representa a porcentagem de objetos que foram excluídos.
   - **(somente leitura)** aparece após o nome do bucket na página de detalhes do bucket.
   - **(Excluindo objetos: somente leitura)** aparece ao lado do nome do bucket na página Buckets.

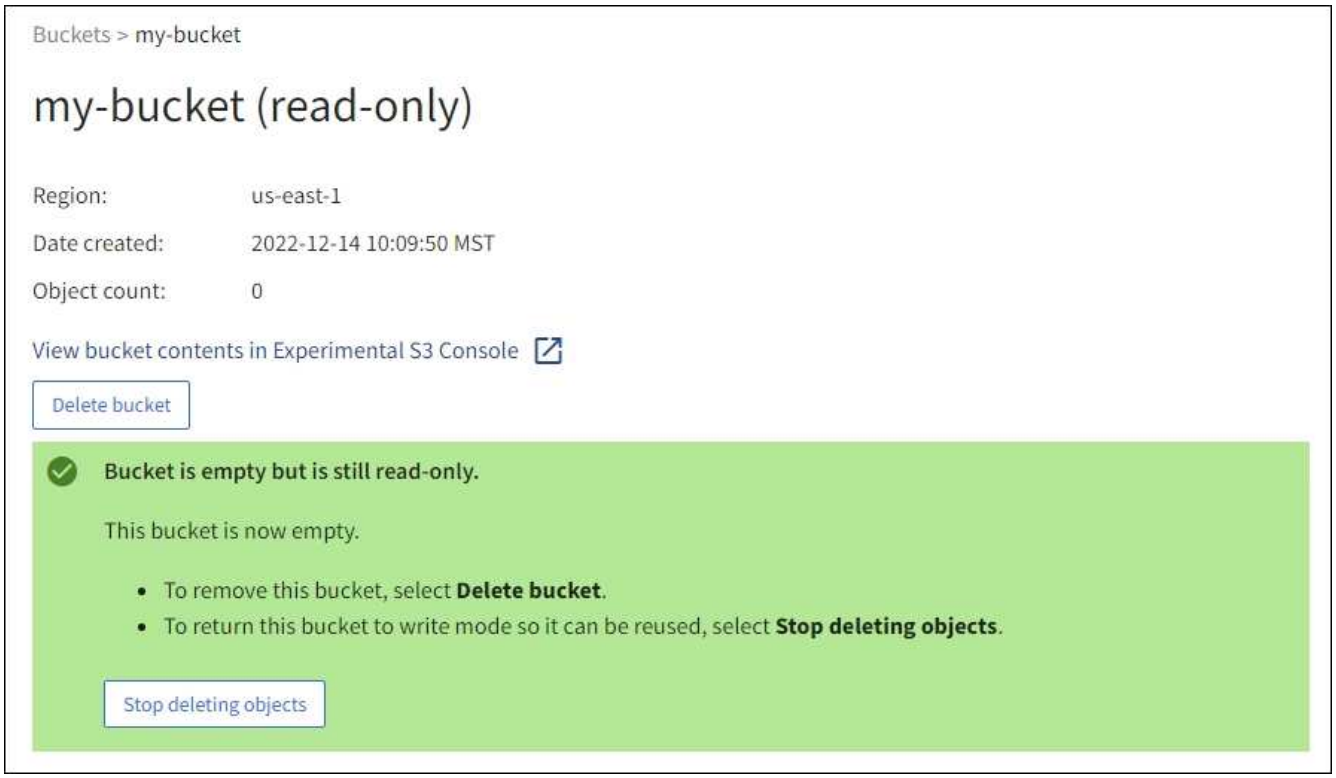


5. Conforme necessário enquanto a operação estiver em execução, selecione **Parar de excluir objetos** para interromper o processo. Em seguida, opcionalmente, selecione **Excluir objetos no bucket** para retomar o processo.

   Quando você seleciona **Parar de excluir objetos**, o bucket 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 está vazio, o banner de status é atualizado, mas o bucket permanece somente leitura.



7. Faça um dos seguintes:
   - Saia da página para manter o bucket no modo somente leitura. Por exemplo, você pode manter um bucket vazio no 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 depois que todos os objetos forem excluídos, os marcadores de exclusão poderão 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 bucket S3

Você pode usar o Gerenciador de Tenants para excluir um ou mais buckets do S3 que estão vazios.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Gerenciar todos os buckets ou permissão de acesso root" . Essas permissões substituem as configurações de permissões em 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 S3 usando o Gerenciador de Tenants. Você também

pode excluir buckets S3 usando o"API de gerenciamento de inquilinos" ou o"API REST S3" .

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 **ARMAZENAMENTO (S3)** > **Buckets**.

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

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

   Menu de ações

   a. Marque a caixa de seleção de cada bucket que você deseja excluir.

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

   Página de detalhes

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

   b. Selecione **Excluir bucket**.

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

   O StorageGRID confirma que cada bucket está vazio e então exclui cada bucket. Esta 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 excluir o bucket.

Usar o console S3

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

O console S3 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 objetos
- 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 operações de CLI ou API em todas as situações.

Se o uso do Console S3 fizer com que as operações demorem muito (por exemplo, minutos ou horas), considere:

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Se você quiser gerenciar objetos, pertença a um grupo de usuários que tenha permissão de acesso Root. Como alternativa, você pertence a um grupo de usuários que tem a permissão Usar a guia Console do S3 e a permissão Exibir todos os buckets ou Gerenciar todos os buckets. Ver "Permissões de gerenciamento de inquilinos" .
- Uma política de grupo ou bucket S3 foi configurada para o usuário. Ver "Use políticas de acesso a buckets e grupos" .
- Você sabe 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 **ARMAZENAMENTO** > **Buckets** > ***nome do bucket***.
2. Selecione a aba Console S3.
3. Cole o ID da chave de acesso e a chave de acesso secreta nos campos. Caso contrário, selecione **Carregar chaves de acesso** e selecione seu `.csv` arquivo.
4. Selecione * Sign in*.
5. A tabela de objetos de bucket é exibida. Você pode gerenciar objetos conforme necessário.

Informações adicionais

- **Pesquisar por prefixo**: O recurso de pesquisa por prefixo pesquisa apenas objetos que começam com uma palavra específica relativa à pasta atual. A pesquisa não inclui objetos que contenham a palavra em outro lugar. Esta regra também se aplica a objetos dentro de pastas. Por exemplo, uma busca por `folder1/folder2/somefile-` retornaria objetos que estão dentro do `folder1/folder2/` pasta e comece com a palavra `somefile-` .
- **Arrastar e soltar**: Você pode arrastar e soltar arquivos do gerenciador de arquivos do seu computador para o Console S3. Entretanto, você não pode carregar pastas.
- **Operações em pastas**: Quando você move, copia ou renomeia uma pasta, todos os objetos na pasta são atualizados um de cada vez, o que pode levar algum tempo.
- **Exclusão permanente quando o controle de versão do bucket está desabilitado**: quando você substitui ou exclui um objeto em um bucket com o controle de versão desabilitado, a operação é permanente. Ver "Alterar o controle de versão do objeto para um bucket" .

Gerenciar serviços da plataforma S3

Serviços da plataforma S3

Antes de implementar serviços de plataforma, revise a visão geral e as considerações para usar esses serviços.

Para obter informações sobre o S3, consulte"Usar API REST do S3" .

Visão geral dos serviços da plataforma

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

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

Qualquer combinação de serviços de plataforma pode ser configurada para um único bucket S3. Por exemplo, você pode configurar ambos"Serviço CloudMirror" e"notificações" em um bucket StorageGRID S3 para que você possa 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 rastrear suas despesas 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 de grade.

Como os serviços da plataforma são configurados

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

Depois de criar um ponto de extremidade externo, você pode habilitar um serviço de plataforma para um bucket adicionando configuração XML ao bucket. A configuração XML identifica os objetos nos quais o bucket deve atuar, a ação que o bucket deve executar e o ponto de extremidade 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 quiser todos os objetos cujas chaves começam com `/images` para ser replicado em 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, adicione uma configuração de notificações.
- Se quiser indexar os metadados desses objetos, você 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	API REST S3	Consulte
Replicação do CloudMirror	• Obter replicação do Bucket • PutBucketReplicação	• "Replicação do CloudMirror" • "Operações em baldes"
Notificações	• Obter configuração de notificação de bucket • Configuração de notificação PutBucket	• "Notificações" • "Operações em baldes"
Integração de pesquisa	• Configuração de notificação de metadados do GET Bucket • Configuração de notificação de metadados do PUT Bucket	• "Integração de pesquisa" • "Operações personalizadas do StorageGRID"

Considerações sobre o uso de serviços de plataforma

Consideração	Detalhes
Monitoramento de 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 longo período de tempo e houver um grande acúmulo de solicitações, solicitações adicionais de clientes (como solicitações PUT) para o StorageGRID falharão. Você deve tentar novamente essas solicitações com falha quando o ponto de extremidade estiver acessível.
Limitação do ponto de extremidade de destino	O software StorageGRID pode limitar as solicitações S3 recebidas para um bucket se a taxa na qual as solicitações estão sendo enviadas exceder a taxa na qual o ponto de extremidade de destino pode receber as solicitações. A limitação só ocorre quando há um acúmulo de solicitações aguardando para serem enviadas ao ponto de extremidade 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, reduza a taxa de ingestão ou use um ponto de extremidade com maior capacidade. Se o acúmulo de solicitações continuar a crescer, as operações do cliente S3 (como solicitações PUT) acabarão falhando. As solicitações do CloudMirror têm maior probabilidade de serem afetadas pelo desempenho do ponto de extremidade de destino porque essas solicitações geralmente envolvem mais transferência de dados do que as solicitações de integração de pesquisa ou notificação de eventos.

Consideração	Detalhes
Garantias de encomenda	O StorageGRID garante a ordenação das operações em um objeto dentro de um site. Desde que todas as operações em um objeto estejam no mesmo site, o estado final do objeto (para replicação) sempre será igual ao estado em StorageGRID. O StorageGRID faz o melhor esforço possível para ordenar solicitações quando operações são feitas em sites do StorageGRID . Por exemplo, se você gravar um objeto inicialmente no site A e depois substituir 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, as solicitações de notificação de eventos e do CloudMirror não são enviadas quando um objeto no bucket de origem é excluído devido às regras do StorageGRID ILM. Por exemplo, nenhuma solicitação de notificação de eventos ou do CloudMirror será enviada se uma regra do ILM excluir um objeto após 14 dias. Em contraste, 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 para `required` na configuração do seu broker Kafka, isso pode causar problemas de configuração do endpoint Kafka. A autenticação de endpoints do Kafka usa os seguintes tipos de autenticação. Esses tipos são diferentes daqueles usados para autenticação de outros endpoints, como o Amazon SNS, e exigem credenciais de nome de usuário e senha. • SASL/SIM • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Observação:** As configurações de proxy de armazenamento configuradas não se aplicam aos pontos de extremidade dos serviços da plataforma Kafka.

Considerações sobre o uso do serviço de replicação CloudMirror

Consideração	Detalhes
Status de replicação	O StorageGRID não oferece suporte a `x-amz-replication-status` cabeçalho.

Consideração	Detalhes
Tamanho do objeto	O tamanho máximo para objetos que podem ser replicados para um bucket de destino pelo serviço de replicação do CloudMirror é 5 TiB, que é o mesmo que o tamanho máximo de objeto *compatível*. **Observação**: O tamanho máximo *recomendado* para uma única operação PutObject é 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multiparte.
Controle de versão de bucket e IDs de versão	Se o bucket S3 de origem no StorageGRID tiver o versionamento habilitado, você também deverá habilitar o versionamento para o bucket de destino. Ao usar o controle de versão, observe que a ordenação das versões de objetos no bucket de destino é de melhor esforço e não é garantida pelo serviço CloudMirror, devido a limitações no protocolo S3. **Observação**: 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 no protocolo S3. Como os IDs de versão para a origem e o destino não estão relacionados, não há como garantir que uma atualização de tag para um ID de versão específico será replicada. Em contraste, o serviço CloudMirror replica solicitações PutObjectTagging ou 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 tiver versão). Ingestões normais com tags (não atualizações de marcação) também são replicadas.
Uploads multipartes e `ETag` valores	Ao espelhar objetos que foram carregados usando um upload multiparte, o serviço CloudMirror não preserva as partes. Como resultado, o `ETag` o valor para o 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 oferece suporte a objetos criptografados com SSE-C. Se você tentar ingerir um objeto no bucket de origem para replicação do CloudMirror e a solicitação incluir os cabeçalhos de solicitação SSE-C, a operação falhará.
Bucket com bloqueio de objeto S3 habilitado	A replicação não é suportada para buckets de origem ou destino com o S3 Object Lock habilitado.

Entenda o serviço de replicação do CloudMirror

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

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

> A replicação do CloudMirror não será suportada se o bucket de origem tiver o S3 Object Lock habilitado.

CloudMirror e ILM

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

CloudMirror e replicação entre grades

A replicação do CloudMirror tem semelhanças e diferenças importantes com o recurso de replicação entre grades. Consulte "Comparar a replicação entre grades e a replicação do CloudMirror" .

CloudMirror e buckets S3

A replicação do CloudMirror normalmente 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.

Baldes existentes

Quando você habilita a replicação do CloudMirror para um bucket existente, somente os novos objetos adicionados a esse bucket são replicados. Nenhum objeto existente no bucket é replicado. Para forçar a replicação de objetos existentes, você pode atualizar os metadados do objeto existente executando uma cópia do objeto.

> Se você estiver usando a replicação do CloudMirror para copiar objetos para um destino do 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 baldes de destino

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

Buckets versionados ou não versionados

Você pode configurar a replicação do 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 que o 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 os buckets de origem e destino forem versionados, o marcador de exclusão será replicado. Se o bucket de destino não

tiver versão, a exclusão de um objeto no bucket de origem não replicará o marcador de exclusão para o bucket de destino nem excluirá o objeto de destino.

Proteção contra loops de replicação

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

> ⓘ O cabeçalho personalizado usado para marcar uma réplica é `x-ntap-sg-replica` . Essa marcação evita um espelho em cascata. O StorageGRID suporta um CloudMirror bidirecional entre duas grades.

Eventos no bucket de destino

A exclusividade 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 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.

Entenda as notificações para buckets

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

Por exemplo, você pode configurar alertas a 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 são entregues ao destino. Se um evento associado a um objeto for bem-sucedido, uma notificação sobre esse evento será 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, não há garantia de que a ordem temporal das notificações no destino corresponda à ordem dos eventos no bucket de origem, principalmente para operações originadas de diferentes sites do StorageGRID . Você pode usar o `sequencer` digite a 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:ObjetoCriado:
  - s3:ObjectCreated:Colocar
  - s3:ObjetoCriado:Post
  - s3:ObjetoCriado:Copiar
  - s3:ObjetoCriado:CompleteMultipartUpload
  - s3:ObjetoRemovido:

- s3:ObjetoRemovido:Excluir
- s3:ObjetoRemovido:ExcluirMarcadorCriado
- s3:Restauração de Objeto:Postagem

- As notificações de eventos enviadas do 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 StorageGRID
fonte do evento	`sgws:s3`
Região aws	*não incluído*
x-amz-id-2	*não incluído*
arn	`urn:sgws:s3:::bucket_name`

Entenda o serviço de integração de pesquisa

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

O serviço de integração de pesquisa é um serviço StorageGRID personalizado que envia automaticamente e de forma assíncrona metadados de objetos do S3 para um ponto de extremidade de destino sempre que um objeto é criado ou excluído, ou 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 dos dados do seu objeto.

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

Embora a integração do Elasticsearch possa ser configurada em um bucket com o S3 Object Lock habilitado, os metadados do S3 Object Lock (incluindo a data de retenção e o status de retenção legal) 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 a um destino, seu XML de configuração é chamado de "XML de configuração de notificação *metadata*". 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 o XML de configuração de notificação de metadados ao bucket que especifica em quais objetos atuar e o destino dos metadados do objeto.

As notificações de metadados são geradas no formato 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 do objeto e metadados do usuário.

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

Notificações de pesquisa

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 grade.
- Metadados ou tags de 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 do usuário ou tags. No entanto, as notificações não são enviadas para nenhum objeto que já estava no bucket. Para garantir que os metadados de todos os objetos no bucket sejam enviados ao destino, você deve fazer um dos seguintes procedimentos:

- Configure o serviço de integração de pesquisa imediatamente após criar o bucket e antes de adicionar qualquer objeto.
- Execute uma ação em todos os objetos já existentes no bucket que acionará uma mensagem de notificação de metadados a ser enviada ao destino.

Serviço de integração de pesquisa e Elasticsearch

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

Gerenciar endpoints de serviços de plataforma

Configurar pontos de extremidade de serviços de plataforma

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

O acesso aos serviços da plataforma é habilitado por locatário por um administrador do StorageGRID . Para criar ou usar um ponto de extremidade de serviços de plataforma, você deve ser um usuário locatário com permissão de acesso Gerenciar pontos de extremidade ou Raiz, em uma grade cuja rede foi configurada para permitir que os Nós de Armazenamento acessem recursos de ponto de extremidade externos. Para um único locatário, você pode configurar no máximo 500 pontos de extremidade de serviços de plataforma. Entre em contato com o administrador do StorageGRID para obter mais informações.

O que é um ponto de extremidade de serviços de plataforma?

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

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

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

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

Pontos de extremidade para replicação do CloudMirror

O StorageGRID oferece suporte a endpoints de replicação que representam buckets do S3. Esses buckets podem ser hospedados no Amazon Web Services, na mesma implantação ou em uma implantação remota do StorageGRID ou em outro serviço.

Pontos finais para notificações

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

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

Pontos de extremidade para o serviço de integração de pesquisa

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

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

Informações relacionadas

"Administrar StorageGRID"

Especifique URN para o ponto de extremidade dos serviços de plataforma

Ao criar um ponto de extremidade de serviços de plataforma, você deve especificar um

Nome de Recurso Exclusivo (URN). Você usará o URN para referenciar o ponto de extremidade ao criar um XML de configuração para o serviço da plataforma. O URN para cada ponto de extremidade deve ser exclusivo.

O StorageGRID valida os pontos de extremidade dos serviços da plataforma conforme você os cria. Antes de criar um ponto de extremidade de serviços de plataforma, confirme se o recurso especificado no ponto de extremidade existe e se pode ser acessado.

Elementos URN

O URN para um ponto de extremidade de serviços de plataforma deve começar com `arn:aws` ou `urn:mysite` , do seguinte modo:

- 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 endpoint do CloudMirror 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
Replicação do CloudMirror	`s3`
Notificações	`sns`ou `kafka`
Integração de pesquisa	`es`

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

O elemento final do URN identifica o recurso de destino específico no URI de destino.

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

URNs para serviços hospedados na AWS e GCP

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

- Replicação do CloudMirror:

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

- Notificações:

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

- Integração de pesquisa:

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

> Para um ponto de extremidade de integração de pesquisa da AWS, o `domain-name` deve incluir a string literal `domain/` , como 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 maneira que crie um URN válido e exclusivo, desde que o URN inclua os elementos necessários na terceira e última posição. Você pode deixar os elementos indicados como opcionais em branco ou especificá-los de qualquer forma que ajude a identificar o recurso e tornar a URN única. Por exemplo:

- Replicação do CloudMirror:

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

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

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

- Notificações:

  Especifique um ponto de extremidade do Amazon Simple Notification Service:

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

  Especifique um ponto de extremidade do Kafka:

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

- Integração de pesquisa:

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

> Para pontos de extremidade de integração de pesquisa hospedados localmente, o `domain-name` element pode ser qualquer string, desde que o URN do ponto final seja único.

Criar ponto de extremidade de serviços de plataforma

Você deve criar pelo menos um ponto de extremidade do tipo correto antes de poder habilitar um serviço de plataforma.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Os serviços da plataforma foram habilitados para sua conta de locatário por um administrador do StorageGRID .
- Você pertence a um grupo de usuários que tem o"Gerenciar endpoints ou permissão de acesso root" .
- O recurso referenciado pelo ponto de extremidade dos serviços da plataforma foi criado:
  - Replicação do CloudMirror: bucket S3
  - Notificação de evento: Amazon Simple Notification Service (Amazon SNS) ou tópico Kafka
  - Notificação de pesquisa: índice do Elasticsearch, se o cluster de destino não estiver configurado para criar índices automaticamente.
- Você tem as informações sobre o recurso de destino:
  - Host e porta para o Uniform Resource Identifier (URI)

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

  - Nome de Recurso Único (URN)

    "Especifique URN para o ponto de extremidade dos serviços de 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

Pontos de extremidade de replicação do CloudMirror

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

- Chave de acesso: ID da chave de acesso e chave de acesso secreta
- CAP (C2S Access Portal): URL de credenciais temporárias, certificados de servidor e cliente, chaves de cliente e uma senha de chave privada de cliente opcional.

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 finais 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 estiver usando um certificado CA personalizado)

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

Passos

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

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

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

   Use um dos seguintes formatos:

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

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

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

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

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

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

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

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

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

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

5. Insira o Nome de Recurso Exclusivo (URN) para o ponto de extremidade.

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

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

Pontos de extremidade de integração de pesquisa

Insira ou carregue as credenciais para um ponto de extremidade 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 somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
Chave de acesso	Usa credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta
HTTP básico	Usa um nome de usuário e uma senha para autenticar conexões com o destino.	• Nome de usuário • Senha

Pontos de extremidade de replicação do CloudMirror

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

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

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
Chave de acesso	Usa credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta
CAP (Portal de Acesso C2S)	Usa 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 somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
Chave de acesso	Usa credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta

Pontos finais do Kafka

Insira ou carregue as credenciais para um ponto de extremidade 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 somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
SASL/SIM	Usa um nome de usuário e uma senha com texto simples para autenticar conexões com o destino.	• Nome de usuário • Senha
SASL/SCRAM-SHA-256	Usa um nome de usuário e uma 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	Usa um nome de usuário e uma senha usando um protocolo de desafio-resposta e hash SHA-512 para autenticar conexões com o destino.	• Nome de usuário • Senha

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

8. Selecione **Continuar**.
9. Selecione um botão de opção para **Verificar servidor** para escolher como a conexão TLS com o ponto de extremidade será verificada.

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

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

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

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

Informações relacionadas

- "Especifique URN para o ponto de extremidade dos serviços de plataforma"
- "Configurar a replicação do CloudMirror"
- "Configurar notificações de eventos"
- "Configurar serviço de integração de pesquisa"

Teste de conexão para ponto de extremidade de serviços de plataforma

Se a conexão com um serviço de plataforma tiver sido alterada, você poderá testar a conexão do ponto de extremidade para validar se o recurso de destino existe e se pode ser acessado usando as credenciais especificadas.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Gerenciar endpoints ou permissão de acesso root" .

Sobre esta tarefa

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

Passos

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

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

2. Selecione o ponto de extremidade cuja conexão você deseja testar.

   A página de detalhes do endpoint é exibida.

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

Editar ponto de extremidade dos serviços da plataforma

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Gerenciar endpoints ou permissão de acesso root" .

Passos

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

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

2. Selecione o ponto de extremidade que você deseja editar.

   A página de detalhes do endpoint é exibida.

3. Selecione **Configuração**.
4. Conforme necessário, altere a configuração do ponto de extremidade.

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

   a. Para alterar o nome de exibição do ponto de extremidade, selecione o ícone de edição .
   b. Conforme necessário, altere o URI.
   c. Conforme necessário, altere o tipo de autenticação.
      - Para autenticação de chave de acesso, altere a chave conforme necessário selecionando **Editar chave S3** e colando uma nova ID de chave de acesso e uma chave de acesso secreta. Se precisar cancelar suas alterações, selecione **Reverter edição da chave S3**.

- Para autenticação CAP (C2S Access Portal), altere a URL de credenciais temporárias ou a senha da chave privada do cliente opcional 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 de verificação do servidor.

5. Selecione **Testar e salvar alterações**.
   - Uma mensagem de sucesso será exibida se o ponto de extremidade puder ser alcançado usando as credenciais especificadas. A conexão com o ponto de extremidade é verificada a partir de um nó em cada site.
   - Uma mensagem de erro será exibida se a validação do endpoint falhar. Modifique o ponto de extremidade para corrigir o erro e selecione **Testar e salvar alterações**.

Excluir ponto de extremidade de serviços de plataforma

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

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Gerenciar endpoints ou permissão de acesso root" .

Passos

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

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

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

> Se você excluir um ponto de extremidade de serviços de plataforma que está em uso, o serviço de plataforma associado será desabilitado para todos os buckets que usarem o ponto de extremidade. Quaisquer solicitações que ainda não tenham sido concluídas serão descartadas. Quaisquer novas solicitações continuarão a ser geradas até que você altere a configuração do seu bucket para não fazer mais referência ao URN excluído. O StorageGRID relatará essas solicitações como erros irrecuperáveis.

3. Selecione **Ações** > **Excluir ponto de extremidade**.

   Uma mensagem de confirmação é exibida.

4. Selecione **Excluir ponto de extremidade**.

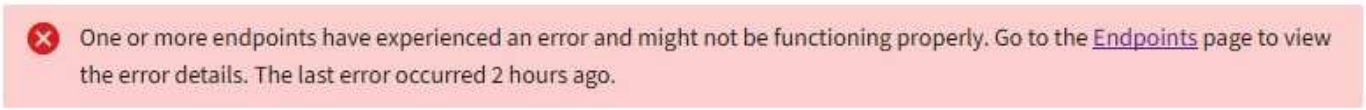
Solucionar erros de endpoint de serviços de plataforma

Se ocorrer um erro quando o StorageGRID tentar se comunicar com um ponto de extremidade de serviços da plataforma, uma mensagem será exibida no painel. Na página Pontos de extremidade dos serviços da plataforma, a coluna Último erro indica há

quanto tempo o erro ocorreu. Nenhum erro será exibido se as permissões associadas às credenciais de um endpoint estiverem incorretas.

Determinar se ocorreu um erro

Se algum erro de ponto de extremidade de serviços de plataforma tiver ocorrido nos últimos 7 dias, o painel do Gerenciador de Tenants 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 pontos de extremidade dos serviços da plataforma. Para ver 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 guia exibe apenas o erro mais recente de um ponto de extremidade e indica há quanto tempo o erro ocorreu. Erros que incluem o ícone X vermelho ocorreu nos últimos 7 dias.

Verifique se o erro ainda está presente

Alguns erros podem continuar a ser exibidos na coluna **Último erro** mesmo depois de serem resolvidos. Para verificar se um erro é atual ou para forçar a remoção de um erro resolvido da tabela:

Passos

1. Selecione o ponto final.

   A página de detalhes do endpoint é exibida.

2. Selecione **Conexão** > **Testar conexão**.

Selecionar **Testar conexão** faz com que o StorageGRID valide se o ponto de extremidade dos serviços da plataforma existe e se pode ser acessado com as credenciais atuais. A conexão com o ponto de extremidade 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 de CloudMirroring pode ocorrer se o StorageGRID não conseguir acessar o bucket S3 de destino porque não tem as permissões de acesso corretas ou a chave de acesso expirou. A mensagem é "As credenciais do endpoint ou o acesso ao destino precisam ser atualizados" e os detalhes são "AccessDenied" ou "InvalidAccessKeyId".

Se você precisar editar o endpoint para resolver 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 ponto de extremidade é validada a partir de um nó em cada site.

Passos

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

Credenciais de endpoint com permissões insuficientes

Quando o StorageGRID valida um ponto de extremidade de serviços de plataforma, ele confirma que as credenciais do ponto de extremidade podem ser usadas para entrar em contato com o recurso de destino e realiza uma verificação básica de permissões. No entanto, o 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 de plataforma (como "403 Forbidden"), verifique as permissões associadas às credenciais do endpoint.

Informações relacionadas

- **Administrar StorageGRID › Solucionar problemas de serviços de plataforma**
- "Criar ponto de extremidade de serviços de plataforma"
- "Teste de conexão para ponto de extremidade de serviços de plataforma"
- "Editar ponto de extremidade dos serviços da plataforma"

Configurar a replicação do CloudMirror

Para habilitar a replicação do CloudMirror para um bucket, crie e aplique um XML de configuração de replicação de bucket válido.

Antes de começar

- Os serviços da plataforma foram habilitados para sua conta de locatário por um administrador do StorageGRID .
- Você já criou um bucket para atuar como fonte de replicação.
- O ponto de extremidade que você pretende usar como destino para a replicação do CloudMirror já existe e você tem seu URN.
- Você pertence a um grupo de usuários que tem o"Gerenciar todos os buckets ou permissão de acesso root" . Essas permissões substituem as configurações de permissão em políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Tenants.

Sobre esta tarefa

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

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

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

Observe os seguintes requisitos e características ao configurar a replicação do CloudMirror:

- Ao criar e aplicar um XML de configuração de replicação de bucket válido, ele deve usar o URN de um ponto de extremidade de bucket do S3 para cada destino.
- A replicação não é suportada para buckets de origem ou destino com o S3 Object Lock habilitado.
- Se você habilitar a replicação do 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 deve atualizar os objetos existentes para acionar a replicação.
- Se você especificar uma classe de armazenamento no XML de configuração de replicação, o StorageGRID usará essa classe ao executar operações no ponto de extremidade S3 de destino. O ponto de extremidade de destino também deve suportar a classe de armazenamento especificada. Certifique-se de seguir todas as recomendações fornecidas pelo fornecedor do sistema de destino.

Passos

1. Habilite a replicação para seu bucket de origem:
   - Use 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 o StorageGRID suporta apenas a V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue as convenções V1 para exclusão de versões de objetos. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes.
     - Use o URN de um ponto de extremidade do bucket S3 como destino.
     - Opcionalmente, adicione o `<StorageClass>` elemento e especifique um dos seguintes:
       - `STANDARD`: A classe de armazenamento padrão. Se você não especificar uma classe de armazenamento ao carregar um objeto, o `STANDARD` classe de armazenamento é 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`: Use esta classe de armazenamento para dados não críticos e reproduzíveis que podem ser armazenados com menos redundância do que os `STANDARD` classe de armazenamento.
     - Se você especificar um `Role` no XML de configuração ele será ignorado. Este 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 **ARMAZENAMENTO (S3)** > **Buckets**.
3. Selecione o nome do bucket de origem.

   A página de detalhes do bucket é exibida.

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

> Os serviços da plataforma devem ser habilitados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a API de gerenciamento de grade. 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, conforme especificado na configuração de replicação.

      No exemplo mostrado anteriormente, os objetos que correspondem ao prefixo "2020" são replicados.

   b. Confirme se o objeto foi replicado para o bucket de destino.

      Para objetos pequenos, a replicação acontece rapidamente.

Informações relacionadas

"Criar ponto de extremidade de serviços de plataforma"

Configurar notificações de eventos

Você habilita notificações para um bucket criando um XML de configuração de notificação e usando o Tenant Manager para aplicar o XML a um bucket.

Antes de começar

- Os serviços da plataforma foram habilitados para sua conta de locatário por um administrador do StorageGRID .
- Você já criou um bucket para atuar como fonte de notificações.
- O ponto de extremidade que você pretende usar como destino para notificações de eventos já existe e você tem seu URN.
- Você pertence a um grupo de usuários que tem o"Gerenciar todos os buckets ou permissão de acesso root" . Essas permissões substituem as configurações de permissão em políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Tenants.

Sobre esta tarefa

Você configura notificações de eventos associando o XML de configuração de notificação a um bucket de origem. O XML de configuração de notificação segue as convenções do S3 para configurar notificações de bucket, com o tópico de destino do Kafka ou do Amazon SNS especificado como o URN de um endpoint.

Para obter informações gerais sobre notificações de eventos e como configurá-las, consulte o "Documentação da Amazon" . Para obter informações sobre como o StorageGRID implementa a API de configuração de notificação do bucket S3, consulte o"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, ele deve usar o URN de um ponto de extremidade de notificações de eventos para cada destino.
- Embora a notificação de eventos possa ser configurada em um bucket com o S3 Object Lock habilitado, os metadados do S3 Object Lock (incluindo Retain Until Date e status de retenção legal) dos objetos não serão incluídos nas mensagens de notificação.
- Depois de configurar as notificações de eventos, sempre que um evento especificado ocorrer para um objeto no bucket de origem, uma notificação será gerada e enviada ao tópico do Amazon SNS ou Kafka usado como endpoint de destino.
- Se você habilitar notificações de eventos para um bucket que contém objetos, as notificações serão enviadas somente para ações executadas após a configuração de notificação ser salva.

Passos

1. Habilite notificações para seu bucket de origem:
   - Use um editor de texto para criar o XML de configuração de notificação necessário para habilitar notificações de eventos, conforme especificado na API de notificação do S3.
   - Ao configurar o XML, use o URN de um ponto de extremidade de notificações de eventos como o tópico de destino.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. No Gerenciador 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 de plataforma** > **Notificações de eventos**.
5. Marque a caixa de seleção **Ativar notificações de eventos**.
6. Cole o XML de configuração de notificação na caixa de texto e selecione **Salvar alterações**.

Os serviços da plataforma devem ser habilitados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a API de gerenciamento de grade. 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 se uma notificação foi entregue ao tópico de destino do Amazon SNS ou do Kafka.

      Por exemplo, se o seu tópico de destino estiver hospedado no Amazon SNS, você poderá configurar o serviço para lhe 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"

"Usar API REST do S3"

"Criar ponto de extremidade de serviços de plataforma"

Configurar o serviço de integração de pesquisa

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 habilitados para sua conta de locatário por um administrador do StorageGRID .
- Você já criou um bucket S3 cujo conteúdo deseja indexar.
- O ponto de extremidade que você pretende usar como destino para o serviço de integração de pesquisa já existe e você tem seu URN.
- Você pertence a um grupo de usuários que tem o"Gerenciar todos os buckets ou permissão de acesso root" . Essas permissões substituem as configurações de permissão em políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Tenants.

Sobre esta tarefa

Depois de 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 de metadados do objeto para o ponto de extremidade de destino.

Se você habilitar o serviço de integração de pesquisa para um bucket que já contém objetos, as notificações de metadados não serão enviadas automaticamente para objetos existentes. Atualize esses objetos existentes para garantir que seus metadados sejam adicionados ao índice de pesquisa de destino.

Passos

1. Habilitar integração de pesquisa para um bucket:
    - Use 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 ponto de extremidade 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 que têm prefixos sobrepostos não são válidas e são rejeitadas quando enviadas. Por exemplo, uma configuração que inclui uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não é permitido.

      Conforme necessário, consulte oexemplos para a configuração de metadados XML .

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

Elementos no XML de configuração de notificação de metadados:

Nome	Descrição	Obrigatório
Configuração de Notificação de Metadados	Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos Rule.	Sim
Regra	Tag de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
EU IA	Identificador exclusivo para a regra. Incluído no elemento Rule.	Não
Status	O status pode ser "Habilitado" ou "Desabilitado". Nenhuma ação é tomada para regras que estão desabilitadas. Incluído no elemento Rule.	Sim
Prefixo	Objetos que correspondem ao prefixo são afetados pela regra, e seus metadados são enviados ao destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento Rule.	Sim
Destino	Tag 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 a URN de um ponto de extremidade StorageGRID com as seguintes propriedades: • `es`deve ser o terceiro elemento. • A URN deve terminar com o índice e o tipo onde os metadados são armazenados, no formato `domain-name/myindex/mytype` . Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles assumem a seguinte forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O ponto de extremidade deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. URN está incluído no elemento Destino.	Sim

2. No Gerenciador de inquilinos, selecione **ARMAZENAMENTO (S3)** > **Buckets**.
3. Selecione o nome do bucket de origem.

   A página de detalhes do bucket é exibida.

4. Selecione **Serviços de plataforma** > **Integração de pesquisa**
5. Marque a caixa de seleção **Ativar integração de pesquisa**.
6. Cole a configuração de notificação de metadados na caixa de texto e selecione **Salvar alterações**.

   Os serviços da plataforma devem ser habilitados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a API de gerenciamento. Entre em contato com o 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 que contém os metadados e as tags do objeto foi adicionado ao índice de pesquisa especificado no ponto de extremidade.

Depois que você terminar

Conforme necessário, você pode desabilitar a integração de pesquisa para um bucket usando um dos

seguintes métodos:

- Selecione **ARMAZENAMENTO (S3)** > **Buckets** e desmarque a caixa de seleção **Ativar integração de pesquisa**.
- Se você estiver usando a API do S3 diretamente, use uma solicitação de notificação de metadados DELETE Bucket. 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 de todos os objetos são enviados para o mesmo destino.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Exemplo: configuração de notificação de metadados com duas regras

Neste exemplo, metadados de objetos para objetos que correspondem ao prefixo `/images` é enviado para um destino, enquanto metadados de objeto para objetos que correspondem ao prefixo `/videos` é enviado 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

Quando você habilita o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado ao ponto de extremidade de destino sempre que metadados ou tags de objeto são adicionados, atualizados ou excluídos.

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

`bucket`: Nome do balde

`key`: Nome da chave do objeto

`versionID`: Versão do objeto, para objetos em buckets versionados

`region`: Região de balde, por exemplo `us-east-1`

Metadados do sistema

`size`: Tamanho do objeto (em bytes) conforme visível para um cliente HTTP

`md5`: Hash do objeto

Metadados do usuário

`metadata`: Todos os metadados do usuário para o objeto, como pares chave-valor

`key:value`

Etiquetas

`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, o StorageGRID passa datas e números para o Elasticsearch como strings ou como notificações de eventos do S3. Para configurar o Elasticsearch para interpretar essas strings como

datas ou números, siga as instruções do Elasticsearch para mapeamento de campos dinâmicos e para mapeamento de formatos de data. Habilite os mapeamentos de campos dinâmicos no índice antes de configurar o serviço de integração de pesquisa. Depois que um documento é indexado, você não pode editar os tipos de campo do documento no índice.

Usar API REST do S3

Versões e atualizações suportadas pela API REST do S3

O StorageGRID oferece suporte à API Simple Storage Service (S3), que é implementada como um conjunto de serviços web Representational State Transfer (REST).

O suporte para a API REST do S3 permite que você conecte aplicativos orientados a serviços desenvolvidos para serviços da Web do S3 com armazenamento de objetos local que usa o sistema StorageGRID . São necessárias alterações mínimas no uso atual de chamadas da API REST do S3 por um aplicativo cliente.

Versões suportadas

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

Item	Versão
Especificação da API S3	"Documentação da Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service"
HTTP	1,1 Para obter mais informações sobre HTTP, consulte HTTP/1.1 (RFCs 7230-35). "IETF RFC 2616: Protocolo de Transferência de Hipertexto (HTTP/1.1)" **Observação**: O StorageGRID não oferece suporte a pipeline HTTP/1.1.

Atualizações no suporte à API REST do S3

Liberar	Comentários
11,9	• Adicionado suporte para valores de soma de verificação SHA-256 pré-calculados para as seguintes solicitações e cabeçalhos suportados. Você pode usar este recurso para verificar a integridade dos objetos enviados: ◦ Upload completo de várias partes: `x-amz-checksum-sha256` ◦ CriarMultipartUpload: `x-amz-checksum-algorithm` ◦ ObterObjeto: `x-amz-checksum-mode` ◦ HeadObject: `x-amz-checksum-mode` ◦ ListarPartes ◦ ColocarObjeto: `x-amz-checksum-sha256` ◦ UploadPart: `x-amz-checksum-sha256` • Foi adicionada a capacidade do administrador da grade de controlar as configurações de conformidade e retenção no nível do locatário. Essas configurações afetam as configurações de bloqueio de objeto do S3. ◦ Modo de retenção padrão do bucket e modo de retenção de objeto: Governança ou Conformidade, se permitido pelo administrador da grade. ◦ Período de retenção padrão do bucket e data de retenção do objeto: deve ser menor ou igual ao permitido pelo período máximo de retenção definido pelo administrador da grade. • Suporte aprimorado para `aws-chunked` codificação e streaming de conteúdo `x-amz-content-sha256` valores. Limitações: ◦ Se presente, `chunk-signature` é opcional e não validado ◦ Se presente, `x-amz-trailer` o conteúdo é ignorado
11,8	Atualizou os nomes das operações do S3 para corresponder aos nomes usados no "Documentação da Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service" .
11,7	• Adicionado"Referência rápida: solicitações de API do S3 suportadas" . • Adicionado suporte para usar o modo GOVERNANCE com o S3 Object Lock. • Adicionado suporte para StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta para solicitações GET Object e HEAD Object. Este cabeçalho fornece o status de replicação de um objeto para replicação entre grades. • Solicitações SelectObjectContent agora oferecem suporte a objetos Parquet.

Liberar	Comentários
11,6	• Adicionado suporte para usar o `partNumber` parâmetro de solicitação em solicitações GET Object e HEAD Object. • Adicionado suporte para um modo de retenção padrão e um período de retenção padrão no nível do bucket para o S3 Object Lock. • Adicionado suporte para o `s3:object-lock-remaining-retention-days` chave de condição de política para definir o intervalo de períodos de retenção permitidos para seus objetos. • Foi alterado o tamanho máximo *recomendado* para uma única operação PUT Object para 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multiparte.
11,5	• Adicionado suporte para gerenciamento de criptografia de bucket. • Suporte adicionado para bloqueio de objeto S3 e solicitações de conformidade legadas obsoletas. • Adicionado suporte para usar DELETE Multiple Objects em buckets versionados. • O `Content-MD5` O cabeçalho da solicitação agora é suportado corretamente.
11,4	• Adicionado suporte para marcação de Bucket DELETE, marcação de Bucket GET e marcação de Bucket PUT. Tags de alocação de custos não são suportadas. • Para buckets criados no StorageGRID 11.4, não é mais necessário restringir nomes de chaves de objeto para atender às práticas recomendadas de desempenho. • Adicionado suporte para notificações de bucket no `s3:ObjectRestore:Post` tipo de evento. • Os limites de tamanho da AWS para partes multipartes agora são aplicados. Cada parte em um upload multiparte deve ter entre 5 MiB e 5 GiB. A última parte pode ser menor que 5 MiB. • Adicionado suporte para TLS 1.3
11,3	• Adicionado suporte para criptografia do lado do servidor de dados de objetos com chaves fornecidas pelo cliente (SSE-C). • Adicionado suporte para operações de ciclo de vida de bucket DELETE, GET e PUT (somente ação de expiração) e para `x-amz-expiration` cabeçalho de resposta. • Objeto PUT atualizado, Objeto PUT - Cópia e Upload Multipartes para descrever o impacto das regras do ILM que usam posicionamento síncrono na ingestão. • As cifras TLS 1.1 não são mais suportadas.

Liberar	Comentários
11,2	Adicionado suporte para restauração de objetos POST para uso com pools de armazenamento em nuvem. Adicionado suporte para usar a sintaxe da AWS para ARN, chaves de condição de política e variáveis de política em políticas de grupo e bucket. As políticas de grupo e bucket existentes que usam a sintaxe StorageGRID continuarão a ser suportadas. **Observação:** Os usos de ARN/URN em outras configurações JSON/XML, incluindo aqueles usados em recursos personalizados do StorageGRID , não foram alterados.
11,1	Adicionado suporte para compartilhamento de recursos entre origens (CORS), HTTP para conexões de cliente S3 com nós de grade e configurações de conformidade em buckets.
11,0	Adicionado suporte para configuração de serviços de plataforma (replicação do CloudMirror, notificações e integração de pesquisa do Elasticsearch) para buckets. Também foi adicionado suporte para restrições de localização de marcação de objetos para buckets e consistência disponível.
10,4	Adicionado suporte para alterações de verificação de ILM no controle de versão, atualizações da página Nomes de Domínio de Endpoint, condições e variáveis em políticas, exemplos de políticas e a permissão PutOverwriteObject.
10,3	Adicionado suporte para controle de versão.
10,2	Adicionado suporte para políticas de acesso de grupo e bucket, e para cópia multiparte (Upload Part - Copy).
10,1	Adicionado suporte para upload multiparte, solicitações de estilo de hospedagem virtual e autenticação v4.
10,0	Suporte inicial da API REST do S3 pelo sistema StorageGRID . A versão atualmente suportada da *Simple Storage Service API Reference* é 2006-03-01.

Referência rápida: solicitações de API do S3 suportadas

Esta página resume como o StorageGRID oferece suporte às APIs do Amazon Simple Storage Service (S3).

Esta página inclui apenas as operações do S3 suportadas pelo StorageGRID.

Para ver a documentação da AWS para cada operação, selecione o link no título.

Parâmetros de consulta URI comuns e cabeçalhos de solicitação

A menos que indicado, os seguintes parâmetros comuns de consulta de URI são suportados:

- `versionId`(conforme necessário para operações de objeto)

A menos que indicado, os seguintes cabeçalhos de solicitação comuns são suportados:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informações relacionadas

- "Detalhes da implementação da API REST S3"
- "Referência da API do Amazon Simple Storage Service: Cabeçalhos de solicitação comuns"

"AbortarMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, mais este parâmetro de consulta URI adicional:

- `uploadId`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações para uploads multipartes"

"Upload completo de várias partes"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, mais este parâmetro de consulta URI adicional:

- `uploadId`
- `x-amz-checksum-sha256`

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`

- `Part`
- `PartNumber`

Documentação do StorageGRID

"Upload completo de várias partes"

"CopiarObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes cabeçalhos adicionais:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"CopiarObjeto"

"CriarBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes cabeçalhos adicionais:

- `x-amz-bucket-object-lock-enabled`

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em baldes"

"CriarMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes cabeçalhos adicionais:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"CriarMultipartUpload"

"ExcluirBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Documentação do StorageGRID

"Operações em baldes"

"ExcluirBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"DeleteBucketEncryption"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Ciclo de vida do DeleteBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

- "Operações em baldes"
- "Criar configuração do ciclo de vida do S3"

"Política de exclusão de balde"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"DeleteBucketReplication"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ExcluirBucketTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ExcluirObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, mais este cabeçalho de solicitação adicional:

- `x-amz-bypass-governance-retention`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"ExcluirObjetos"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, mais este cabeçalho de solicitação adicional:

- `x-amz-bypass-governance-retention`

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em objetos"

"ExcluirMarcaçãoDeObjeto"

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"ObterBucketAcl"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ObterBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Obter criptografia do Bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Obter configuração do ciclo de vida do Bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

- "Operações em baldes"
- "Criar configuração do ciclo de vida do S3"

"ObterBucketLocation"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Obter configuração de notificação de bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ObterBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Obter replicação do Bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Obter marcação de balde"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ObterVersionamento doBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ObterObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

E estes cabeçalhos de solicitação adicionais:

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"ObterObjeto"

"ObterAclObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"ObterObjetoLegalHold"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objeto do S3"

"ObterConfiguraçãoObjectLock"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objeto do S3"

"ObterRetençãoDeObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objeto do S3"

"Obter marcação de objeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em objetos"

"Balde de cabeça"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"CabeçaObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes cabeçalhos adicionais:

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"CabeçaObjeto"

"ListBuckets"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

Operações no serviço › ListBuckets

"ListarMultipartUploads"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

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

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"ListarMultipartUploads"

"Objetos de Lista"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ListObjectsV2"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"Versões do objeto de lista"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"Operações em baldes"

"ListarPartes"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros adicionais:

- `max-parts`

- `part-number-marker`
- `uploadId`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"ListarMultipartUploads"

"ColoqueBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em baldes"

"PutBucketEncryption"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

Documentação do StorageGRID

"Operações em baldes"

"Configuração do ciclo de vida do PutBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- `And`
- `Days`
- `Expiration`

- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

Documentação do StorageGRID

- "Operações em baldes"
- "Criar configuração do ciclo de vida do S3"

"Configuração de notificação PutBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

Documentação do StorageGRID

"Operações em baldes"

"PutBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Para obter detalhes sobre os campos de corpo JSON suportados, consulte"Use políticas de acesso a buckets e grupos" .

"PutBucketReplicação"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Tags XML do corpo da solicitação

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

Documentação do StorageGRID

"Operações em baldes"

"Colocar marcação de balde"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em baldes"

"Versão PutBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Parâmetros do corpo da solicitação

O StorageGRID suporta estes parâmetros do corpo da solicitação:

- `VersioningConfiguration`
- `Status`

Documentação do StorageGRID

"Operações em baldes"

"ColocarObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes cabeçalhos adicionais:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corpo da solicitação

- Dados binários do objeto

Documentação do StorageGRID

"ColocarObjeto"

"ColocarObjetoLegalHold"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objeto do S3"

"PutObjectLockConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objeto do S3"

"ColocarRetençãoDeObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, mais este cabeçalho adicional:

- `x-amz-bypass-governance-retention`

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Use a API REST do S3 para configurar o bloqueio de objeto do S3"

"Colocar marcação de objeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

"Operações em objetos"

"RestaurarObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Para obter detalhes sobre os campos corporais suportados, consulte"RestaurarObjeto" .

"SelecionarObjetoConteúdo"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação.

Corpo da solicitação

Para obter detalhes sobre os campos corporais suportados, consulte o seguinte:

- "Use o S3 Select"
- "SelecionarObjetoConteúdo"

"UploadPart"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `partNumber`
- `uploadId`

E estes cabeçalhos de solicitação adicionais:

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corpo da solicitação

- Dados binários da peça

Documentação do StorageGRID

"UploadPart"

"UploadPartCopy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todosparâmetros e cabeçalhos comuns para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `partNumber`
- `uploadId`

E estes cabeçalhos de solicitação adicionais:

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

- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

"UploadPartCopy"

Testar configuração da API REST do S3

Você pode usar a Amazon Web Services Command Line Interface (AWS CLI) para testar sua conexão com o sistema e verificar se você consegue ler e gravar objetos.

Antes de começar

- Você baixou e instalou o AWS CLI de "aws.amazon.com/cli" .
- Opcionalmente, você tem"criou um ponto de extremidade do balanceador de carga" . Caso contrário, você sabe o endereço IP do nó de armazenamento ao qual deseja se conectar e o número da porta a ser usada. Ver "Endereços IP e portas para conexões de clientes" .
- Você tem"criou uma conta de locatário S3" .
- Você fez login no inquilino e"criou uma chave de acesso" .

Para obter detalhes sobre essas etapas, consulte"Configurar conexões do cliente" .

Passos

1. Configure as definições da AWS CLI para usar a conta que você criou no sistema StorageGRID :
   a. Entrar no modo de configuração: `aws configure`
   b. Digite o ID da chave de acesso da conta que você criou.
   c. Digite a chave de acesso secreta da conta que você criou.
   d. Digite a região padrão a ser usada. Por exemplo, `us-east-1` .
   e. Digite o formato de saída padrão a ser usado ou pressione **Enter** para selecionar JSON.
2. Crie um bucket.

   Este exemplo pressupõe que você configurou um ponto de extremidade do balanceador de carga para usar o endereço IP 10.96.101.17 e a porta 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Se o bucket for criado com sucesso, o local do bucket será retornado, conforme visto no exemplo a seguir:

```
"Location": "/testbucket"
```

3. Carregar um objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Se o objeto for carregado com sucesso, uma Etag será retornada, que é um hash dos dados do objeto.

4. Liste o conteúdo do bucket para verificar se o objeto foi carregado.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Exclua o objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Exclua o bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Como o StorageGRID implementa a API REST do S3

Solicitações conflitantes de clientes

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos".

O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

Valores de consistência

A consistência fornece um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de armazenamento e sites. Você pode alterar a consistência conforme exigido pelo seu aplicativo.

Por padrão, o StorageGRID garante consistência de leitura após gravação para objetos recém-criados. Qualquer GET após um PUT concluído com sucesso poderá ler os dados recém-gravados. Substituições de objetos existentes, atualizações de metadados e exclusões são eventualmente consistentes. As substituições geralmente levam segundos ou minutos para se propagar, mas podem levar até 15 dias.

Se você quiser executar operações de objeto com uma consistência diferente, você pode:

- Especifique uma consistência paracada balde .
- Especifique uma consistência paracada operação de API .
- Altere a consistência padrão em toda a grade executando uma das seguintes tarefas:
  - No Grid Manager, vá para **CONFIGURAÇÃO** > **Sistema** > **Configurações de armazenamento** > **Consistência padrão**.
  - .

> Uma alteração na consistência de toda a grade se aplica somente aos buckets criados após a configuração ter sido alterada. Para determinar os detalhes de uma alteração, consulte o log de auditoria localizado em `/var/local/log` (pesquise por **consistencyLevel**).

Valores de consistência

A consistência afeta como os metadados que o StorageGRID usa para rastrear objetos são distribuídos entre os nós e, portanto, a disponibilidade dos objetos para solicitações do cliente.

Você pode definir a consistência de um bucket ou de uma operação de API para um dos seguintes valores:

- **Todos**: Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
- **Strong-global**: Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
- **Strong-site**: Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.
- **Leitura após nova gravação**: (Padrão) Fornece 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**: Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que raramente são lidos ou para operações HEAD ou GET em chaves que não existem). Não suportado para buckets do S3 FabricPool .

Use a consistência "Leitura após nova gravação" e "Disponível"

Quando uma operação HEAD ou GET usa a consistência "Leitura após nova gravação", o StorageGRID executa a pesquisa em várias etapas, da seguinte maneira:

- Primeiro, ele procura o objeto usando uma consistência baixa.
- Se essa pesquisa falhar, ela será repetida no próximo valor de consistência até atingir uma consistência equivalente ao comportamento de strong-global.

Se uma operação HEAD ou GET usar a consistência "Leitura após nova gravação", mas o objeto não existir, a pesquisa de objetos sempre alcançará uma consistência equivalente ao comportamento de strong-global. Como essa consistência exige que várias cópias dos metadados do objeto estejam disponíveis em cada site, você poderá receber um alto número de erros 500 do servidor interno se dois ou mais nós de armazenamento no mesmo site estiverem indisponíveis.

A menos que você precise de garantias de consistência semelhantes às do Amazon S3, você pode evitar esses erros para operações HEAD e GET definindo a consistência como "Disponível". Quando uma operação HEAD ou GET usa a consistência "Disponível", o StorageGRID fornece apenas consistência eventual. Ele não tenta novamente uma operação com falha para aumentar a consistência, portanto, não exige que várias cópias dos metadados do objeto estejam disponíveis.

Especificar consistência para operação de API

Para definir a consistência de uma operação de API individual, os valores de consistência devem ser suportados para a operação e você deve especificar a consistência no cabeçalho da solicitação. Este exemplo define a consistência como "Strong-site" para uma operação GetObject.

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

> Você deve usar a mesma consistência para as operações PutObject e GetObject.

Especificar consistência para bucket

Para definir a consistência do bucket, você pode usar o StorageGRID"Consistência do balde PUT" solicitar. Ou você pode"alterar a consistência de um balde" do gerente do inquilino.

Ao definir a consistência de um bucket, esteja ciente do seguinte:

- Definir a consistência de um bucket determina qual consistência será usada para operações do S3 executadas nos objetos no bucket ou na configuração do bucket. Não afeta as operações no próprio bucket.
- A consistência de uma operação de API individual substitui a consistência do bucket.
- Em geral, os buckets devem usar a consistência padrão, "Leitura após nova gravação". Se as solicitações não estiverem funcionando corretamente, altere o comportamento do cliente do aplicativo, se possível. Ou configure o cliente para especificar a consistência para cada solicitação de API. Defina a consistência no nível do bucket somente como último recurso.

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

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

Por exemplo, a consistência usada quando um objeto é armazenado afeta o posicionamento inicial dos metadados do objeto, enquanto o comportamento de ingestão selecionado para a regra ILM afeta o posicionamento inicial das cópias do objeto. Como o StorageGRID requer acesso aos metadados de um objeto e seus dados para atender às solicitações do cliente, selecionar níveis correspondentes de proteção para consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas do sistema mais previsíveis.

A seguir"opções de ingestão" estão disponíveis para regras ILM:

Comprometimento duplo

O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

Estrito

Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja retornado ao cliente.

Equilibrado

O StorageGRID tenta fazer todas as cópias especificadas na regra ILM na ingestão; se isso não for possível, cópias provisórias são feitas e o sucesso é retornado ao cliente. As cópias especificadas na regra ILM são feitas quando possível.

Exemplo de como a consistência e a regra ILM podem interagir

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

- **Regra do ILM**: Crie duas cópias de objetos, uma no site local e outra em um site remoto. Use o comportamento de ingestão estrito.
- **consistência**: Forte-global (os metadados do objeto são imediatamente distribuídos para todos os sites).

Quando um cliente armazena um objeto na grade, o StorageGRID faz cópias do objeto e distribui metadados para ambos os sites antes de retornar o sucesso ao cliente.

O objeto é totalmente protegido contra perda no momento da ingestão bem-sucedida da mensagem. Por exemplo, se o site local for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existirão no site remoto. O objeto é totalmente recuperável.

Se, em vez disso, você usasse a mesma regra de ILM e a consistência de site forte, o cliente poderia receber uma mensagem de sucesso depois que os dados do objeto fossem replicados para o site remoto, mas antes que os metadados do objeto fossem distribuídos lá. Nesse caso, o nível de proteção dos metadados do objeto não corresponde ao nível de proteção dos dados do objeto. Se o site local for perdido logo após a ingestão, os metadados do objeto serão perdidos. O objeto não pode ser recuperado.

A inter-relação entre consistência e regras de ILM pode ser complexa. Entre em contato com a NetApp se precisar de assistência.

Controle de versão de objetos

Você pode definir o estado de controle de versão de um bucket se quiser manter várias versões de cada objeto. Habilitar o controle de versão para um bucket pode ajudar a proteger contra a exclusão acidental de objetos e permite que você recupere e restaure versões anteriores de um objeto.

O sistema StorageGRID implementa o controle de versão com suporte para a maioria dos recursos e com algumas limitações. O StorageGRID suporta até 10.000 versões de cada objeto.

O controle de versão de objetos pode ser combinado com o gerenciamento do ciclo de vida das informações (ILM) do StorageGRID ou com a configuração do ciclo de vida do bucket do S3. Você deve habilitar explicitamente o controle de versão para cada bucket. Quando o controle de versão é habilitado para um bucket, cada objeto adicionado ao bucket recebe um ID de versão, que é gerado pelo sistema StorageGRID .

O uso de MFA (autenticação multifator) não é suportado.

> O controle de versão pode ser habilitado somente em buckets criados com o StorageGRID versão 10.3 ou posterior.

ILM e controle de versão

As políticas de ILM são aplicadas a cada versão de um objeto. Um processo de verificação de ILM verifica continuamente todos os objetos e os reavalia em relação à política de ILM atual. Quaisquer alterações feitas nas políticas do ILM serão aplicadas a todos os objetos ingeridos anteriormente. Isso inclui versões ingeridas anteriormente se o controle de versão estiver habilitado. A verificação de ILM aplica novas alterações de ILM a objetos ingeridos anteriormente.

Para objetos S3 em buckets habilitados para controle de versão, o suporte ao controle de versão permite que você crie regras ILM que usam "Tempo não atual" como o Tempo de referência (selecione **Sim** para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas?" em"Etapa 1 do assistente Criar uma regra ILM"). Quando um objeto é atualizado, suas versões anteriores se tornam obsoletas. Usar um filtro "Tempo não atual" permite criar políticas que reduzem o impacto de armazenamento de versões anteriores de objetos.

> Ao carregar uma nova versão de um objeto usando uma operação de upload multipartes, o tempo não atual para a versão original do objeto reflete quando o upload multipartes foi criado para a nova versão, não quando o upload multipartes foi concluído. Em casos limitados, o horário não atual da versão original pode ser horas ou dias anterior ao horário da versão atual.

Informações relacionadas

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

Use a API REST do S3 para configurar o bloqueio de objeto do S3

Se a configuração global do S3 Object Lock estiver habilitada para seu sistema StorageGRID , você poderá criar buckets com o S3 Object Lock habilitado. Você pode especificar a retenção padrão para cada bucket ou configurações de retenção para cada versão do objeto.

Como habilitar o bloqueio de objeto S3 para um bucket

Se a configuração global S3 Object Lock estiver habilitada para seu sistema StorageGRID , você poderá habilitar o S3 Object Lock ao criar cada bucket.

O bloqueio de objeto do S3 é uma configuração permanente que só pode ser ativada quando você cria um bucket. Não é possível adicionar ou desabilitar o S3 Object Lock após a criação de um bucket.

Para habilitar o bloqueio de objeto S3 para um bucket, use um destes métodos:

- Crie o bucket usando o Tenant Manager. Ver "Criar bucket S3" .
- Crie o bucket usando uma solicitação CreateBucket com o `x-amz-bucket-object-lock-enabled` cabeçalho da solicitação. Ver "Operações em baldes" .

O S3 Object Lock requer controle de versão do bucket, que é ativado automaticamente quando o bucket é criado. Não é possível suspender o controle de versão do bucket. Ver "Controle de versão de objetos" .

Configurações de retenção padrão para um bucket

Quando o Bloqueio de Objeto S3 estiver habilitado para um bucket, você poderá, opcionalmente, habilitar a retenção padrão para o bucket e especificar um modo de retenção padrão e um período de retenção padrão.

Modo de retenção padrão

- No modo CONFORMIDADE:
  - O objeto não pode ser excluído até que sua data de retenção seja atingida.
  - A data de retenção do objeto pode ser aumentada, mas não diminuída.
  - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- No modo GOVERNANÇA:
  - Usuários com o `s3:BypassGovernanceRetention` permissão pode usar o `x-amz-bypass-governance-retention: true` cabeçalho de solicitação para ignorar as configurações de retenção.
  - Esses usuários podem excluir uma versão do objeto antes que sua data de retenção seja atingida.
  - Esses usuários podem aumentar, diminuir ou remover a data de retenção de um objeto.

Período de retenção padrão

Cada bucket pode ter um período de retenção padrão especificado em anos ou dias.

Como definir a retenção padrão para um bucket

Para definir a retenção padrão para um bucket, use um destes métodos:

- Gerencie as configurações do bucket no Gerenciador de locatários. Ver"Criar um bucket S3" e"Atualizar retenção padrão do bloqueio de objeto S3" .
- Emita uma solicitação PutObjectLockConfiguration para o bucket para especificar o modo padrão e o número padrão de dias ou anos.

PutObjectLockConfiguration

A solicitação PutObjectLockConfiguration permite que você defina e modifique o modo de retenção padrão e o período de retenção padrão para um bucket que tenha o S3 Object Lock habilitado. Você também pode remover as configurações de retenção padrão configuradas anteriormente.

Quando novas versões de objetos são ingeridas no bucket, o modo de retenção padrão é aplicado se `x-amz-object-lock-mode` e `x-amz-object-lock-retain-until-date` não são especificados. O período de retenção padrão é usado para calcular a data de retenção se `x-amz-object-lock-retain-until-date` não é especificado.

Se o período de retenção padrão for modificado após a ingestão de uma versão do objeto, a data de retenção da versão do objeto permanecerá a mesma e não será recalculada usando o novo período de retenção padrão.

Você deve ter o `s3:PutBucketObjectLockConfiguration` permissão, ou ser root da conta, para concluir esta operação.

O `Content-MD5` O cabeçalho da solicitação deve ser especificado na solicitação PUT.

Exemplo de solicitação

Este exemplo habilita o S3 Object Lock para um bucket e define o modo de retenção padrão como COMPLIANCE e o período de retenção padrão como 6 anos.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Como determinar a retenção padrão para um bucket

Para determinar se o S3 Object Lock está habilitado para um bucket e para ver o modo de retenção padrão e o período de retenção, use um destes métodos:

- Visualize o bucket no Gerenciador de locatários. Ver "Exibir buckets S3" .
- Emita uma solicitação GetObjectLockConfiguration.

ObterConfiguraçãoObjectLock

A solicitação GetObjectLockConfiguration permite que você determine se o S3 Object Lock está habilitado para um bucket e, se estiver, veja se há um modo de retenção padrão e um período de retenção configurados para o bucket.

Quando novas versões de objetos são ingeridas no bucket, o modo de retenção padrão é aplicado se `x-amz-`

`object-lock-mode` não é especificado. O período de retenção padrão é usado para calcular a data de retenção se `x-amz-object-lock-retain-until-date` não é especificado.

Você deve ter o `s3:GetBucketObjectLockConfiguration` permissão, ou ser root da conta, para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Exemplo de resposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Como especificar configurações de retenção para um objeto

Um bucket com o S3 Object Lock ativado pode conter uma combinação de objetos com e sem configurações de retenção do S3 Object Lock.

As configurações de retenção no nível do objeto são especificadas usando a API REST do S3. As configurações de retenção de um objeto substituem quaisquer configurações de retenção padrão do bucket.

Você pode especificar as seguintes configurações para cada objeto:

- **Modo de retenção**: CONFORMIDADE ou GOVERNANÇA.
- **Retain-until-date**: Uma data que especifica por quanto tempo a versão do objeto deve ser retida pelo StorageGRID.
  - No modo CONFORMIDADE, se a data de retenção for no futuro, o objeto poderá ser recuperado, mas não poderá ser modificado ou excluído. A data de retenção pode ser aumentada, mas esta data não pode ser diminuída ou removida.
  - No modo GOVERNANÇA, usuários com permissão especial podem ignorar a configuração de retenção até a data. Eles podem excluir uma versão do objeto antes que seu período de retenção termine. Eles também podem aumentar, diminuir ou até mesmo remover a data de retenção.
- **Retenção legal**: Aplicar uma retenção legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar reter legalmente um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até ser explicitamente removida.

  A configuração de retenção legal para um objeto é independente do modo de retenção e da data de retenção. Se uma versão do objeto estiver sob retenção legal, ninguém poderá excluí-la.

Para especificar as configurações de bloqueio de objeto do S3 ao adicionar uma versão de objeto a um bucket, emita um"ColocarObjeto" ,"CopiarObjeto" , ou"CriarMultipartUpload" solicitar.

Você pode usar o seguinte:

- `x-amz-object-lock-mode`, que pode ser COMPLIANCE ou GOVERNANCE (diferencia maiúsculas de minúsculas).

  > Se você especificar `x-amz-object-lock-mode` , você também deve especificar `x-amz-object-lock-retain-until-date` .

- `x-amz-object-lock-retain-until-date`
  - O valor reter-até-data deve estar no formato `2020-08-10T21:46:00Z` . Segundos fracionários são permitidos, mas apenas 3 dígitos decimais são preservados (precisão de milissegundos). Outros formatos ISO 8601 não são permitidos.
  - A data de retenção deve ser no futuro.
- `x-amz-object-lock-legal-hold`

  Se a retenção legal estiver LIGADA (diferencia maiúsculas de minúsculas), o objeto será colocado sob retenção legal. Se a retenção legal estiver DESLIGADA, nenhuma retenção legal será aplicada. Qualquer outro valor resulta em um erro 400 Bad Request (InvalidArgument).

Se você usar qualquer um desses cabeçalhos de solicitação, esteja ciente destas restrições:

- O `Content-MD5` o cabeçalho da solicitação é necessário se houver `x-amz-object-lock-*` O cabeçalho da solicitação está presente na solicitação PutObject. `Content-MD5` não é necessário para CopyObject ou CreateMultipartUpload.
- Se o bucket não tiver o S3 Object Lock habilitado e um `x-amz-object-lock-*` Se o cabeçalho da solicitação estiver presente, um erro 400 Bad Request (InvalidRequest) será retornado.

- A solicitação PutObject suporta o uso de `x-amz-storage-class: REDUCED_REDUNDANCY` para corresponder ao comportamento da AWS. No entanto, quando um objeto é ingerido em um bucket com o S3 Object Lock habilitado, o StorageGRID sempre executará uma ingestão de confirmação dupla.
- Uma resposta de versão GET ou HeadObject subsequente incluirá os cabeçalhos `x-amz-object-lock-mode` , `x-amz-object-lock-retain-until-date` , e `x-amz-object-lock-legal-hold` , se configurado e se o remetente da solicitação tiver o correto `s3:Get*` permissões.

Você pode usar o `s3:object-lock-remaining-retention-days` chave de condição de política para limitar os períodos mínimos e máximos de retenção permitidos para seus objetos.

Como atualizar as configurações de retenção de um objeto

Se precisar atualizar as configurações de retenção ou retenção legal para uma versão de objeto existente, você pode executar as seguintes operações de sub-recursos do objeto:

- `PutObjectLegalHold`

  Se o novo valor de retenção legal for LIGADO, o objeto será colocado sob retenção legal. Se o valor de retenção legal estiver DESLIGADO, a retenção legal será suspensa.

- `PutObjectRetention`
  - O valor do modo pode ser CONFORMIDADE ou GOVERNANÇA (diferencia maiúsculas de minúsculas).
  - O valor reter-até-data deve estar no formato `2020-08-10T21:46:00Z` . Segundos fracionários são permitidos, mas apenas 3 dígitos decimais são preservados (precisão de milissegundos). Outros formatos ISO 8601 não são permitidos.
  - Se uma versão do objeto tiver uma data de retenção existente, você só poderá aumentá-la. O novo valor deve estar no futuro.

Como usar o modo GOVERNANÇA

Usuários que possuem o `s3:BypassGovernanceRetention` a permissão pode ignorar as configurações de retenção ativas de um objeto que usa o modo GOVERNANCE. Qualquer operação DELETE ou PutObjectRetention deve incluir o `x-amz-bypass-governance-retention:true` cabeçalho da solicitação. Esses usuários podem executar estas operações adicionais:

- Execute as operações DeleteObject ou DeleteObjects para excluir uma versão do objeto antes que seu período de retenção termine.

  Objetos que estão sob retenção legal não podem ser excluídos. A retenção legal deve estar DESLIGADA.

- Execute operações PutObjectRetention que alterem o modo de versão de um objeto de GOVERNANCE para COMPLIANCE antes que o período de retenção do objeto tenha decorrido.

  Alterar o modo de CONFORMIDADE para GOVERNANÇA nunca é permitido.

- Execute operações PutObjectRetention para aumentar, diminuir ou remover o período de retenção de uma versão do objeto.

Informações relacionadas

- "Gerenciar objetos com o S3 Object Lock"

- "Use o S3 Object Lock para reter objetos"
- "Guia do usuário do Amazon Simple Storage Service: Bloqueio de objetos"

Criar configuração do ciclo de vida do S3

Você pode criar uma configuração de ciclo de vida do S3 para controlar quando objetos específicos são excluídos do sistema StorageGRID .

O exemplo simples nesta seção ilustra como uma configuração de ciclo de vida do S3 pode controlar quando determinados objetos são excluídos (expirados) de buckets específicos do S3. O exemplo nesta seção é apenas para fins ilustrativos. Para obter detalhes completos sobre a criação de configurações do ciclo de vida do S3, consulte "Guia do usuário do Amazon Simple Storage Service: gerenciamento do ciclo de vida do objeto" . Observe que o StorageGRID suporta apenas ações de expiração; ele não suporta ações de transição.

O que é configuração de ciclo de vida

Uma configuração de ciclo de vida é um conjunto de regras aplicadas aos objetos em buckets específicos do S3. Cada regra especifica quais objetos são afetados e quando esses objetos expirarão (em uma data específica ou após um determinado número de dias).

O StorageGRID suporta até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML:

- Expiração: Exclua um objeto quando uma data especificada for atingida ou quando um número especificado de dias for atingido, a partir do momento em que o objeto foi ingerido.
- NoncurrentVersionExpiration: Exclui um objeto quando um número especificado de dias é atingido, começando em quando o objeto se tornou não atual.
- Filtro (Prefixo, Tag)
- Status
- EU IA

Cada objeto segue as configurações de retenção de um ciclo de vida de bucket do S3 ou de uma política do ILM. Quando um ciclo de vida de bucket do S3 é configurado, as ações de expiração do ciclo de vida substituem a política do ILM para objetos que correspondem ao filtro de ciclo de vida do bucket. Objetos que não correspondem ao filtro de ciclo de vida do bucket usam as configurações de retenção da política do ILM. Se um objeto corresponder a um filtro de ciclo de vida de bucket e nenhuma ação de expiração for explicitamente especificada, as configurações de retenção da política ILM não serão usadas e ficará implícito que as versões do objeto serão retidas para sempre. Ver "Exemplo de prioridades para o ciclo de vida do bucket S3 e política de ILM" .

Como resultado, um objeto pode ser removido da grade mesmo que as instruções de posicionamento em uma regra ILM ainda se apliquem ao objeto. Ou um objeto pode ser retido na grade mesmo depois que quaisquer instruções de posicionamento do ILM para o objeto tenham expirado. Para obter detalhes, consulte "Como o ILM opera ao longo da vida de um objeto" .

> ⓘ A configuração do ciclo de vida do bucket pode ser usada com buckets que tenham o S3 Object Lock habilitado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis legados.

O StorageGRID oferece suporte ao uso das seguintes operações de bucket para gerenciar configurações de ciclo de vida:

- Ciclo de vida do DeleteBucket
- Obter configuração do ciclo de vida do Bucket
- Configuração do ciclo de vida do PutBucket

Criar configuração de ciclo de vida

Como primeira etapa na criação de uma configuração de ciclo de vida, você cria um arquivo JSON que inclui uma ou mais regras. Por exemplo, este arquivo JSON inclui três regras, como segue:

1. A regra 1 se aplica somente a objetos que correspondem ao prefixo `category1` / e que tenham uma `key2` valor de `tag2` . O `Expiration` O parâmetro especifica que os objetos que correspondem ao filtro expirarão à meia-noite de 22 de agosto de 2020.
2. A regra 2 se aplica somente a objetos que correspondem ao prefixo `category2` /. O `Expiration` O parâmetro especifica que os objetos que correspondem ao filtro expirarão 100 dias após serem ingeridos.

   > Regras que especificam um número de dias são relativas a quando o objeto foi ingerido. Se a data atual exceder a data de ingestão mais o número de dias, alguns objetos poderão ser removidos do bucket assim que a configuração do ciclo de vida for aplicada.

3. A regra 3 se aplica somente a objetos que correspondem ao prefixo `category3` /. O `Expiration` O parâmetro especifica que quaisquer versões não atuais de objetos correspondentes expirarão 50 dias após se tornarem não atuais.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Aplicar configuração de ciclo de vida ao bucket

Depois de criar o arquivo de configuração do ciclo de vida, aplique-o a um bucket emitindo uma solicitação PutBucketLifecycleConfiguration.

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

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar se uma configuração de ciclo de vida foi aplicada com sucesso ao bucket, emita uma solicitação GetBucketLifecycleConfiguration. Por exemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Uma resposta bem-sucedida lista a configuração do ciclo de vida que você acabou de aplicar.

Validar se a expiração do ciclo de vida do bucket se aplica ao objeto

Você pode determinar se uma regra de expiração na configuração do ciclo de vida se aplica a um objeto específico ao emitir uma solicitação PutObject, HeadObject ou GetObject. Se uma regra se aplicar, a resposta inclui uma `Expiration` parâmetro que indica quando o objeto expira e qual regra de expiração foi correspondida.

> Como o ciclo de vida do bucket substitui o ILM, o `expiry-date` é mostrada a data real em que o objeto será excluído. Para obter detalhes, consulte "Como a retenção de objetos é determinada" .

Por exemplo, esta solicitação PutObject foi emitida em 22 de junho de 2020 e coloca um objeto no `testbucket` balde.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

A resposta de sucesso indica que o objeto irá expirar em 100 dias (01 de outubro de 2020) e que correspondeu à Regra 2 da configuração do ciclo de vida.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Por exemplo, esta solicitação HeadObject foi usada para obter metadados para o mesmo objeto no bucket testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

A resposta de sucesso inclui os metadados do objeto e indica que o objeto irá expirar em 100 dias e que correspondeu à Regra 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Para buckets habilitados para controle de versão, o `x-amz-expiration` O cabeçalho de resposta se aplica somente às versões atuais dos objetos.

Recomendações para implementar a API REST do S3

Você deve seguir estas recomendações ao implementar a API REST do S3 para uso com o StorageGRID.

Recomendações para HEADs para objetos inexistentes

Se o seu aplicativo verifica rotineiramente se um objeto existe em um caminho onde você não espera que o objeto realmente exista, você deve usar o "Disponível""consistência" . Por exemplo, você deve usar a consistência "Disponível" se seu aplicativo fizer HEAD de um local antes de fazer PUT nele.

Caso contrário, se a operação HEAD não encontrar o objeto, você poderá receber um alto número de erros 500 do Servidor Interno se dois ou mais Nós de Armazenamento no mesmo site estiverem indisponíveis ou um site remoto estiver inacessível.

Você pode definir a consistência "Disponível" para cada bucket usando o"Consistência do balde PUT" solicitação, ou você pode especificar a consistência no cabeçalho da solicitação para uma operação de API

individual.

Recomendações para chaves de objeto

Siga estas recomendações para nomes de chaves de objeto, com base em quando o bucket foi criado pela primeira vez.

Buckets criados no StorageGRID 11.4 ou anterior

- Não use valores aleatórios como os quatro primeiros caracteres das chaves do objeto. Isso contrasta com a antiga recomendação da AWS para prefixos de chaves. Em vez disso, use prefixos não aleatórios e não exclusivos, como `image` .
- Se você seguir a antiga recomendação da AWS de usar caracteres aleatórios e exclusivos em prefixos de chave, prefixe as chaves de objeto com um nome de diretório. Ou seja, use este formato:

  `mybucket/mydir/f8e3-image3132.jpg`

  Em vez deste formato:

  `mybucket/f8e3-image3132.jpg`

Buckets criados no StorageGRID 11.4 ou posterior

Não é necessário restringir nomes de chaves de objetos para atender às melhores práticas de desempenho. Na maioria dos casos, você pode usar valores aleatórios para os quatro primeiros caracteres dos nomes das chaves do objeto.

> Uma exceção a isso é uma carga de trabalho do S3 que remove continuamente todos os objetos após um curto período de tempo. Para minimizar o impacto no desempenho deste caso de uso, varie uma parte inicial do nome da chave a cada vários milhares de objetos com algo como a data. Por exemplo, suponha que um cliente S3 normalmente grava 2.000 objetos/segundo e a política de ciclo de vida do ILM ou do bucket remove todos os objetos após três dias. Para minimizar o impacto no desempenho, você pode nomear as chaves usando um padrão como este: `/mybucket/mydir/`*`yyyymmddhhmmss-random_UUID`*`.jpg`

Recomendações para "leituras de intervalo"

Se o"opção global para compactar objetos armazenados" estiver habilitado, os aplicativos cliente S3 devem evitar executar operações GetObject que especifiquem um intervalo de bytes a serem retornados. Essas operações de "leitura de intervalo" são ineficientes porque o StorageGRID precisa descompactar efetivamente os objetos para acessar os bytes solicitados. Operações GetObject que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é ineficiente ler um intervalo de 10 MB de um objeto compactado de 50 GB.

Se os intervalos forem lidos de objetos compactados, as solicitações do cliente poderão expirar.

> Se você precisar compactar objetos e seu aplicativo cliente precisar usar leituras de intervalo, aumente o tempo limite de leitura do aplicativo.

Suporte para API REST do Amazon S3

Detalhes da implementação da API REST S3

O sistema StorageGRID implementa a API do Simple Storage Service (versão da API 2006-03-01) com suporte para a maioria das operações e com algumas limitações. Você precisa entender os detalhes de implementação ao integrar aplicativos cliente da API REST do S3.

O sistema StorageGRID oferece suporte a solicitações no estilo de hospedagem virtual e solicitações no estilo de caminho.

Manuseio de data

A implementação StorageGRID da API REST do S3 suporta apenas formatos de data HTTP válidos.

O sistema StorageGRID suporta apenas formatos de data HTTP válidos para quaisquer cabeçalhos que aceitem valores de data. A parte de hora da data pode ser especificada no formato Greenwich Mean Time (GMT) ou no formato Universal Coordinated Time (UTC) sem deslocamento de fuso horário (+0000 deve ser especificado). Se você incluir o `x-amz-date` cabeçalho na sua solicitação, ele substitui qualquer valor especificado no cabeçalho da solicitação Date. Ao usar o AWS Signature versão 4, o `x-amz-date` O cabeçalho deve estar presente na solicitação assinada porque o cabeçalho de data não é suportado.

Cabeçalhos de solicitação comuns

O sistema StorageGRID suporta os cabeçalhos de solicitação comuns definidos por "Referência da API do Amazon Simple Storage Service: Cabeçalhos de solicitação comuns" , com uma exceção.

Cabeçalho da solicitação	Implementação
Autorização	Suporte total para AWS Signature versão 2 Suporte para AWS Signature versão 4, com as seguintes exceções: • Quando você fornece o valor real da soma de verificação da carga útil em `x-amz-content-sha256` , o valor é aceito sem validação, como se o valor `UNSIGNED-PAYLOAD` tinha sido fornecido para o cabeçalho. Quando você fornece um `x-amz-content-sha256` valor do cabeçalho que implica `aws-chunked` streaming (por exemplo, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), as assinaturas dos blocos não são verificadas em relação aos dados dos blocos.
token de segurança x-amz	Não implementado. Devoluções `XNotImplemented` .

Cabeçalhos de resposta comuns

O sistema StorageGRID suporta todos os cabeçalhos de resposta comuns definidos pela *Simple Storage Service API Reference*, com uma exceção.

Cabeçalho de resposta	Implementação
x-amz-id-2	Não utilizado

Autenticar solicitações

O sistema StorageGRID oferece suporte ao acesso autenticado e anônimo a objetos usando a API S3.

A API do S3 oferece suporte ao Signature versão 2 e ao Signature versão 4 para autenticação de solicitações da API do S3.

Solicitações autenticadas devem ser assinadas usando seu ID de chave de acesso e sua chave de acesso secreta.

O sistema StorageGRID suporta dois métodos de autenticação: HTTP `Authorization` cabeçalho e usando parâmetros de consulta.

Use o cabeçalho de autorização HTTP

O HTTP `Authorization` O cabeçalho é usado por todas as operações da API do S3, exceto solicitações anônimas, quando permitido pela política de bucket. O `Authorization` O cabeçalho contém todas as informações de assinatura necessárias para autenticar uma solicitação.

Usar parâmetros de consulta

Você pode usar parâmetros de consulta para adicionar informações de autenticação a uma URL. Isso é conhecido como pré-assinatura de URL, que pode ser usado para conceder acesso temporário a recursos específicos. Usuários com a URL pré-assinada não precisam saber a chave de acesso secreta para acessar o recurso, o que permite que você forneça acesso restrito de terceiros a um recurso.

Operações no serviço

O sistema StorageGRID suporta as seguintes operações no serviço.

Operação	Implementação
ListBuckets (anteriormente chamado de Serviço GET)	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
Uso de armazenamento GET	O StorageGRID"Uso de armazenamento GET" A solicitação informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta. Esta é uma operação no serviço com um caminho de / e um parâmetro de consulta personalizado(`?x-ntap-sg-usage`) adicionado.
OPÇÕES /	Os aplicativos clientes podem emitir `OPTIONS /` solicitações para a porta S3 em um nó de armazenamento, sem fornecer credenciais de autenticação S3, para determinar se o nó de armazenamento está disponível. Você pode usar essa solicitação para monitoramento ou para permitir que balanceadores de carga externos identifiquem quando um nó de armazenamento está inativo.

Operações em baldes

O sistema StorageGRID suporta no máximo 5.000 buckets para cada conta de locatário do S3.

Cada grade pode ter no máximo 100.000 buckets.

Para dar suporte a 5.000 buckets, cada nó de armazenamento na grade deve ter no mínimo 64 GB de RAM.

As restrições de nome de bucket seguem as restrições de região padrão dos EUA da AWS, mas você deve restringi-las ainda mais às convenções de nomenclatura de DNS para oferecer suporte a solicitações de estilo de hospedagem virtual do S3.

Veja o seguinte para mais informações:

- "Guia do usuário do Amazon Simple Storage Service: cotas, restrições e limitações de bucket"
- "Configurar nomes de domínio de endpoint S3"

As operações ListObjects (GET Bucket) e ListObjectVersions (versões do objeto GET Bucket) oferecem suporte ao StorageGRID"valores de consistência" .

Você pode verificar se as atualizações do último horário de acesso estão habilitadas ou desabilitadas para buckets individuais. Ver "Último horário de acesso do Bucket GET" .

A tabela a seguir descreve como o StorageGRID implementa as operações de bucket da API REST do S3. Para executar qualquer uma dessas operações, é necessário fornecer as credenciais de acesso necessárias para a conta.

Operação	Implementação
CriarBucket	Cria um novo bucket. Ao criar o bucket, você se torna o proprietário do bucket. • Os nomes dos buckets devem obedecer às seguintes regras: ◦ Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário). ◦ Deve ser compatível com DNS. ◦ Deve conter no mínimo 3 e no máximo 63 caracteres. ◦ Pode ser uma série de um ou mais rótulos, com rótulos adjacentes separados por um ponto. Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hifens. ◦ Não deve parecer um endereço IP formatado em texto. ◦ Não deve usar pontos em solicitações de estilo de hospedagem virtual. Os períodos causarão problemas com a verificação do certificado curinga do servidor. • Por padrão, os buckets são criados no `us-east-1` região; no entanto, você pode usar o `LocationConstraint` elemento request no corpo da solicitação para especificar uma região diferente. Ao usar o `LocationConstraint` elemento, você deve especificar o nome exato de uma região que foi definida usando o Grid Manager ou a Grid Management API. Entre em contato com o administrador do sistema se você não souber o nome da região que deve usar. **Observação**: Ocorrerá um erro se sua solicitação CreateBucket usar uma região que não foi definida em StorageGRID. • Você pode incluir o `x-amz-bucket-object-lock-enabled` cabeçalho de solicitação para criar um bucket com o S3 Object Lock habilitado. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3" . Você deve habilitar o S3 Object Lock ao criar o bucket. Não é possível adicionar ou desabilitar o S3 Object Lock após a criação de um bucket. O S3 Object Lock requer controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.
ExcluirBucket	Exclui o bucket.
ExcluirBucketCors	Exclui a configuração CORS do bucket.
DeleteBucketEncryption	Exclui a criptografia padrão do bucket. Os objetos criptografados existentes permanecem criptografados, mas quaisquer novos objetos adicionados ao bucket não são criptografados.
Ciclo de vida do DeleteBucket	Exclui a configuração do ciclo de vida do bucket. Ver "Criar configuração do ciclo de vida do S3" .

Operação	Implementação
Política de exclusão de balde	Exclui a política anexada ao bucket.
DeleteBucketReplication	Exclui a configuração de replicação anexada ao bucket.
ExcluirBucketTagging	Usa o `tagging` sub-recurso para remover todas as tags de um bucket. **Cuidado**: Se uma tag de política ILM não padrão for definida para este bucket, haverá um `NTAP-SG-ILM-BUCKET-TAG` tag de bucket com um valor atribuído a ela. Não emita uma solicitação DeleteBucketTagging se houver um `NTAP-SG-ILM-BUCKET-TAG` etiqueta de balde. Em vez disso, emita uma solicitação PutBucketTagging apenas com o `NTAP-SG-ILM-BUCKET-TAG` tag e seu valor atribuído para remover todas as outras tags do bucket. Não modifique ou remova o `NTAP-SG-ILM-BUCKET-TAG` etiqueta de balde.
ObterBucketAcl	Retorna uma resposta positiva e o ID, DisplayName e Permissão do proprietário do bucket, indicando que o proprietário tem acesso total ao bucket.
ObterBucketCors	Retorna o `cors` configuração para o bucket.
Obter criptografia do Bucket	Retorna a configuração de criptografia padrão para o bucket.
Obter configuração do ciclo de vida do Bucket (anteriormente chamado de ciclo de vida do GET Bucket)	Retorna a configuração do ciclo de vida do bucket. Ver "Criar configuração do ciclo de vida do S3" .
ObterBucketLocation	Retorna a região que foi definida usando o `LocationConstraint` elemento na solicitação CreateBucket. Se a região do balde for `us-east-1` , uma string vazia é retornada para a região.
Obter configuração de notificação de bucket (anteriormente chamado de notificação GET Bucket)	Retorna a configuração de notificação anexada ao bucket.
ObterBucketPolicy	Retorna a política anexada ao bucket.
Obter replicação do Bucket	Retorna a configuração de replicação anexada ao bucket.

Operação	Implementação
Obter marcação de balde	Usa o `tagging` sub-recurso para retornar todas as tags de um bucket. **Cuidado**: Se uma tag de política ILM não padrão for definida para este bucket, haverá um `NTAP-SG-ILM-BUCKET-TAG` tag de bucket com um valor atribuído a ela. Não modifique ou remova esta tag.
ObterVersionamento doBucket	Esta implementação utiliza o `versioning` sub-recurso para retornar o estado de controle de versão de um bucket. • *blank*: O controle de versão nunca foi habilitado (o bucket é "Sem versão") • Habilitado: o controle de versão está habilitado • Suspenso: o controle de versão foi habilitado anteriormente e está suspenso
ObterConfiguraçãoObject Lock	Retorna o modo de retenção padrão do bucket e o período de retenção padrão, se configurado. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3" .
Balde de cabeça	Determina se um bucket existe e se você tem permissão para acessá-lo. Esta operação retorna: • `x-ntap-sg-bucket-id`: O UUID do bucket no formato UUID. • `x-ntap-sg-trace-id`: O ID de rastreamento exclusivo da solicitação associada.
ListObjects e ListObjectsV2 (anteriormente chamado de GET Bucket)	Retorna alguns ou todos (até 1.000) objetos em um bucket. A classe de armazenamento para objetos pode ter um dos dois valores, mesmo que o objeto tenha sido ingerido com o `REDUCED_REDUNDANCY` opção de classe de armazenamento: • `STANDARD`, que indica que o objeto está armazenado em um pool de armazenamento composto por nós de armazenamento. • `GLACIER`, que indica que o objeto foi movido para o bucket externo especificado pelo Cloud Storage Pool. Se o bucket contiver um grande número de chaves excluídas com o mesmo prefixo, a resposta poderá incluir algumas `CommonPrefixes` que não contêm chaves.
Versões do objeto de lista (anteriormente chamadas de versões do objeto GET Bucket)	Com acesso READ em um bucket, usando esta operação com o `versions` subresource lista metadados de todas as versões de objetos no bucket.

Operação	Implementação
ColoqueBucketCors	Define a configuração CORS para um bucket para que o bucket possa atender a solicitações de origem cruzada. O compartilhamento de recursos entre origens (CORS) é um mecanismo de segurança que permite que aplicativos web clientes em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket S3 chamado `images` para armazenar gráficos. Ao definir a configuração CORS para o `images` bucket, você pode permitir que as imagens nesse bucket sejam exibidas no site `http://www.example.com` .
PutBucketEncryption	Define o estado de criptografia padrão de um bucket existente. Quando a criptografia em nível de bucket está habilitada, todos os novos objetos adicionados ao bucket são criptografados. O StorageGRID oferece suporte à criptografia do lado do servidor com chaves gerenciadas StorageGRID. Ao especificar a regra de configuração de criptografia do lado do servidor, defina o `SSEAlgorithm` parâmetro para `AES256` , e não use o `KMSMasterKeyID` parâmetro. A configuração de criptografia padrão do bucket será ignorada se a solicitação de upload do objeto já especificar a criptografia (ou seja, se a solicitação incluir o `x-amz-server-side-encryption-*` cabeçalho da solicitação).
Configuração do ciclo de vida do PutBucket (anteriormente chamado de ciclo de vida do PUT Bucket)	Cria uma nova configuração de ciclo de vida para o bucket ou substitui uma configuração de ciclo de vida existente. O StorageGRID suporta até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML: • Expiração (Dias, Data, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtro (Prefixo, Tag) • Status • EU IA O StorageGRID não oferece suporte a estas ações: • AbortarIncompletoMultipartUpload • Transição Ver "Criar configuração do ciclo de vida do S3" . Para entender como a ação Expiração em um ciclo de vida de bucket interage com as instruções de posicionamento do ILM, consulte"Como o ILM opera ao longo da vida de um objeto" . **Observação**: a configuração do ciclo de vida do bucket pode ser usada com buckets que tenham o S3 Object Lock habilitado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis legados.

Operação	Implementação

Configuração de notificação PutBucket
 	
(anteriormente chamado de notificação PUT Bucket)
	Configura notificações para o bucket usando o XML de configuração de notificação incluído no corpo da solicitação. Você deve estar ciente dos seguintes detalhes de implementação:
	
	• O StorageGRID oferece suporte ao Amazon Simple Notification Service (Amazon SNS) ou a tópicos do Kafka como destinos. Os endpoints do Simple Queue Service (SQS) ou do Amazon Lambda não são suportados.
	• O destino das notificações deve ser especificado como o URN de um ponto de extremidade do StorageGRID . Os endpoints podem ser criados usando o Tenant Manager ou a Tenant Management API.
	
	O ponto de extremidade deve existir para que a configuração da notificação seja bem-sucedida. Se o ponto final não existir, um `400 Bad Request` erro é retornado com o código `InvalidArgument` .
	
	• Não é possível configurar uma notificação para os seguintes tipos de eventos. Esses tipos de eventos **não** são suportados.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• As notificações de eventos enviadas do StorageGRID usam o formato JSON padrão, exceto que elas não incluem algumas chaves e usam valores específicos para outras, conforme mostrado na lista a seguir:
	◦ **fonte do evento**
	
	`sgws:s3`
	
	◦ **Região aws**
	
	não incluído
	
	◦ **x-amz-id-2**
	
	não incluído
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	Define a política anexada ao bucket. Ver "Use políticas de acesso a buckets e grupos" .

Operação	Implementação
PutBucketReplicação	Configura"Replicação do StorageGRID CloudMirror" para o bucket usando o XML de configuração de replicação fornecido no corpo da solicitação. Para replicação do CloudMirror, você deve estar ciente dos seguintes detalhes de implementação: • O StorageGRID suporta apenas a V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue as convenções V1 para exclusão de versões de objetos. Para mais detalhes, veja "Guia do usuário do Amazon Simple Storage Service: configuração de replicação" . • A replicação de buckets pode ser configurada em buckets versionados ou não versionados. • Você pode especificar um bucket de destino diferente em cada regra do XML de configuração de replicação. Um bucket de origem pode ser replicado para mais de um bucket de destino. • Os buckets de destino devem ser especificados como o URN dos endpoints do StorageGRID , conforme especificado no Tenant Manager ou na Tenant Management API. Ver "Configurar a replicação do CloudMirror" . O ponto de extremidade deve existir para que a configuração da replicação seja bem-sucedida. Se o ponto final não existir, a solicitação falhará como um `400 Bad Request` . A mensagem de erro diz: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Você não precisa especificar um `Role` no XML de configuração. Este valor não é usado pelo StorageGRID e será ignorado se enviado. • Se você omitir a classe de armazenamento do XML de configuração, o StorageGRID usará o `STANDARD` classe de armazenamento por padrão. • Se você excluir um objeto do bucket de origem ou excluir o próprio bucket de origem, o comportamento de replicação entre regiões será o seguinte: ◦ Se você excluir o objeto ou bucket antes que ele seja replicado, o objeto/bucket não será replicado e você não será notificado. ◦ Se você excluir o objeto ou bucket após ele ter sido replicado, o StorageGRID seguirá o comportamento de exclusão padrão do Amazon S3 para a V1 da replicação entre regiões.

Operação	Implementação
Colocar marcação de balde	Usa o `tagging` sub-recurso para adicionar ou atualizar um conjunto de tags para um bucket. Ao adicionar tags de bucket, esteja ciente das seguintes limitações: • Tanto o StorageGRID quanto o Amazon S3 suportam até 50 tags para cada bucket. • As tags associadas a um bucket devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento. • Os valores das tags podem ter até 256 caracteres Unicode. • Chaves e valores diferenciam maiúsculas de minúsculas. **Cuidado**: Se uma tag de política ILM não padrão for definida para este bucket, haverá um `NTAP-SG-ILM-BUCKET-TAG` tag de bucket com um valor atribuído a ela. Certifique-se de que o `NTAP-SG-ILM-BUCKET-TAG` A tag bucket é incluída com o valor atribuído em todas as solicitações PutBucketTagging. Não modifique ou remova esta tag. **Observação**: esta operação substituirá quaisquer tags atuais que o bucket já tenha. Se alguma tag existente for omitida do conjunto, essas tags serão removidas do bucket.
Versão PutBucket	Usa o `versioning` sub-recurso para definir o estado de controle de versão de um bucket existente. Você pode definir o estado de controle de versão com um dos seguintes valores: • Habilitado: habilita o controle de versão para os objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo. • Suspenso: desabilita o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão `null` .
PutObjectLockConfiguration	Configura ou remove o modo de retenção padrão do bucket e o período de retenção padrão. Se o período de retenção padrão for modificado, a data de retenção das versões de objetos existentes permanecerá a mesma e não será recalculada usando o novo período de retenção padrão. Ver"Use a API REST do S3 para configurar o bloqueio de objeto do S3" para informações detalhadas.

Operações em objetos

Operações em objetos

Esta seção descreve como o sistema StorageGRID implementa operações da API REST do S3 para objetos.

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

- StorageGRID"valores de consistência" são suportados por todas as operações em objetos, com exceção das seguintes:
  - ObterAclObjeto
  - `OPTIONS /`
  - ColocarObjetoLegalHold
  - ColocarRetençãoDeObjeto
  - SelecionarObjetoConteúdo
- Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.
- Todos os objetos em um bucket StorageGRID são de propriedade do proprietário do bucket, incluindo objetos criados por um usuário anônimo ou por outra conta.
- Objetos de dados ingeridos no sistema StorageGRID por meio do Swift não podem ser acessados pelo S3.

A tabela a seguir descreve como o StorageGRID implementa operações de objeto da API REST do S3.

Operação	Implementação
ExcluirObjeto	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. Ao processar uma solicitação DeleteObject, o StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais armazenados. Se bem-sucedido, o StorageGRID retornará uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas em 30 segundos (por exemplo, porque um local está temporariamente indisponível), o StorageGRID enfileira as cópias para remoção e então indica o sucesso ao cliente. **Controle de versão** Para remover uma versão específica, o solicitante deve ser o proprietário do bucket e usar o `versionId` sub-recurso. Usar este sub-recurso exclui permanentemente a versão. Se o `versionId` corresponde a um marcador de exclusão, o cabeçalho de resposta `x-amz-delete-marker` é retornado definido para `true` . • Se um objeto for excluído sem o `versionId` sub-recurso em um bucket com controle de versão habilitado, isso resulta na geração de um marcador de exclusão. O `versionId` para o marcador de exclusão é retornado usando o `x-amz-version-id` cabeçalho de resposta e o `x-amz-delete-marker` o cabeçalho de resposta é retornado definido como `true` . • Se um objeto for excluído sem o `versionId` sub-recurso em um bucket com controle de versão suspenso, isso resulta em uma exclusão permanente de uma versão 'nula' já existente ou de um marcador de exclusão 'nulo' e na geração de um novo marcador de exclusão 'nulo'. O `x-amz-delete-marker` o cabeçalho de resposta é retornado definido como `true` . **Observação**: Em certos casos, podem existir vários marcadores de exclusão para um objeto. Ver"Use a API REST do S3 para configurar o bloqueio de objeto do S3" para aprender como excluir versões de objetos no modo GOVERNANCE.
ExcluirObjetos (anteriormente chamado de DELETE Multiple Objects)	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. Vários objetos podem ser excluídos na mesma mensagem de solicitação. Ver"Use a API REST do S3 para configurar o bloqueio de objeto do S3" para aprender como excluir versões de objetos no modo GOVERNANCE.

Operação	Implementação
ExcluirMarcaçãoDeObjeto	Usa o `tagging` sub-recurso para remover todas as tags de um objeto. **Controle de versão** Se o `versionId` se o parâmetro de consulta não for especificado na solicitação, a operação excluirá todas as tags da versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status "MethodNotAllowed" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true` .
ObterObjeto	"ObterObjeto"
ObterAclObjeto	Se as credenciais de acesso necessárias forem fornecidas para a conta, a operação retornará uma resposta positiva e o ID, o DisplayName e a Permissão do proprietário do objeto, indicando que o proprietário tem acesso total ao objeto.
ObterObjetoLegalHold	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"
ObterRetençãoDeObjeto	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"
Obter marcação de objeto	Usa o `tagging` sub-recurso para retornar todas as tags de um objeto. **Controle de versão** Se o `versionId` se o parâmetro de consulta não for especificado na solicitação, a operação retornará todas as tags da versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status "MethodNotAllowed" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true` .
CabeçaObjeto	"CabeçaObjeto"
RestaurarObjeto	"RestaurarObjeto"
ColocarObjeto	"ColocarObjeto"
CopiarObjeto (anteriormente chamado de Objeto PUT - Copiar)	"CopiarObjeto"
ColocarObjetoLegalHold	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"
ColocarRetençãoDeObjeto	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"

Operação	Implementação
Colocar marcação de objeto	Usa o `tagging` sub-recurso para adicionar um conjunto de tags a um objeto existente. **Limites de tags de objeto** Você pode adicionar tags a novos objetos ao carregá-los ou adicioná-las a objetos existentes. Tanto o StorageGRID quanto o Amazon S3 suportam até 10 tags para cada objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento e os valores de tag podem ter até 256 caracteres Unicode de comprimento. Chaves e valores diferenciam maiúsculas de minúsculas. **Atualizações de tags e comportamento de ingestão** Quando você usa PutObjectTagging para atualizar as tags de um objeto, o StorageGRID não ingere novamente o objeto. Isso significa que a opção para Comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento do objeto que sejam acionadas pela atualização são feitas quando o ILM é reavaliado pelos processos normais de ILM em segundo plano. Isso significa que, se a regra ILM usar a opção Estrita para comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objetos necessários não puderem ser feitos (por exemplo, porque um local recém-necessário não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível. **Resolução de conflitos** Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação. **Controle de versão** Se o `versionId` o parâmetro de consulta não é especificado na solicitação, a operação adiciona tags à versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status "MethodNotAllowed" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true` .
SelecionarObjetoConteúdo	"SelecionarObjetoConteúdo"

Use o S3 Select

O StorageGRID oferece suporte às seguintes cláusulas, tipos de dados e operadores do Amazon S3 Select para o"Comando SelectObjectContent" .

Itens não listados não são suportados.

Para sintaxe, veja"SelecionarObjetoConteúdo" . Para obter mais informações sobre o S3 Select, consulte o "Documentação da AWS para S3 Select" .

Somente contas de locatários que tenham o S3 Select habilitado podem emitir consultas SelectObjectContent. Veja o"considerações e requisitos para usar o S3 Select" .

Cláusulas

- Lista SELECIONAR
- cláusula FROM
- Cláusula WHERE
- Cláusula LIMIT

Tipos de dados

- bool
- inteiro
- corda
- flutuador
- decimal, numérico
- carimbo de data/hora

Operadores

Operadores lógicos

- E
- NÃO
- OU

Operadores de comparação

- <
- >
- ⇐
- >=
- =
- =
- <>
- !=
- ENTRE
- EM

Operadores de correspondência de padrões

- COMO
- _
- %

Operadores unitários

- É NULO
- NÃO É NULO

Operadores matemáticos

- +
- -
- *
- /
- %

O StorageGRID segue a precedência do operador Amazon S3 Select.

Funções agregadas

- MÉDIA()
- CONTAR(*)
- MÁXIMO()
- MÍNIMO()
- SOMA()

Funções condicionais

- CASO
- COALESCE
- NULLIF

Funções de conversão

- CAST (para tipo de dados suportado)

Funções de data

- DATA_ADICIONADA
- DATA_DIFF
- EXTRAIR
- PARA_STRING
- PARA_CARIMBO_DE_HORA

- UTCNOW

Funções de string

- COMPRIMENTO_CARACTERE, COMPRIMENTO_CARACTERE
- MAIS BAIXO
- SUBSTRING
- APARAR
- SUPERIOR

Use criptografia do lado do servidor

A criptografia do lado do servidor permite que você proteja os dados do seu objeto em repouso. O StorageGRID criptografa os dados enquanto grava o objeto e descriptografa os dados quando você acessa o objeto.

Se você quiser usar a criptografia do lado do servidor, poderá escolher uma das duas opções mutuamente exclusivas, com base em como as chaves de criptografia são gerenciadas:

- **SSE (criptografia do lado do servidor com chaves gerenciadas StorageGRID)**: quando você emite uma solicitação S3 para armazenar um objeto, o StorageGRID criptografa o objeto com uma chave exclusiva. Quando você emite uma solicitação S3 para recuperar o objeto, o StorageGRID usa a chave armazenada para descriptografar o objeto.
- **SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente)**: Quando você emite uma solicitação S3 para armazenar um objeto, você fornece sua própria chave de criptografia. Ao recuperar um objeto, você fornece a mesma chave de criptografia como parte de sua solicitação. Se as duas chaves de criptografia corresponderem, o objeto será descriptografado e os dados do objeto serão retornados.

  Embora o StorageGRID gerencie todas as operações de criptografia e descriptografia de objetos, você deve gerenciar as chaves de criptografia fornecidas.

  > As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente.

  > Se um objeto for criptografado com SSE ou SSE-C, todas as configurações de criptografia em nível de bucket ou de grade serão ignoradas.

Usar SSE

Para criptografar um objeto com uma chave exclusiva gerenciada pelo StorageGRID, use o seguinte cabeçalho de solicitação:

```
x-amz-server-side-encryption
```

O cabeçalho de solicitação SSE é suportado pelas seguintes operações de objeto:

- "ColocarObjeto"
- "CopiarObjeto"

- "CriarMultipartUpload"

Usar SSE-C

Para criptografar um objeto com uma chave exclusiva que você gerencia, use três cabeçalhos de solicitação:

Cabeçalho da solicitação	Descrição
`x-amz-server-side-encryption-customer-algorithm`	Especifique o algoritmo de criptografia. O valor do cabeçalho deve ser `AES256`.
`x-amz-server-side-encryption-customer-key`	Especifique a chave de criptografia que será usada para criptografar ou descriptografar o objeto. O valor da chave deve ser de 256 bits, codificado em base64.
`x-amz-server-side-encryption-customer-key-MD5`	Especifique o resumo MD5 da chave de criptografia de acordo com o RFC 1321, que é usado para garantir que a chave de criptografia foi transmitida sem erros. O valor do resumo MD5 deve ser codificado em base64 de 128 bits.

Os cabeçalhos de solicitação SSE-C são suportados pelas seguintes operações de objeto:

- "ObterObjeto"
- "CabeçaObjeto"
- "ColocarObjeto"
- "CopiarObjeto"
- "CriarMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Considerações sobre o uso de criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Antes de usar o SSE-C, esteja ciente das seguintes considerações:

- Você deve usar https.

> O StorageGRID rejeita quaisquer solicitações feitas via http ao usar SSE-C. Por questões de segurança, considere que qualquer chave enviada acidentalmente via http estará comprometida. Descarte a chave e gire conforme apropriado.

- O ETag na resposta não é o MD5 dos dados do objeto.
- Você deve gerenciar o mapeamento de chaves de criptografia para objetos. O StorageGRID não armazena chaves de criptografia. Você é responsável por rastrear a chave de criptografia fornecida para cada objeto.
- Se o seu bucket tiver controle de versão habilitado, cada versão do objeto deverá ter sua própria chave de criptografia. Você é responsável por rastrear a chave de criptografia usada para cada versão do objeto.

- Como você gerencia chaves de criptografia no lado do cliente, também deve gerenciar quaisquer proteções adicionais, como rotação de chaves, no lado do cliente.

> As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente.

- Se a replicação entre grades ou a replicação do CloudMirror estiver configurada para o bucket, você não poderá ingerir objetos SSE-C. A operação de ingestão falhará.

Informações relacionadas

"Guia do usuário do Amazon S3: usando criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)"

CopiarObjeto

Você pode usar a solicitação S3 CopyObject para criar uma cópia de um objeto que já está armazenado no S3. Uma operação CopyObject é o mesmo que executar GetObject seguido de PutObject.

Resolver conflitos

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

Tamanho do objeto

O tamanho máximo *recomendado* para uma única operação PutObject é 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use"upload multiparte" em vez de.

O tamanho máximo *compatível* para uma única operação PutObject é 5 TiB (5.497.558.138.880 bytes).

> Se você atualizou do StorageGRID 11.6 ou anterior, o alerta de tamanho de objeto S3 PUT muito grande será acionado se você tentar carregar um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11.7 ou 11.8, o alerta não será acionado neste caso. No entanto, para se alinhar ao padrão AWS S3, versões futuras do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

Caracteres UTF-8 em metadados do usuário

Se uma solicitação incluir valores UTF-8 (sem escape) no nome da chave ou no valor dos metadados definidos pelo usuário, o comportamento do StorageGRID será indefinido.

O StorageGRID não analisa nem interpreta caracteres UTF-8 de escape incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Caracteres UTF-8 escapados são tratados como caracteres ASCII:

- As solicitações serão bem-sucedidas se os metadados definidos pelo usuário incluírem caracteres UTF-8 de escape.
- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome da chave ou valor incluir caracteres não imprimíveis.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, seguido por um par nome-valor contendo metadados definidos pelo usuário
- `x-amz-metadata-directive`: O valor padrão é `COPY` , que permite copiar o objeto e os metadados associados.

  Você pode especificar `REPLACE` para substituir os metadados existentes ao copiar o objeto ou para atualizar os metadados do objeto.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: O valor padrão é `COPY` , que permite copiar o objeto e todas as tags.

  Você pode especificar `REPLACE` para substituir as tags existentes ao copiar o objeto ou para atualizar as tags.

- Cabeçalhos de solicitação de bloqueio de objeto S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular o modo de versão do objeto e reter até a data. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3" .

- Cabeçalhos de solicitação SSE:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    VerCabeçalhos de solicitação para criptografia do lado do servidor

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

  Quando você copia um objeto, se o objeto de origem tiver uma soma de verificação, o StorageGRID não copia esse valor de soma de verificação para o novo objeto. Este comportamento se aplica independentemente de você tentar usar ou não `x-amz-checksum-algorithm` na solicitação do objeto.

- `x-amz-website-redirect-location`

Opções de classe de armazenamento

O `x-amz-storage-class` O cabeçalho de solicitação é suportado e afeta quantas cópias de objeto o StorageGRID cria se a regra ILM correspondente usa o Dual commit ou Balanced"opção de ingestão" .

- `STANDARD`

  (Padrão) Especifica uma operação de ingestão de confirmação dupla quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

- `REDUCED_REDUNDANCY`

  Especifica uma operação de ingestão de confirmação única quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

  > Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Usando x-amz-copy-source em CopyObject

Se o bucket de origem e a chave, especificados no `x-amz-copy-source` cabeçalho, são diferentes do bucket de destino e da chave, uma cópia dos dados do objeto de origem é gravada no destino.

Se a origem e o destino corresponderem, e o `x-amz-metadata-directive` cabeçalho é especificado como `REPLACE` , os metadados do objeto são atualizados com os valores de metadados fornecidos na solicitação. Nesse caso, o StorageGRID não ingere novamente o objeto. Isto tem duas consequências importantes:

- Você não pode usar CopyObject para criptografar um objeto existente no local ou para alterar a criptografia de um objeto existente no local. Se você fornecer o `x-amz-server-side-encryption` cabeçalho ou o `x-amz-server-side-encryption-customer-algorithm` cabeçalho, StorageGRID

rejeita a solicitação e retorna `XNotImplemented` .

- A opção para Comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento do objeto que sejam acionadas pela atualização são feitas quando o ILM é reavaliado pelos processos normais de ILM em segundo plano.

  Isso significa que, se a regra ILM usar a opção Estrita para comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objetos necessários não puderem ser feitos (por exemplo, porque um local recém-necessário não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível.

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você"usar criptografia do lado do servidor" , os cabeçalhos de solicitação que você fornece dependem se o objeto de origem está criptografado e se você planeja criptografar o objeto de destino.

- Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deverá incluir os três cabeçalhos a seguir na solicitação CopyObject para que o objeto possa ser descriptografado e copiado:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especifique `AES256` .
  - `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia que você forneceu quando criou o objeto de origem.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu quando criou o objeto de origem.
- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva que você fornece e gerencia, inclua os três cabeçalhos a seguir:
  - `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Especifique uma nova chave de criptografia para o objeto de destino.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da nova chave de criptografia.

  > As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para"usando criptografia do lado do servidor" .

- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva gerenciada pelo StorageGRID (SSE), inclua este cabeçalho na solicitação CopyObject:
  - `x-amz-server-side-encryption`

  > O `server-side-encryption` o valor do objeto não pode ser atualizado. Em vez disso, faça uma cópia com um novo `server-side-encryption` valor usando `x-amz-metadata-directive` : `REPLACE` .

Controle de versão

Se o bucket de origem for versionado, você pode usar o `x-amz-copy-source` cabeçalho para copiar a

versão mais recente de um objeto. Para copiar uma versão específica de um objeto, você deve especificar explicitamente a versão a ser copiada usando o `versionId` sub-recurso. Se o bucket de destino for versionado, a versão gerada será retornada no `x-amz-version-id` cabeçalho de resposta. Se o controle de versão for suspenso para o bucket de destino, então `x-amz-version-id` retorna um valor "nulo".

ObterObjeto

Você pode usar a solicitação S3 GetObject para recuperar um objeto de um bucket S3.

GetObject e objetos multipartes

Você pode usar o `partNumber` parâmetro de solicitação para recuperar uma parte específica de um objeto multiparte ou segmentado. O `x-amz-mp-parts-count` O elemento de resposta indica quantas partes o objeto possui.

Você pode definir `partNumber` para 1 para objetos segmentados/multipartes e objetos não segmentados/não multipartes; no entanto, o `x-amz-mp-parts-count` O elemento de resposta é retornado somente para objetos segmentados ou multipartes.

Caracteres UTF-8 em metadados do usuário

O StorageGRID não analisa nem interpreta caracteres UTF-8 de escape em metadados definidos pelo usuário. As solicitações GET para um objeto com caracteres UTF-8 de escape em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome da chave ou valor incluir caracteres não imprimíveis.

Cabeçalho de solicitação suportado

O seguinte cabeçalho de solicitação é suportado:

- `x-amz-checksum-mode`: Especifique `ENABLED`

  O `Range` cabeçalho não é suportado com `x-amz-checksum-mode` para GetObject. Quando você inclui `Range` no pedido com `x-amz-checksum-mode` habilitado, o StorageGRID não retorna um valor de soma de verificação na resposta.

Cabeçalho de solicitação não suportado

O seguinte cabeçalho de solicitação não é suportado e retorna `XNotImplemented` :

- `x-amz-website-redirect-location`

Controle de versão

Se um `versionId` sub-recurso não for especificado, a operação buscará a versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status "Não encontrado" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true` .

Cabeçalhos de solicitação para criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use todos os três cabeçalhos se o objeto estiver criptografado com uma chave exclusiva fornecida por você.

- `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256` .
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do objeto.

> As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em"Use criptografia do lado do servidor" .

Comportamento de GetObject para objetos do Cloud Storage Pool

Se um objeto foi armazenado em um"Pool de armazenamento em nuvem" , o comportamento de uma solicitação GetObject depende do estado do objeto. Ver"CabeçaObjeto" para mais detalhes.

> Se um objeto estiver armazenado em um Cloud Storage Pool e uma ou mais cópias do objeto também existirem na grade, as solicitações GetObject tentarão recuperar dados da grade antes de recuperá-los do Cloud Storage Pool.

Estado do objeto	Comportamento de GetObject
Objeto ingerido no StorageGRID , mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de armazenamento tradicional ou usando codificação de eliminação	`200 OK` Uma cópia do objeto é recuperada.
Objeto no Cloud Storage Pool, mas ainda não transitado para um estado não recuperável	`200 OK` Uma cópia do objeto é recuperada.
Objeto transitado para um estado não recuperável	`403 Forbidden` , `InvalidObjectState` Use um"RestaurarObjeto" solicitação para restaurar o objeto a um estado recuperável.
Objeto em processo de restauração de um estado não recuperável	`403 Forbidden` , `InvalidObjectState` Aguarde a conclusão da solicitação RestoreObject.
Objeto totalmente restaurado no Cloud Storage Pool	`200 OK` Uma cópia do objeto é recuperada.

Objetos multipartes ou segmentados em um pool de armazenamento em nuvem

Se você carregou um objeto multiparte ou se o StorageGRID dividiu um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no Cloud Storage Pool por meio da amostragem de um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação GetObject pode retornar

incorretamente `200 OK` quando algumas partes do objeto já foram transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não foram restauradas.

Nestes casos:

- A solicitação GetObject pode retornar alguns dados, mas parar no meio da transferência.
- Uma solicitação GetObject subsequente pode retornar `403 Forbidden` .

GetObject e replicação entre grades

Se você estiver usando"federação de grade" e"replicação entre grades" estiver habilitado para um bucket, o cliente S3 poderá verificar o status de replicação de um objeto emitindo uma solicitação GetObject. A resposta inclui o StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta, que terá um dos seguintes valores:

Grade	Status de replicação
Fonte	• **CONCLUÍDO**: A replicação foi bem-sucedida. • **PENDENTE**: O objeto ainda não foi replicado. • **FALHA**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	**REPLICA**: O objeto foi replicado da grade de origem.

> ⓘ O StorageGRID não oferece suporte a `x-amz-replication-status` cabeçalho.

CabeçaObjeto

Você pode usar a solicitação S3 HeadObject para recuperar metadados de um objeto sem retornar o próprio objeto. Se o objeto estiver armazenado em um Cloud Storage Pool, você poderá usar o HeadObject para determinar o estado de transição do objeto.

HeadObject e objetos multipartes

Você pode usar o `partNumber` parâmetro de solicitação para recuperar metadados para uma parte específica de um objeto multiparte ou segmentado. O `x-amz-mp-parts-count` O elemento de resposta indica quantas partes o objeto possui.

Você pode definir `partNumber` para 1 para objetos segmentados/multipartes e objetos não segmentados/não multipartes; no entanto, o `x-amz-mp-parts-count` O elemento de resposta é retornado somente para objetos segmentados ou multipartes.

Caracteres UTF-8 em metadados do usuário

O StorageGRID não analisa nem interpreta caracteres UTF-8 de escape em metadados definidos pelo usuário. As solicitações HEAD para um objeto com caracteres UTF-8 escapados em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome da chave ou valor incluir caracteres não imprimíveis.

Cabeçalho de solicitação suportado

O seguinte cabeçalho de solicitação é suportado:

- `x-amz-checksum-mode`

  O `partNumber` parâmetro e `Range` cabeçalho não é suportado com `x-amz-checksum-mode` para HeadObject. Quando você os inclui na solicitação com `x-amz-checksum-mode` habilitado, o StorageGRID não retorna um valor de soma de verificação na resposta.

Cabeçalho de solicitação não suportado

O seguinte cabeçalho de solicitação não é suportado e retorna `XNotImplemented` :

- `x-amz-website-redirect-location`

Controle de versão

Se um `versionId` sub-recurso não for especificado, a operação buscará a versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status "Não encontrado" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true` .

Cabeçalhos de solicitação para criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use todos esses três cabeçalhos se o objeto estiver criptografado com uma chave exclusiva fornecida por você.

- `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256` .
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do objeto.

> ⚠ As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em"Use criptografia do lado do servidor" .

Respostas do HeadObject para objetos do Cloud Storage Pool

Se o objeto for armazenado em um"Pool de armazenamento em nuvem" , os seguintes cabeçalhos de resposta são retornados:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Os cabeçalhos de resposta fornecem informações sobre o estado de um objeto à medida que ele é movido para um pool de armazenamento em nuvem, opcionalmente transferido para um estado não recuperável e restaurado.

Estado do objeto	Resposta ao HeadObject
Objeto ingerido no StorageGRID , mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de armazenamento tradicional ou usando codificação de eliminação	`200 OK`(Nenhum cabeçalho de resposta especial é retornado.)

Objeto no Cloud Storage Pool, mas ainda não transitado para um estado não recuperável	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Até que o objeto seja transferido para um estado não recuperável, o valor para `expiry-date` está definido para um tempo distante no futuro. O tempo exato da transição não é controlado pelo sistema StorageGRID .

O objeto passou para um estado não recuperável, mas pelo menos uma cópia também existe na grade	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	O valor para `expiry-date` está definido para um tempo distante no futuro.
	
	Observação: Se a cópia na grade não estiver disponível (por exemplo, um nó de armazenamento estiver inativo), você deverá emitir uma"RestaurarObjeto" solicite a restauração da cópia do Cloud Storage Pool antes de poder recuperar o objeto com sucesso.

O objeto passou para um estado não recuperável e não há nenhuma cópia na grade	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objeto em processo de restauração de um estado não recuperável	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Estado do objeto	Resposta ao HeadObject

Objeto totalmente restaurado no Cloud Storage Pool	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	O `expiry-date` indica quando o objeto no Cloud Storage Pool será retornado a um estado não recuperável.

Objetos multipartes ou segmentados no Cloud Storage Pool

Se você carregou um objeto multiparte ou se o StorageGRID dividiu um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no Cloud Storage Pool por meio da amostragem de um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação HeadObject pode retornar incorretamente `x-amz-restore: ongoing-request="false"` quando algumas partes do objeto já foram transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não foram restauradas.

HeadObject e replicação entre grades

Se você estiver usando"federação de grade" e"replicação entre grades" estiver habilitado para um bucket, o cliente S3 poderá verificar o status de replicação de um objeto emitindo uma solicitação HeadObject. A resposta inclui o StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta, que terá um dos seguintes valores:

Grade	Status de replicação
Fonte	• **CONCLUÍDO**: A replicação foi bem-sucedida. • **PENDENTE**: O objeto ainda não foi replicado. • **FALHA**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	**REPLICA**: O objeto foi replicado da grade de origem.

> O StorageGRID não oferece suporte a `x-amz-replication-status` cabeçalho.

ColocarObjeto

Você pode usar a solicitação PutObject do S3 para adicionar um objeto a um bucket.

Resolver conflitos

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma

operação.

Tamanho do objeto

O tamanho máximo *recomendado* para uma única operação PutObject é 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use"upload multiparte" em vez de.

O tamanho máximo *compatível* para uma única operação PutObject é 5 TiB (5.497.558.138.880 bytes).

> Se você atualizou do StorageGRID 11.6 ou anterior, o alerta de tamanho de objeto S3 PUT muito grande será acionado se você tentar carregar um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11.7 ou 11.8, o alerta não será acionado neste caso. No entanto, para se alinhar ao padrão AWS S3, versões futuras do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

Tamanho dos metadados do usuário

O Amazon S3 limita o tamanho dos metadados definidos pelo usuário em cada cabeçalho de solicitação PUT a 2 KB. O StorageGRID limita os metadados do usuário a 24 KiB. O tamanho dos metadados definidos pelo usuário é medido pela soma do número de bytes na codificação UTF-8 de cada chave e valor.

Caracteres UTF-8 em metadados do usuário

Se uma solicitação incluir valores UTF-8 (sem escape) no nome da chave ou no valor dos metadados definidos pelo usuário, o comportamento do StorageGRID será indefinido.

O StorageGRID não analisa nem interpreta caracteres UTF-8 de escape incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Caracteres UTF-8 escapados são tratados como caracteres ASCII:

- As solicitações PutObject, CopyObject, GetObject e HeadObject serão bem-sucedidas se os metadados definidos pelo usuário incluírem caracteres UTF-8 de escape.
- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome da chave ou valor incluir caracteres não imprimíveis.

Limites de tags de objeto

Você pode adicionar tags a novos objetos ao carregá-los ou adicioná-las a objetos existentes. Tanto o StorageGRID quanto o Amazon S3 suportam até 10 tags para cada objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento e os valores de tag podem ter até 256 caracteres Unicode de comprimento. Chaves e valores diferenciam maiúsculas de minúsculas.

Propriedade do objeto

No StorageGRID, todos os objetos são de propriedade da conta do proprietário do bucket, incluindo objetos criados por uma conta não proprietária ou um usuário anônimo.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Cache-Control`

- `Content-Disposition`
- `Content-Encoding`

  Quando você especifica `aws-chunked` para`Content-Encoding` O StorageGRID não verifica os seguintes itens:

  - O StorageGRID não verifica o `chunk-signature` contra os dados do bloco.
  - O StorageGRID não verifica o valor que você fornece para `x-amz-decoded-content-length` contra o objeto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  A codificação de transferência em blocos é suportada se `aws-chunked` a assinatura de carga útil também é usada.
- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguido por um par nome-valor contendo metadados definidos pelo usuário.

  Ao especificar o par nome-valor para metadados definidos pelo usuário, use este formato geral:

  ```
  x-amz-meta-name: value
  ```

  Se você quiser usar a opção **Tempo de criação definido pelo usuário** como o Tempo de referência para uma regra ILM, você deve usar `creation-time` como o nome dos metadados que registram quando o objeto foi criado. Por exemplo:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  O valor para `creation-time` é avaliado como segundos desde 1º de janeiro de 1970.

  > Uma regra de ILM não pode usar um **horário de criação definido pelo usuário** para o horário de referência e a opção de ingestão balanceada ou restrita. Um erro é retornado quando a regra ILM é criada.

- `x-amz-tagging`
- Cabeçalhos de solicitação de bloqueio de objeto S3
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`

- `x-amz-object-lock-legal-hold`

  Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular o modo de versão do objeto e reter até a data. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3" .

- Cabeçalhos de solicitação SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    VerCabeçalhos de solicitação para criptografia do lado do servidor

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

  O `x-amz-website-redirect-location` retornos de cabeçalho `XNotImplemented` .

Opções de classe de armazenamento

O `x-amz-storage-class` O cabeçalho da solicitação é suportado. O valor submetido para `x-amz-storage-class` afeta como o StorageGRID protege os dados do objeto durante a ingestão e não quantas cópias persistentes do objeto são armazenadas no sistema StorageGRID (o que é determinado pelo ILM).

Se a regra ILM correspondente a um objeto ingerido usar a opção de ingestão estrita, o `x-amz-storage-class` cabeçalho não tem efeito.

Os seguintes valores podem ser usados para `x-amz-storage-class` :

- `STANDARD`(Padrão)
  - **Confirmação dupla**: se a regra do ILM especificar a opção Confirmação dupla para o comportamento de ingestão, assim que um objeto for ingerido, uma segunda cópia desse objeto será criada e distribuída para um nó de armazenamento diferente (confirmação dupla). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais atendem às instruções de posicionamento na regra. Caso contrário, talvez seja necessário fazer novas cópias de objetos em locais diferentes e as cópias provisórias iniciais talvez precisem ser excluídas.
  - **Balanceado**: Se a regra do ILM especificar a opção Balanceado e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes Nós de Armazenamento.

    Se o StorageGRID puder criar imediatamente todas as cópias de objetos especificadas na regra ILM

(posicionamento síncrono), o `x-amz-storage-class` cabeçalho não tem efeito.

- `REDUCED_REDUNDANCY`
  - **Confirmação dupla**: se a regra do ILM especificar a opção Confirmação dupla para o comportamento de ingestão, o StorageGRID criará uma única cópia provisória à medida que o objeto for ingerido (confirmação única).
  - **Balanceado**: Se a regra ILM especificar a opção Balanceado, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito. O `REDUCED_REDUNDANCY` A opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso usando `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia extra do objeto para cada operação de ingestão.

  Usando o `REDUCED_REDUNDANCY` opção não é recomendada em outras circunstâncias. `REDUCED_REDUNDANCY` aumenta o risco de perda de dados do objeto durante a ingestão. Por exemplo, você pode perder dados se a cópia única for armazenada inicialmente em um nó de armazenamento que falhe antes que a avaliação do ILM possa ocorrer.

> Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se existir apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Especificando `REDUCED_REDUNDANCY` afeta apenas quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Isso não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas de ILM ativas e não resulta no armazenamento de dados em níveis mais baixos de redundância no sistema StorageGRID .

> Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Cabeçalhos de solicitação para criptografia do lado do servidor

Você pode usar os seguintes cabeçalhos de solicitação para criptografar um objeto com criptografia do lado do servidor. As opções SSE e SSE-C são mutuamente exclusivas.

- **SSE**: Use o cabeçalho a seguir se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID.
  - `x-amz-server-side-encryption`

    Quando o `x-amz-server-side-encryption` o cabeçalho não está incluído na solicitação PutObject, a grade inteira"configuração de criptografia de objeto armazenado" é omitido da resposta PutObject.

- **SSE-C**: Use todos esses três cabeçalhos se quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.

- `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256` .
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.

> As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para"usando criptografia do lado do servidor" .

> Se um objeto for criptografado com SSE ou SSE-C, todas as configurações de criptografia em nível de bucket ou de grade serão ignoradas.

Controle de versão

Se o controle de versão estiver habilitado para um bucket, um único `versionId` é gerado automaticamente para a versão do objeto que está sendo armazenado. Esse `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho de resposta.

Se o controle de versão for suspenso, a versão do objeto será armazenada com um valor nulo `versionId` e se uma versão nula já existir, ela será substituída.

Cálculos de assinatura para o cabeçalho de autorização

Ao usar o `Authorization` cabeçalho para autenticar solicitações, o StorageGRID difere do AWS nas seguintes maneiras:

- StorageGRID não requer `host` cabeçalhos a serem incluídos dentro `CanonicalHeaders` .
- StorageGRID não requer `Content-Type` para ser incluído dentro `CanonicalHeaders` .
- StorageGRID não requer `x-amz-*` cabeçalhos a serem incluídos dentro `CanonicalHeaders` .

> Como prática recomendada geral, sempre inclua esses cabeçalhos dentro `CanonicalHeaders` para garantir que eles sejam verificados; no entanto, se você excluir esses cabeçalhos, o StorageGRID não retornará um erro.

Para mais detalhes, consulte "Cálculos de assinatura para o cabeçalho de autorização: transferindo carga útil em um único bloco (AWS Signature versão 4)" .

Informações relacionadas

- "Gerenciar objetos com ILM"
- "Referência da API do Amazon Simple Storage Service: PutObject"

RestaurarObjeto

Você pode usar a solicitação S3 RestoreObject para restaurar um objeto armazenado em um pool de armazenamento em nuvem.

Tipo de solicitação suportado

O StorageGRID suporta apenas solicitações RestoreObject para restaurar um objeto. Não suporta o `SELECT` tipo de restauração. Selecione solicitações de retorno `XNotImplemented` .

Controle de versão

Opcionalmente, especifique `versionId` para restaurar uma versão específica de um objeto em um bucket versionado. Se você não especificar `versionId` , a versão mais recente do objeto é restaurada

Comportamento de RestoreObject em objetos do Cloud Storage Pool

Se um objeto foi armazenado em um"Pool de armazenamento em nuvem" , uma solicitação RestoreObject tem o seguinte comportamento, com base no estado do objeto. Ver"CabeçaObjeto" para mais detalhes.

> Se um objeto estiver armazenado em um Cloud Storage Pool e uma ou mais cópias do objeto também existirem na grade, não haverá necessidade de restaurar o objeto emitindo uma solicitação RestoreObject. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação GetObject.

Estado do objeto	Comportamento de RestoreObject
Objeto ingerido no StorageGRID , mas ainda não avaliado pelo ILM, ou o objeto não está em um pool de armazenamento em nuvem	`403 Forbidden` , `InvalidObjectState`
Objeto no Cloud Storage Pool, mas ainda não transitado para um estado não recuperável	`200 OK`Nenhuma alteração é feita. **Nota**: Antes que um objeto seja transferido para um estado não recuperável, você não pode alterar sua `expiry-date` .
Objeto transitado para um estado não recuperável	`202 Accepted`Restaura uma cópia recuperável do objeto para o Cloud Storage Pool pelo número de dias especificado no corpo da solicitação. No final desse período, o objeto é devolvido a um estado não recuperável. Opcionalmente, use o `Tier` elemento de solicitação para determinar quanto tempo o trabalho de restauração levará para terminar(`Expedited` , `Standard` , ou `Bulk`). Se você não especificar `Tier` , o `Standard` camada é usada. **Importante**: Se um objeto tiver sido transferido para o S3 Glacier Deep Archive ou o Cloud Storage Pool usar o armazenamento de Blobs do Azure, você não poderá restaurá-lo usando o `Expedited` nível. O seguinte erro é retornado `403 Forbidden` , `InvalidTier` : `Retrieval option is not supported by this storage class` .

Estado do objeto	Comportamento de RestoreObject
Objeto em processo de restauração de um estado não recuperável	`409 Conflict` , `RestoreAlreadyInProgress`
Objeto totalmente restaurado no Cloud Storage Pool	`200 OK` **Observação:** Se um objeto foi restaurado para um estado recuperável, você pode alterá-lo `expiry-date` reemitindo a solicitação RestoreObject com um novo valor para `Days` . A data de restauração é atualizada em relação ao horário da solicitação.

SelecionarObjetoConteúdo

Você pode usar a solicitação SelectObjectContent do S3 para filtrar o conteúdo de um objeto do S3 com base em uma instrução SQL simples.

Para mais informações, consulte "Referência da API do Amazon Simple Storage Service: SelectObjectContent" .

Antes de começar

- A conta do locatário tem a permissão S3 Select.
- Você tem `s3:GetObject` permissão para o objeto que você deseja consultar.
- O objeto que você deseja consultar deve estar em um dos seguintes formatos:
  - **CSV**. Pode ser usado como está ou compactado em arquivos GZIP ou BZIP2.
  - **Parquet**. Requisitos adicionais para objetos Parquet:
    - O S3 Select suporta apenas compactação em colunas usando GZIP ou Snappy. O S3 Select não oferece suporte à compactação de objetos inteiros para objetos Parquet.
    - O S3 Select não suporta saída Parquet. Você deve especificar o formato de saída como CSV ou JSON.
    - O tamanho máximo do grupo de linhas descompactado é 512 MB.
    - Você deve usar os tipos de dados especificados no esquema do objeto.
    - Você não pode usar os tipos lógicos INTERVAL, JSON, LIST, TIME ou UUID.
- Sua expressão SQL tem um comprimento máximo de 256 KB.
- Qualquer registro na entrada ou nos resultados tem um comprimento máximo de 1 MiB.

Exemplo de sintaxe de solicitação CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemplo de sintaxe de solicitação Parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemplo de consulta SQL

Esta consulta obtém o nome do estado, as populações de 2010, as populações estimadas de 2015 e a porcentagem de alteração dos dados do censo dos EUA. Registros no arquivo que não são estados são ignorados.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

As primeiras linhas do arquivo a ser consultado, `SUB-EST2020_ALL.csv` , fica assim:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Exemplo de uso do AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

As primeiras linhas do arquivo de saída, `changes.csv` , fica assim:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Exemplo de uso do AWS-CLI (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

As primeiras linhas do arquivo de saída, changes.csv, se parecem com isto:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operações para uploads multipartes

Operações para uploads multipartes

Esta seção descreve como o StorageGRID oferece suporte a operações para uploads multipartes.

As seguintes condições e notas se aplicam a todas as operações de upload multipartes:

- Você não deve exceder 1.000 uploads multipartes simultâneos para um único bucket porque os resultados das consultas ListMultipartUploads para esse bucket podem retornar resultados incompletos.
- O StorageGRID impõe limites de tamanho da AWS para partes multipartes. Os clientes do S3 devem seguir estas diretrizes:
  - Cada parte em um upload multiparte deve ter entre 5 MiB (5.242.880 bytes) e 5 GiB (5.368.709.120 bytes).
  - A última parte pode ser menor que 5 MiB (5.242.880 bytes).
  - Em geral, os tamanhos das peças devem ser os maiores possíveis. Por exemplo, use tamanhos de peça de 5 GiB para um objeto de 100 GiB. Como cada parte é considerada um objeto único, o uso de tamanhos de parte grandes reduz a sobrecarga de metadados do StorageGRID .
  - Para objetos menores que 5 GiB, considere usar o upload não multiparte.
- O ILM é avaliado para cada parte de um objeto multiparte à medida que é ingerido e para o objeto como um todo quando o upload multiparte é concluído, se a regra ILM usar o Balanceado ou o Estrito"opção de ingestão" . Você deve estar ciente de como isso afeta o posicionamento de objetos e peças:
  - Se o ILM for alterado enquanto um upload multiparte do S3 estiver em andamento, algumas partes do objeto poderão não atender aos requisitos atuais do ILM quando o upload multiparte for concluído. Qualquer peça que não seja colocada corretamente é colocada na fila para reavaliação do ILM e

movida para o local correto posteriormente.

  - Ao avaliar o ILM para uma peça, o StorageGRID filtra o tamanho da peça, não o tamanho do objeto. Isso significa que partes de um objeto podem ser armazenadas em locais que não atendem aos requisitos do ILM para o objeto como um todo. Por exemplo, se uma regra especificar que todos os objetos de 10 GB ou maiores sejam armazenados no DC1, enquanto todos os objetos menores sejam armazenados no DC2, cada parte de 1 GB de um upload multiparte de 10 partes será armazenada no DC2 na ingestão. Entretanto, quando o ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.

- Todas as operações de upload multipartes oferecem suporte ao StorageGRID"valores de consistência" .
- Quando um objeto é ingerido usando upload multipartes, o"limite de segmentação de objetos (1 GiB)" não é aplicado.
- Conforme necessário, você pode usar"criptografia do lado do servidor" com uploads multipartes. Para usar SSE (criptografia do lado do servidor com chaves gerenciadas StorageGRID), você inclui o `x-amz-server-side-encryption` cabeçalho de solicitação somente na solicitação CreateMultipartUpload. Para usar SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente), especifique os mesmos três cabeçalhos de solicitação de chave de criptografia na solicitação CreateMultipartUpload e em cada solicitação UploadPart subsequente.

Operação	Implementação
AbortarMultipartUpload	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
Upload completo de várias partes	Ver"Upload completo de várias partes"
CriarMultipartUpload (anteriormente chamado de Iniciar Upload Multipartes)	Ver"CriarMultipartUpload"
ListarMultipartUploads	Ver"ListarMultipartUploads"
ListarPartes	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
UploadPart	Ver"UploadPart"
UploadPartCopy	Ver"UploadPartCopy"

Upload completo de várias partes

A operação CompleteMultipartUpload conclui um upload multiparte de um objeto reunindo as partes carregadas anteriormente.

> ⓘ O StorageGRID suporta valores não consecutivos em ordem crescente para `partNumber` parâmetro de solicitação com CompleteMultipartUpload. O parâmetro pode começar com qualquer valor.

Resolver conflitos

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  O `x-amz-storage-class` cabeçalho afeta quantas cópias de objeto o StorageGRID cria se a regra ILM correspondente especificar o"Opção de confirmação dupla ou ingestão balanceada" .

- `STANDARD`

  (Padrão) Especifica uma operação de ingestão de confirmação dupla quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

- `REDUCED_REDUNDANCY`

  Especifica uma operação de ingestão de confirmação única quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

  > Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

> Se um upload multiparte não for concluído em 15 dias, a operação será marcada como inativa e todos os dados associados serão excluídos do sistema.

> O `ETag` o valor retornado não é uma soma MD5 dos dados, mas segue a implementação da API do Amazon S3 `ETag` valor para objetos multipartes.

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controle de versão

Esta operação conclui um upload multiparte. Se o controle de versão estiver habilitado para um bucket, a versão do objeto será criada após a conclusão do upload multiparte.

Se o controle de versão estiver habilitado para um bucket, um único `versionId` é gerado automaticamente para a versão do objeto que está sendo armazenado. Esse `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho de resposta.

Se o controle de versão for suspenso, a versão do objeto será armazenada com um valor nulo `versionId` e se uma versão nula já existir, ela será substituída.

> Quando o controle de versão está habilitado para um bucket, a conclusão de um upload multiparte sempre cria uma nova versão, mesmo que haja uploads multiparte simultâneos concluídos na mesma chave de objeto. Quando o controle de versão não está habilitado para um bucket, é possível iniciar um upload multiparte e, em seguida, fazer com que outro upload multiparte seja iniciado e concluído primeiro na mesma chave de objeto. Em buckets não versionados, o upload multiparte concluído por último tem precedência.

Falha na replicação, notificação ou notificação de metadados

Se o bucket onde o upload multiparte ocorre estiver configurado para um serviço de plataforma, o upload multiparte será bem-sucedido mesmo se a ação de replicação ou notificação associada falhar.

Um locatário pode acionar a replicação com falha ou a notificação atualizando os metadados ou as tags do objeto. Um locatário pode reenviar os valores existentes para evitar fazer alterações indesejadas.

Consulte "Solucionar problemas de serviços de plataforma" .

CriarMultipartUpload

A operação CreateMultipartUpload (anteriormente chamada de Initiate Multipart Upload) inicia um upload multipart para um objeto e retorna um ID de upload.

O `x-amz-storage-class` O cabeçalho da solicitação é suportado. O valor submetido para `x-amz-storage-class` afeta como o StorageGRID protege os dados do objeto durante a ingestão e não quantas cópias persistentes do objeto são armazenadas no sistema StorageGRID (o que é determinado pelo ILM).

Se a regra ILM correspondente a um objeto ingerido usar o Strict"opção de ingestão" , o `x-amz-storage-class` cabeçalho não tem efeito.

Os seguintes valores podem ser usados para `x-amz-storage-class` :

- `STANDARD`(Padrão)
  - **Confirmação dupla**: se a regra do ILM especificar a opção de ingestão de confirmação dupla, assim que um objeto for ingerido, uma segunda cópia desse objeto será criada e distribuída para um nó de armazenamento diferente (confirmação dupla). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais atendem às instruções de posicionamento na regra. Caso contrário, talvez seja necessário fazer novas cópias de objetos em locais diferentes e as cópias provisórias iniciais talvez precisem ser excluídas.
  - **Balanceado**: Se a regra do ILM especificar a opção Balanceado e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes Nós de Armazenamento.

    Se o StorageGRID puder criar imediatamente todas as cópias de objetos especificadas na regra ILM (posicionamento síncrono), o `x-amz-storage-class` cabeçalho não tem efeito.

- `REDUCED_REDUNDANCY`
  - **Confirmação dupla**: se a regra do ILM especificar a opção Confirmação dupla, o StorageGRID criará uma única cópia provisória à medida que o objeto for ingerido (confirmação única).
  - **Balanceado**: Se a regra ILM especificar a opção Balanceado, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito. O `REDUCED_REDUNDANCY` A opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso usando `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia extra do objeto para cada operação de ingestão.

  Usando o `REDUCED_REDUNDANCY` opção não é recomendada em outras circunstâncias. `REDUCED_REDUNDANCY` aumenta o risco de perda de dados do objeto durante a ingestão. Por exemplo, você pode perder dados se a cópia única for armazenada inicialmente em um nó de armazenamento que falhe antes que a avaliação do ILM possa ocorrer.

> Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se existir apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Especificando `REDUCED_REDUNDANCY` afeta apenas quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Isso não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas de ILM ativas e não resulta no armazenamento de dados em níveis mais baixos de redundância no sistema StorageGRID .

> Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Type`
- `x-amz-checksum-algorithm`

  Atualmente, apenas o valor SHA256 para `x-amz-checksum-algorithm` é suportado.

- `x-amz-meta-`, seguido por um par nome-valor contendo metadados definidos pelo usuário

  Ao especificar o par nome-valor para metadados definidos pelo usuário, use este formato geral:

```
x-amz-meta-_name_: `value`
```

  Se você quiser usar a opção **Tempo de criação definido pelo usuário** como o Tempo de referência para uma regra ILM, você deve usar `creation-time` como o nome dos metadados que registram quando o

objeto foi criado. Por exemplo:

```
x-amz-meta-creation-time: 1443399726
```

O valor para `creation-time` é avaliado como segundos desde 1º de janeiro de 1970.

> Adicionando `creation-time` pois metadados definidos pelo usuário não são permitidos se você estiver adicionando um objeto a um bucket que tenha a Conformidade legada habilitada. Um erro será retornado.

- Cabeçalhos de solicitação de bloqueio de objeto S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular a versão do objeto retain-until-date.

  "Use a API REST do S3 para configurar o bloqueio de objeto do S3"

- Cabeçalhos de solicitação SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Cabeçalhos de solicitação para criptografia do lado do servidor

> Para obter informações sobre como o StorageGRID lida com caracteres UTF-8, consulte"ColocarObjeto" .

Cabeçalhos de solicitação para criptografia do lado do servidor

Você pode usar os seguintes cabeçalhos de solicitação para criptografar um objeto multiparte com criptografia do lado do servidor. As opções SSE e SSE-C são mutuamente exclusivas.

- **SSE**: Use o seguinte cabeçalho na solicitação CreateMultipartUpload se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações UploadPart.
  - `x-amz-server-side-encryption`
- **SSE-C**: Use todos esses três cabeçalhos na solicitação CreateMultipartUpload (e em cada solicitação UploadPart subsequente) se quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
  - `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256` .

- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.

> As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para"usando criptografia do lado do servidor" .

Cabeçalhos de solicitação não suportados

O seguinte cabeçalho de solicitação não é suportado:

- `x-amz-website-redirect-location`

  O `x-amz-website-redirect-location` retornos de cabeçalho `XNotImplemented` .

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

ListarMultipartUploads

A operação ListMultipartUploads lista uploads multipartes em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

UploadPart

A operação UploadPart carrega uma parte em um upload multiparte para um objeto.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação CreateMultipartUpload, também deverá incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256` .
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia que você forneceu na solicitação CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação CreateMultipartUpload.

> As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em"Use criptografia do lado do servidor" .

Se você especificou uma soma de verificação SHA-256 durante a solicitação CreateMultipartUpload, também deverá incluir o seguinte cabeçalho de solicitação em cada solicitação UploadPart:

- `x-amz-checksum-sha256`: Especifique a soma de verificação SHA-256 para esta parte.

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

UploadPartCopy

A operação UploadPartCopy carrega uma parte de um objeto copiando dados de um objeto existente como fonte de dados.

A operação UploadPartCopy é implementada com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.

Esta solicitação lê e grava os dados do objeto especificados em `x-amz-copy-source-range` dentro do sistema StorageGRID .

Os seguintes cabeçalhos de solicitação são suportados:

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

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação CreateMultipartUpload, também deverá incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPartCopy:

- `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256` .
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia que você forneceu na solicitação CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação CreateMultipartUpload.

Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deverá incluir os três cabeçalhos a seguir na solicitação UploadPartCopy para que o objeto possa ser descriptografado e copiado:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especifique `AES256` .
- `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia que você forneceu quando criou o objeto de origem.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu quando criou o objeto de origem.

> As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em"Use criptografia do lado do servidor" .

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

Respostas de erro

O sistema StorageGRID suporta todas as respostas de erro padrão da API REST do S3 aplicáveis. Além disso, a implementação do StorageGRID adiciona várias respostas

personalizadas.

Códigos de erro da API S3 suportados

Nome	Status HTTP
Acesso negado	403 Proibido
BadDigest	400 Solicitação Inválida
BucketAlreadyExists	409 Conflito
BaldeNãoVazio	409 Conflito
Corpo Incompleto	400 Solicitação Inválida
Erro interno	Erro interno do servidor 500
Id de chave de acesso inválido	403 Proibido
Argumento inválido	400 Solicitação Inválida
Nome de Bucket inválido	400 Solicitação Inválida
Estado de Bucket inválido	409 Conflito
InvalidDigest	400 Solicitação Inválida
Erro de Algoritmo de Criptografia Inválido	400 Solicitação Inválida
Parte inválida	400 Solicitação Inválida
Pedido de peça inválido	400 Solicitação Inválida
Intervalo inválido	416 Intervalo solicitado não satisfatório
Solicitação inválida	400 Solicitação Inválida
Classe de armazenamento inválida	400 Solicitação Inválida
Tag inválida	400 Solicitação Inválida
URI inválido	400 Solicitação Inválida
ChaveMuitoLonga	400 Solicitação Inválida

Nome	Status HTTP
XML malformado	400 Solicitação Inválida
MetadadosMuitoGrandes	400 Solicitação Inválida
MétodoNãoPermitido	Método 405 não permitido
Comprimento do conteúdo ausente	411 Comprimento necessário
Erro de corpo de solicitação ausente	400 Solicitação Inválida
Cabeçalho de segurança ausente	400 Solicitação Inválida
NoSuchBucket	404 Não Encontrado
Nenhuma Chave	404 Não Encontrado
NoSuchUpload	404 Não Encontrado
Não implementado	501 Não Implementado
Política NoSuchBucket	404 Não Encontrado
Erro de configuração de bloqueio de objeto não encontrado	404 Não Encontrado
Pré-condição falhou	412 Pré-condição falhou
RequestTimeTooSkewed	403 Proibido
Serviço não disponível	503 Serviço indisponível
AssinaturaNãoCorresponde	403 Proibido
Muitos Baldes	400 Solicitação Inválida
UserKeyDeveSerEspecificado	400 Solicitação Inválida

Códigos de erro personalizados do StorageGRID

Nome	Descrição	Status HTTP
XBucketLifecycleNãoPermitido	A configuração do ciclo de vida do bucket não é permitida em um bucket compatível legado	400 Solicitação Inválida

Nome	Descrição	Status HTTP
XBucketPolicyParseException	Falha ao analisar o JSON da política de bucket recebida.	400 Solicitação Inválida
XComplianceConflito	Operação negada devido a configurações de conformidade legadas.	403 Proibido
XComplianceRedundância ReduzidaProibido	Redundância reduzida não é permitida no bucket compatível legado	400 Solicitação Inválida
Comprimento da política XMaxBucket excedido	Sua apólice excede o comprimento máximo permitido da apólice.	400 Solicitação Inválida
XMissingInternalRequestHeader	Falta um cabeçalho de uma solicitação interna.	400 Solicitação Inválida
Conformidade com XNoSuchBucket	O bucket especificado não tem a conformidade legada habilitada.	404 Não Encontrado
XNãoAceitável	A solicitação contém um ou mais cabeçalhos de aceitação que não puderam ser atendidos.	406 Não aceitável
XNãoImplementado	A solicitação que você forneceu implica uma funcionalidade que não está implementada.	501 Não Implementado

Operações personalizadas do StorageGRID

Operações personalizadas do StorageGRID

O sistema StorageGRID suporta operações personalizadas que são adicionadas à API REST do S3.

A tabela a seguir lista as operações personalizadas suportadas pelo StorageGRID.

Operação	Descrição
"Consistência do balde GET"	Retorna a consistência que está sendo aplicada a um bucket específico.
"Consistência do balde PUT"	Define a consistência aplicada a um bucket específico.
"Último horário de acesso do Bucket GET"	Retorna se as últimas atualizações de horário de acesso estão habilitadas ou desabilitadas para um bucket específico.
"Hora do último acesso ao bucket PUT"	Permite que você habilite ou desabilite as atualizações do último horário de acesso para um bucket específico.

Operação	Descrição
"EXCLUIR configuração de notificação de metadados do bucket"	Exclui o XML de configuração de notificação de metadados associado a um bucket específico.
"Configuração de notificação de metadados do GET Bucket"	Retorna o XML de configuração de notificação de metadados associado a um bucket específico.
"Configuração de notificação de metadados do PUT Bucket"	Configura o serviço de notificação de metadados para um bucket.
"Uso de armazenamento GET"	Informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta.
"Obsoleto: CreateBucket com configurações de conformidade"	Obsoleto e sem suporte: não é mais possível criar novos buckets com a Conformidade ativada.
"Obsoleto: conformidade com o GET Bucket"	Obsoleto, mas com suporte: retorna as configurações de conformidade atualmente em vigor para um bucket compatível legado existente.
"Obsoleto: conformidade com PUT Bucket"	Obsoleto, mas com suporte: permite modificar as configurações de conformidade de um bucket compatível legado existente.

Consistência do balde GET

A solicitação de consistência GET Bucket permite que você determine a consistência que está sendo aplicada a um bucket específico.

A consistência padrão é definida para garantir leitura após gravação para objetos recém-criados.

Você deve ter a permissão s3:GetBucketConsistency ou ser root da conta para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Resposta

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

Consistência	Descrição
todos	Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
forte-global	Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
site forte	Garante consistência de leitura após gravação para todas as solicitações de clientes em um site.
leitura após nova escrita	(Padrão) Fornece 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	Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que raramente são lidos ou para operações HEAD ou GET em chaves que não existem). Não suportado para buckets do S3 FabricPool .

Exemplo de resposta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Informações relacionadas

"Valores de consistência"

Consistência do balde PUT

A solicitação de consistência do PUT Bucket permite que você especifique a consistência a ser aplicada às operações executadas em um bucket.

A consistência padrão é definida para garantir leitura após gravação para objetos recém-criados.

Antes de começar

Você deve ter a permissão s3:PutBucketConsistency ou ser root da conta para concluir esta operação.

Solicitar

O `x-ntap-sg-consistency` o parâmetro deve conter um dos seguintes valores:

Consistência	Descrição
todos	Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
forte-global	Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
site forte	Garante consistência de leitura após gravação para todas as solicitações de clientes em um site.
leitura após nova escrita	(Padrão) Fornece 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	Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que raramente são lidos ou para operações HEAD ou GET em chaves que não existem). Não suportado para buckets do S3 FabricPool .

Observação: Em geral, você deve usar a consistência "Leitura após nova gravação". Se as solicitações não estiverem funcionando corretamente, altere o comportamento do cliente do aplicativo, se possível. Ou configure o cliente para especificar a consistência para cada solicitação de API. Defina a consistência no nível do bucket somente como último recurso.

Exemplo de solicitação

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

Informações relacionadas

"Valores de consistência"

Último horário de acesso do Bucket GET

A solicitação de último horário de acesso do GET Bucket permite que você determine se as atualizações de último horário de acesso estão habilitadas ou desabilitadas para buckets individuais.

Você deve ter a permissão s3:GetBucketLastAccessTime ou ser root da conta para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

Este exemplo mostra que as atualizações do último horário de acesso estão habilitadas para o bucket.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

Hora do último acesso ao bucket PUT

A solicitação de último horário de acesso do PUT Bucket permite que você habilite ou desabilite atualizações de último horário de acesso para buckets individuais. Desabilitar as atualizações do último horário de acesso melhora o desempenho e é a configuração padrão para todos os buckets criados com a versão 10.3.0 ou posterior.

Você deve ter a permissão s3:PutBucketLastAccessTime para um bucket ou ser root da conta para concluir esta operação.

> ⓘ A partir da versão 10.3 do StorageGRID , as atualizações do último horário de acesso são desabilitadas por padrão para todos os novos buckets. Se você tiver buckets que foram criados usando uma versão anterior do StorageGRID e quiser corresponder ao novo comportamento padrão, deverá desabilitar explicitamente as atualizações do último horário de acesso para cada um desses buckets anteriores. Você pode habilitar ou desabilitar atualizações para o último horário de acesso usando a solicitação de último horário de acesso do bucket PUT ou na página de detalhes de um bucket no Gerenciador de locatários. Ver "Habilitar ou desabilitar atualizações do último horário de acesso" .

Se as atualizações do último horário de acesso estiverem desabilitadas para um bucket, o seguinte comportamento será aplicado às operações no bucket:

- As solicitações GetObject, GetObjectAcl, GetObjectTagging e HeadObject não atualizam o último horário de acesso. O objeto não é adicionado às filas para avaliação do gerenciamento do ciclo de vida das informações (ILM).
- As solicitações CopyObject e PutObjectTagging que atualizam apenas os metadados também atualizam o horário do último acesso. O objeto é adicionado às filas para avaliação do ILM.
- Se as atualizações do último horário de acesso estiverem desabilitadas para o bucket de origem, as solicitações CopyObject não atualizarão o último horário de acesso para o bucket de origem. O objeto que foi copiado não é adicionado às filas para avaliação do ILM para o bucket de origem. Entretanto, para o destino, as solicitações CopyObject sempre atualizam o horário do último acesso. A cópia do objeto é adicionada às filas para avaliação do ILM.
- CompleteMultipartUpload solicita atualização do último horário de acesso. O objeto concluído é adicionado às filas para avaliação do ILM.

Exemplos de solicitação

Este exemplo habilita o último horário de acesso para um bucket.

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

Este exemplo desabilita o último horário de acesso para um bucket.

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

EXCLUIR configuração de notificação de metadados do bucket

A solicitação de configuração de notificação de metadados DELETE Bucket permite que você desabilite o serviço de integração de pesquisa para buckets individuais excluindo o XML de configuração.

Você deve ter a permissão s3:DeleteBucketMetadataNotification para um bucket ou ser root da conta para concluir esta operação.

Exemplo de solicitação

Este exemplo mostra a desativação do serviço de integração de pesquisa para um bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configuração de notificação de metadados do GET Bucket

A solicitação de configuração de notificação de metadados do GET Bucket permite que você recupere o XML de configuração usado para configurar a integração de pesquisa para buckets individuais.

Você deve ter a permissão s3:GetBucketMetadataNotification ou ser root da conta para concluir esta operação.

Exemplo de solicitação

Esta solicitação recupera a configuração de notificação de metadados para o bucket denominado `bucket` .

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Resposta

O corpo da resposta inclui a configuração de notificação de metadados para o bucket. A configuração de notificação de metadados permite que você determine como o bucket é configurado para integração de pesquisa. Ou seja, ele permite que você determine quais objetos são indexados e para quais endpoints seus metadados de objeto estão sendo enviados.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Cada configuração de notificação de metadados inclui uma ou mais regras. Cada regra especifica os objetos aos quais se aplica e o destino para onde o StorageGRID deve enviar metadados do objeto. Os destinos devem ser especificados usando o URN de um ponto de extremidade StorageGRID .

Nome	Descrição	Obrigatório
Configuração de Notificação de Metadados	Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos Rule.	Sim
Regra	Tag de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
EU IA	Identificador exclusivo para a regra. Incluído no elemento Rule.	Não
Status	O status pode ser "Habilitado" ou "Desabilitado". Nenhuma ação é tomada para regras que estão desabilitadas. Incluído no elemento Rule.	Sim

Nome	Descrição	Obrigatório
Prefixo	Objetos que correspondem ao prefixo são afetados pela regra, e seus metadados são enviados ao destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento Rule.	Sim
Destino	Tag de contêiner para o destino de uma regra. Incluído no elemento Rule.	Sim
Urna	URN do destino para onde os metadados do objeto são enviados. Deve ser a URN de um ponto de extremidade StorageGRID com as seguintes propriedades: • `es`deve ser o terceiro elemento. • A URN deve terminar com o índice e o tipo onde os metadados são armazenados, no formato `domain-name/myindex/mytype` . Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles assumem a seguinte forma: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O ponto de extremidade deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. A urna está incluída no elemento Destino.	Sim

Exemplo de resposta

O XML incluído entre o `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags mostra como a integração com um ponto de extremidade de integração de pesquisa é configurada para o bucket. Neste exemplo, os metadados do objeto estão sendo enviados para um índice do Elasticsearch denominado `current` e digite nomeado `2017` que está hospedado em um domínio AWS chamado `records` .

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informações relacionadas

"Use uma conta de inquilino"

Configuração de notificação de metadados do PUT Bucket

A solicitação de configuração de notificação de metadados do PUT Bucket permite que você habilite o serviço de integração de pesquisa para buckets individuais. O XML de configuração de notificação de metadados fornecido no corpo da solicitação especifica os objetos cujos metadados são enviados ao índice de pesquisa de destino.

Você deve ter a permissão s3:PutBucketMetadataNotification para um bucket ou ser root da conta para concluir esta operação.

Solicitar

A solicitação deve incluir a configuração de notificação de metadados no corpo da solicitação. Cada configuração de notificação de metadados inclui uma ou mais regras. Cada regra especifica os objetos aos quais se aplica e o destino para onde o StorageGRID deve enviar metadados do objeto.

Os objetos podem ser filtrados pelo prefixo do nome do objeto. Por exemplo, você pode enviar metadados para objetos com o prefixo `/images` para um destino e objetos com o prefixo `/videos` para outro.

Configurações que possuem prefixos sobrepostos não são válidas e são rejeitadas quando enviadas. Por exemplo, uma configuração que incluía uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não seria permitido.

Os destinos devem ser especificados usando o URN de um ponto de extremidade StorageGRID . O ponto de extremidade deve existir quando a configuração de notificação de metadados for enviada, ou a solicitação

falhará como um `400 Bad Request` . A mensagem de erro diz: `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.`

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

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

Nome	Descrição	Obrigatório
Configuração de Notificação de Metadados	Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos Rule.	Sim
Regra	Tag de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
EU IA	Identificador exclusivo para a regra. Incluído no elemento Rule.	Não
Status	O status pode ser "Habilitado" ou "Desabilitado". Nenhuma ação é tomada para regras que estão desabilitadas. Incluído no elemento Rule.	Sim

Nome	Descrição	Obrigatório
Prefixo	Objetos que correspondem ao prefixo são afetados pela regra, e seus metadados são enviados ao destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento Rule.	Sim
Destino	Tag de contêiner para o destino de uma regra. Incluído no elemento Rule.	Sim
Urna	URN do destino para onde os metadados do objeto são enviados. Deve ser a URN de um ponto de extremidade StorageGRID com as seguintes propriedades: • `es`deve ser o terceiro elemento. • A URN deve terminar com o índice e o tipo onde os metadados são armazenados, no formato `domain-name/myindex/mytype` . Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles assumem a seguinte forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O ponto de extremidade deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. A urna está incluída no elemento Destino.	Sim

Exemplos de solicitação

Este exemplo mostra como habilitar a integração de pesquisa para um bucket. Neste exemplo, os metadados de todos os objetos são enviados para o mesmo destino.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

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

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

JSON gerado pelo serviço de integração de pesquisa

Quando você habilita o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado ao ponto de extremidade de destino sempre que metadados ou tags de objeto são adicionados, atualizados ou excluídos.

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

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

Metadados de objeto incluídos em notificações de metadados

A tabela lista todos os campos incluídos no documento JSON que é enviado ao ponto de extremidade de destino quando a integração de pesquisa está habilitada.

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

Tipo	Nome do item	Descrição
Informações sobre bucket e objeto	balde	Nome do balde
Informações sobre bucket e objeto	chave	Nome da chave do objeto
Informações sobre bucket e objeto	ID da versão	Versão do objeto, para objetos em buckets versionados
Informações sobre bucket e objeto	região	Região de balde, por exemplo `us-east-1`
Metadados do sistema	tamanho	Tamanho do objeto (em bytes) conforme visível para um cliente HTTP
Metadados do sistema	md5	Hash de objeto
Metadados do usuário	metadados *`key:value`*	Todos os metadados do usuário para o objeto, como pares de chave-valor

Tipo	Nome do item	Descrição
Etiquetas	etiquetas *key:value*	Todas as tags de objeto definidas para o objeto, como pares chave-valor

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

Informações relacionadas

"Use uma conta de inquilino"

Solicitação de uso de armazenamento GET

A solicitação GET Storage Usage informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta.

A quantidade de armazenamento usada por uma conta e seus buckets pode ser obtida por meio de uma solicitação ListBuckets modificada com o `x-ntap-sg-usage` parâmetro de consulta. O uso do armazenamento do bucket é rastreado separadamente das solicitações PUT e DELETE processadas pelo sistema. Pode haver algum atraso antes que os valores de uso correspondam aos valores esperados com base no processamento de solicitações, principalmente se o sistema estiver sob carga pesada.

Por padrão, o StorageGRID tenta recuperar informações de uso usando consistência global forte. Se a consistência global forte não puder ser alcançada, o StorageGRID tentará recuperar as informações de uso em uma consistência de site forte.

Você deve ter a permissão s3:ListAllMyBuckets ou ser root da conta para concluir esta operação.

Exemplo de solicitação

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

Este exemplo mostra uma conta que tem quatro objetos e 12 bytes de dados em dois buckets. Cada bucket contém dois objetos e seis bytes de dados.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Controle de versão

Cada versão do objeto armazenada contribuirá para o `ObjectCount` e `DataBytes` valores na resposta. Os marcadores de exclusão não são adicionados ao `ObjectCount` total.

Informações relacionadas

"Valores de consistência"

Solicitações de bucket obsoletas para conformidade legada

Solicitações de bucket obsoletas para conformidade legada

Talvez seja necessário usar a API REST do StorageGRID S3 para gerenciar buckets que foram criados usando o recurso de conformidade legado.

Recurso de conformidade obsoleto

O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock.

Se você habilitou anteriormente a configuração global de Conformidade, a configuração global de Bloqueio de Objeto S3 será habilitada no StorageGRID 11.6. Não é mais possível criar novos buckets com a Conformidade ativada; no entanto, conforme necessário, você pode usar a API REST do StorageGRID S3 para gerenciar quaisquer buckets compatíveis legados existentes.

- "Use a API REST do S3 para configurar o bloqueio de objeto do S3"
- "Gerenciar objetos com ILM"
- "Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"

Solicitações de conformidade obsoletas:

- "Obsoleto - Modificações na solicitação do bucket PUT para conformidade"

  O elemento XML SGCompliance está obsoleto. Anteriormente, você podia incluir esse elemento personalizado StorageGRID no corpo de solicitação XML opcional de solicitações PUT Bucket para criar um bucket compatível.

- "Obsoleto - Conformidade com o GET Bucket"

  A solicitação de conformidade do GET Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket compatível legado existente.

- "Obsoleto - Conformidade com PUT Bucket"

  A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para modificar as configurações de conformidade de um bucket compatível legado existente. Por exemplo, você pode colocar um bucket existente em retenção legal ou aumentar seu período de retenção.

Obsoleto: modificações na solicitação CreateBucket para conformidade

O elemento XML SGCompliance está obsoleto. Anteriormente, você podia incluir este elemento personalizado StorageGRID no corpo de solicitação XML opcional das solicitações CreateBucket para criar um bucket compatível.

> ⓘ O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock. Veja o seguinte para mais detalhes:
>
> - "Use a API REST do S3 para configurar o bloqueio de objeto do S3"
> - "Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"

Não é mais possível criar novos buckets com a Conformidade ativada. A seguinte mensagem de erro será retornada se você tentar usar as modificações de solicitação CreateBucket para conformidade para criar um novo bucket compatível:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsoleto: solicitação de conformidade do GET Bucket

A solicitação de conformidade do GET Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket compatível legado existente.

> ⓘ O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock. Veja o seguinte para mais detalhes:
>
> - "Use a API REST do S3 para configurar o bloqueio de objeto do S3"
> - "Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"

Você deve ter a permissão s3:GetBucketCompliance ou ser root da conta para concluir esta operação.

Exemplo de solicitação

Este exemplo de solicitação permite que você determine as configurações de conformidade para o bucket denominado `mybucket` .

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

No XML de resposta, `<SGCompliance>` lista as configurações de conformidade em vigor para o bucket. Este exemplo de resposta mostra as configurações de conformidade para um bucket no qual cada objeto será retido por um ano (525.600 minutos), a partir do momento em que o objeto for ingerido na grade. Atualmente não há retenção legal para este balde. Cada objeto será excluído automaticamente após um ano.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrição
Período de retenção em minutos	A duração do período de retenção para objetos adicionados a este bucket, em minutos. O período de retenção começa quando o objeto é ingerido na grade.
Retenção Legal	• Verdadeiro: Este bucket está atualmente sob retenção legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja suspensa, mesmo que o período de retenção tenha expirado. • Falso: Este bucket não está atualmente sob retenção legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Exclusão automática	• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob retenção legal. • Falso: Os objetos neste bucket não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Respostas de erro

Se o bucket não foi criado para ser compatível, o código de status HTTP para a resposta é `404 Not Found`, com um código de erro S3 de `XNoSuchBucketCompliance`.

Obsoleto: solicitação de conformidade do PUT Bucket

A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para modificar as configurações de conformidade de um bucket compatível legado existente. Por exemplo, você pode colocar um bucket existente em retenção legal ou aumentar seu período de retenção.

O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock. Veja o seguinte para mais detalhes:

- "Use a API REST do S3 para configurar o bloqueio de objeto do S3"
- "Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"

Você deve ter a permissão s3:PutBucketCompliance ou ser root da conta para concluir esta operação.

Você deve especificar um valor para cada campo das configurações de conformidade ao emitir uma solicitação de conformidade do PUT Bucket.

Exemplo de solicitação

Este exemplo de solicitação modifica as configurações de conformidade para o bucket denominado `mybucket` . Neste exemplo, os objetos em `mybucket` agora serão retidos por dois anos (1.051.200 minutos) em vez de um ano, a partir do momento em que o objeto for inserido na grade. Não há retenção legal para este balde. Cada objeto será excluído automaticamente após dois anos.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrição
Período de retenção em minutos	A duração do período de retenção para objetos adicionados a este bucket, em minutos. O período de retenção começa quando o objeto é ingerido na grade. **Importante** Ao especificar um novo valor para RetentionPeriodMinutes, você deve especificar um valor que seja igual ou maior que o período de retenção atual do bucket. Depois que o período de retenção do bucket for definido, você não poderá diminuir esse valor; você só poderá aumentá-lo.

Nome	Descrição
Retenção Legal	• Verdadeiro: Este bucket está atualmente sob retenção legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja suspensa, mesmo que o período de retenção tenha expirado. • Falso: Este bucket não está atualmente sob retenção legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Exclusão automática	• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob retenção legal. • Falso: Os objetos neste bucket não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Consistência para configurações de conformidade

Quando você atualiza as configurações de conformidade de um bucket do S3 com uma solicitação de conformidade do bucket PUT, o StorageGRID tenta atualizar os metadados do bucket na grade. Por padrão, o StorageGRID usa a consistência **Strong-global** para garantir que todos os sites do data center e todos os nós de armazenamento que contêm metadados de bucket tenham consistência de leitura após gravação para as configurações de conformidade alteradas.

Se o StorageGRID não conseguir atingir a consistência **Strong-global** porque um site de data center ou vários nós de armazenamento em um site não estão disponíveis, o código de status HTTP para a resposta é `503 Service Unavailable`.

Se você receber essa resposta, entre em contato com o administrador da rede para garantir que os serviços de armazenamento necessários sejam disponibilizados o mais rápido possível. Se o administrador da grade não conseguir disponibilizar Nós de Armazenamento suficientes em cada site, o suporte técnico poderá instruí-lo a tentar novamente a solicitação com falha, forçando a consistência **Strong-site**.

> Nunca force a consistência **Strong-site** para conformidade com o bucket PUT, a menos que você tenha sido instruído a fazê-lo pelo suporte técnico e a menos que você entenda as potenciais consequências do uso desse nível.

Quando a consistência é reduzida para **Strong-site**, o StorageGRID garante que as configurações de conformidade atualizadas terão consistência de leitura após gravação somente para solicitações de clientes dentro de um site. Isso significa que o sistema StorageGRID pode ter temporariamente várias configurações inconsistentes para esse bucket até que todos os sites e nós de armazenamento estejam disponíveis. Configurações inconsistentes podem resultar em comportamento inesperado e indesejado. Por exemplo, se você estiver colocando um bucket sob retenção legal e forçar uma consistência menor, as configurações de conformidade anteriores do bucket (ou seja, retenção legal) poderão continuar em vigor em alguns sites de data center. Como resultado, objetos que você acha que estão em retenção legal podem ser excluídos quando seu período de retenção expirar, pelo usuário ou pela Exclusão Automática, se habilitada.

Para forçar o uso da consistência **Strong-site**, emita novamente a solicitação de conformidade do PUT Bucket e inclua o `Consistency-Control` Cabeçalho de solicitação HTTP, como segue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Respostas de erro

- Se o bucket não foi criado para ser compatível, o código de status HTTP para a resposta é `404 Not Found`.
- Se `RetentionPeriodMinutes` na solicitação for menor que o período de retenção atual do bucket, o código de status HTTP é `400 Bad Request`.

Informações relacionadas

"Obsoleto: modificações na solicitação do bucket PUT para conformidade"

Políticas de acesso a grupos e buckets

Use políticas de acesso a buckets e grupos

O StorageGRID usa a linguagem de política da Amazon Web Services (AWS) para permitir que os locatários do S3 controlem o acesso a buckets e objetos dentro desses buckets. O sistema StorageGRID implementa um subconjunto da linguagem de política da API REST do S3. As políticas de acesso para a API do S3 são escritas em JSON.

Visão geral da política de acesso

Há dois tipos de políticas de acesso suportadas pelo StorageGRID.

- **Políticas de bucket**, que são gerenciadas usando as operações da API S3 GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy ou a API Tenant Manager ou Tenant Management. As políticas de bucket são anexadas aos buckets, portanto, elas são configuradas para controlar o acesso de usuários na conta do proprietário do bucket ou de outras contas ao bucket e aos objetos nele contidos. Uma política de bucket se aplica a apenas um bucket e possivelmente a vários grupos.
- **Políticas de grupo**, que são configuradas usando o Tenant Manager ou a Tenant Management API. As políticas de grupo são anexadas a um grupo na conta, portanto, elas são configuradas para permitir que esse grupo acesse recursos específicos de propriedade dessa conta. Uma política de grupo se aplica a apenas um grupo e possivelmente a vários buckets.

> Não há diferença de prioridade entre políticas de grupo e de bucket.

As políticas de grupo e bucket do StorageGRID seguem uma gramática específica definida pela Amazon. Dentro de cada política há uma série de declarações de política, e cada declaração contém os seguintes elementos:

- ID da declaração (Sid) (opcional)
- Efeito
- Principal/Não Principal
- Recurso/NãoRecurso
- Ação/NãoAção

- Condição (opcional)

As declarações de política são criadas usando esta estrutura para especificar permissões: Conceder <Efeito> para permitir/negar que <Principal> execute <Ação> em <Recurso> quando <Condição> se aplicar.

Cada elemento de política é usado para uma função específica:

Elemento	Descrição
Sido	O elemento Sid é opcional. O Sid serve apenas como uma descrição para o usuário. Ele é armazenado, mas não interpretado pelo sistema StorageGRID .
Efeito	Use o elemento Efeito para estabelecer se as operações especificadas são permitidas ou negadas. Você deve identificar as operações que permite (ou nega) em buckets ou objetos usando as palavras-chave do elemento Action suportadas.
Principal/Não Principal	Você pode permitir que usuários, grupos e contas acessem recursos específicos e executem ações específicas. Se nenhuma assinatura S3 for incluída na solicitação, o acesso anônimo será permitido especificando o caractere curinga (*) como principal. Por padrão, somente o root da conta tem acesso aos recursos de propriedade da conta. Você só precisa especificar o elemento Principal em uma política de bucket. Para políticas de grupo, o grupo ao qual a política está anexada é o elemento Principal implícito.
Recurso/NãoRecurso	O elemento Resource identifica buckets e objetos. Você pode permitir ou negar permissões para buckets e objetos usando o Amazon Resource Name (ARN) para identificar o recurso.
Ação/NãoAção	Os elementos Ação e Efeito são os dois componentes das permissões. Quando um grupo solicita um recurso, o acesso ao recurso é concedido ou negado. O acesso será negado, a menos que você atribua permissões especificamente, mas você pode usar a negação explícita para substituir uma permissão concedida por outra política.
Doença	O elemento Condition é opcional. As condições permitem que você crie expressões para determinar quando uma política deve ser aplicada.

No elemento Ação, você pode usar o caractere curinga (*) para especificar todas as operações ou um subconjunto de operações. Por exemplo, esta Ação corresponde a permissões como s3:GetObject, s3:PutObject e s3:DeleteObject.

```
s3:*Object
```

No elemento Recurso, você pode usar os caracteres curinga (*) e (?). Enquanto o asterisco (*) corresponde a 0 ou mais caracteres, o ponto de interrogação (?) corresponde a qualquer caractere único.

No elemento Principal, caracteres curinga não são suportados, exceto para definir acesso anônimo, que concede permissão a todos. Por exemplo, você define o curinga (*) como o valor Principal.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

No exemplo a seguir, a instrução está usando os elementos Effect, Principal, Action e Resource. Este exemplo mostra uma declaração de política de bucket completa que usa o efeito "Permitir" para dar aos Principais, o grupo de administração `federated-group/admin` e o grupo financeiro `federated-group/finance` , permissões para executar a Ação `s3:ListBucket` no balde chamado `mybucket` e a Ação `s3:GetObject` em todos os objetos dentro desse balde.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

A política de bucket tem um limite de tamanho de 20.480 bytes, e a política de grupo tem um limite de tamanho de 5.120 bytes.

Consistência para políticas

Por padrão, todas as atualizações feitas nas políticas de grupo serão consistentes. Quando uma política de grupo se torna consistente, as alterações podem levar mais 15 minutos para entrar em vigor, devido ao cache de políticas. Por padrão, todas as atualizações feitas nas políticas de bucket são fortemente consistentes.

Conforme necessário, você pode alterar as garantias de consistência para atualizações de política de bucket. Por exemplo, você pode querer que uma alteração em uma política de bucket esteja disponível durante uma

interrupção do site.

Neste caso, você pode definir o `Consistency-Control` cabeçalho na solicitação PutBucketPolicy ou você pode usar a solicitação de consistência PUT Bucket. Quando uma política de bucket se torna consistente, as alterações podem levar mais 8 segundos para entrar em vigor, devido ao cache de políticas.

> Se você definir a consistência para um valor diferente para contornar uma situação temporária, certifique-se de definir a configuração do nível do bucket de volta para seu valor original quando terminar. Caso contrário, todas as solicitações futuras de bucket usarão a configuração modificada.

Use ARN em declarações de política

Em declarações de política, o ARN é usado nos elementos Principal e Resource.

- Use esta sintaxe para especificar o ARN do recurso S3:

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

- Use esta sintaxe para especificar o ARN do recurso de identidade (usuários e grupos):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Outras considerações:

- Você pode usar o asterisco (*) como curinga para corresponder a zero ou mais caracteres dentro da chave do objeto.
- Caracteres internacionais, que podem ser especificados na chave do objeto, devem ser codificados usando JSON UTF-8 ou usando sequências de escape JSON \u. A codificação percentual não é suportada.

  "Sintaxe URN RFC 2141"

  O corpo da solicitação HTTP para a operação PutBucketPolicy deve ser codificado com charset=UTF-8.

Especificar recursos em uma política

Em declarações de política, você pode usar o elemento Resource para especificar o bucket ou objeto para o qual as permissões são permitidas ou negadas.

- Cada declaração de política requer um elemento Recurso. Em uma política, os recursos são denotados pelo elemento `Resource` , ou alternativamente, `NotResource` para exclusão.
- Você especifica recursos com um ARN de recurso S3. Por exemplo:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Você também pode usar variáveis de política dentro da chave do objeto. Por exemplo:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- O valor do recurso pode especificar um bucket que ainda não existe quando uma política de grupo é criada.

Especificar os principais em uma política

Use o elemento Principal para identificar o usuário, grupo ou conta de locatário que tem acesso permitido/negado ao recurso pela declaração de política.

- Cada declaração de política em uma política de bucket deve incluir um elemento Principal. Declarações de política em uma política de grupo não precisam do elemento Principal porque o grupo é entendido como o principal.
- Em uma política, os principais são indicados pelo elemento "Principal" ou, alternativamente, "NotPrincipal" para exclusão.
- Identidades baseadas em conta devem ser especificadas usando um ID ou um ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- Este exemplo usa o ID da conta de locatário 27233906934684427525, que inclui a raiz da conta e todos os usuários na conta:

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Você pode especificar apenas a raiz da conta:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Você pode especificar um usuário federado específico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Você pode especificar um grupo federado específico ("Gerentes"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Você pode especificar um principal anônimo:

```
"Principal": "*"
```

- Para evitar ambiguidade, você pode usar o UUID do usuário em vez do nome de usuário:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Por exemplo, suponha que Alex deixe a organização e o nome de usuário `Alex` é excluído. Se um novo Alex se juntar à organização e for designado para o mesmo `Alex` nome de usuário, o novo usuário pode herdar involuntariamente as permissões concedidas ao usuário original.

- O valor principal pode especificar um nome de grupo/usuário que ainda não existe quando uma política de bucket é criada.

Especificar permissões em uma política

Em uma política, o elemento Ação é usado para permitir/negar permissões para um recurso. Há um conjunto de permissões que você pode especificar em uma política, que são indicadas pelo elemento "Ação" ou, alternativamente, "NãoAção" para exclusão. Cada um desses elementos mapeia operações específicas da API REST do S3.

As tabelas listam as permissões que se aplicam aos buckets e as permissões que se aplicam aos objetos.

> O Amazon S3 agora usa a permissão s3:PutReplicationConfiguration para as ações PutBucketReplication e DeleteBucketReplication. O StorageGRID usa permissões separadas para cada ação, o que corresponde à especificação original do Amazon S3.

> Uma exclusão é realizada quando um put é usado para substituir um valor existente.

Permissões que se aplicam a buckets

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:CriarBucket	CriarBucket	Sim. **Observação**: Use somente em políticas de grupo.
s3:ExcluirBucket	ExcluirBucket	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:DeleteBucketMetadataNotification	EXCLUIR configuração de notificação de metadados do bucket	Sim
s3:DeleteBucketPolicy	Política de exclusão de balde	
s3:ExcluirConfiguração de Replicação	DeleteBucketReplication	Sim, permissões separadas para PUT e DELETE
s3:ObterBucketAcl	ObterBucketAcl	
s3:ObterConformidade doBucket	Conformidade com o GET Bucket (obsoleto)	Sim
s3:ObterConsistência doBucket	Consistência do balde GET	Sim
s3:ObterBucketCORS	ObterBucketCors	
s3:ObterConfiguração de Criptografia	Obter criptografia do Bucket	
s3:GetBucketÚltimoAcessoHora	Último horário de acesso do Bucket GET	Sim
s3:ObterLocalização do Balde	ObterBucketLocation	
s3:GetBucketMetadataNotification	Configuração de notificação de metadados do GET Bucket	Sim
s3:GetBucketNotification	Obter configuração de notificação de bucket	
s3:GetBucketObjectLockConfiguration	ObterConfiguraçãoObjectLock	
s3:ObterPolítica deBucket	ObterBucketPolicy	
s3:Obter marcação de balde	Obter marcação de balde	
s3:GetBucketVersionamento	ObterVersionamento doBucket	
s3:ObterConfiguração do Ciclo de Vida	Obter configuração do ciclo de vida do Bucket	
s3:ObterConfiguração de Replicação	Obter replicação do Bucket	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:ListarTodosOsMeusBuckets	• ListBuckets • Uso de armazenamento GET	Sim, para uso de armazenamento GET. **Observação**: Use somente em políticas de grupo.
s3:ListBucket	• Objetos de Lista • Balde de cabeça • RestaurarObjeto	
s3:ListBucketMultipartUploads	• ListarMultipartUploads • RestaurarObjeto	
s3:ListBucketVersões	Versões do GET Bucket	
s3:Conformidade com PutBucket	Conformidade com o PUT Bucket (obsoleto)	Sim
s3:ConsistênciaPutBucket	Consistência do balde PUT	Sim
s3:ColocarBucketCORS	• ExcluirBucketCors† • ColoqueBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:ColocarBucketÚltimoAcessoHora	Hora do último acesso ao bucket PUT	Sim
s3:PutBucketMetadataNotification	Configuração de notificação de metadados do PUT Bucket	Sim
s3:NotificaçãoPutBucket	Configuração de notificação PutBucket	
s3:PutBucketObjectLockConfiguração	• CreateBucket com o `x-amz-bucket-object-lock-enabled: true` cabeçalho de solicitação (também requer a permissão s3:CreateBucket) • PutObjectLockConfiguration	
s3:PolíticaPutBucket	PutBucketPolicy	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:PutBucketTagging	• ExcluirBucketTagging† • Colocar marcação de balde	
s3:PutBucketVersionamento	Versão PutBucket	
s3:PutLifecycleConfiguration	• Ciclo de vida do DeleteBucket† • Configuração do ciclo de vida do PutBucket	
s3:PutReplicationConfiguration	PutBucketReplicação	Sim, permissões separadas para PUT e DELETE

Permissões que se aplicam a objetos

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:AbortarUploadMultipart	• AbortarMultipartUpload • RestaurarObjeto	
s3:Ignorar Governança Retenção	• ExcluirObjeto • ExcluirObjetos • ColocarRetençãoDeObjeto	
s3:ExcluirObjeto	• ExcluirObjeto • ExcluirObjetos • RestaurarObjeto	
s3:ExcluirMarcaçãoDeObjeto	ExcluirMarcaçãoDeObjeto	
s3:ExcluirMarcaçãoDeVersãoDoObjeto	DeleteObjectTagging (uma versão específica do objeto)	
s3:ExcluirVersãoDoObjeto	DeleteObject (uma versão específica do objeto)	
s3:ObterObjeto	• ObterObjeto • CabeçaObjeto • RestaurarObjeto • SelecionarObjetoConteúdo	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:ObterAclDeObjeto	ObterAclObjeto	
s3:ObterObjetoLegalHold	ObterObjetoLegalHold	
s3:ObterRetençãoDeObjeto	ObterRetençãoDeObjeto	
s3:ObterMarcaçãoDeObjeto	Obter marcação de objeto	
s3:ObterTag deVersão do Objeto	GetObjectTagging (uma versão específica do objeto)	
s3:ObterVersãoDoObjeto	GetObject (uma versão específica do objeto)	
s3:ListMultipartUploadParts	ListParts, RestaurarObjeto	
s3:ColocarObjeto	• ColocarObjeto • CopiarObjeto • RestaurarObjeto • CriarMultipartUpload • Upload completo de várias partes • UploadPart • UploadPartCopy	
s3:ColocarObjetoLegalHold	ColocarObjetoLegalHold	
s3:PutObjectRetention	ColocarRetençãoDeObjeto	
s3:PutObjectTagging	Colocar marcação de objeto	
s3:PutObjectVersionTagging	PutObjectTagging (uma versão específica do objeto)	
s3:ColocarObjetoSobrescrito	• ColocarObjeto • CopiarObjeto • Colocar marcação de objeto • ExcluirMarcaçãoDeObjeto • Upload completo de várias partes	Sim
s3:RestaurarObjeto	RestaurarObjeto	

Usar permissão PutOverwriteObject

A permissão s3:PutOverwriteObject é uma permissão personalizada do StorageGRID que se aplica a operações que criam ou atualizam objetos. A configuração dessa permissão determina se o cliente pode substituir os dados de um objeto, metadados definidos pelo usuário ou marcação de objetos do S3.

As configurações possíveis para essa permissão incluem:

- **Permitir**: O cliente pode substituir um objeto. Esta é a configuração padrão.
- **Negar**: O cliente não pode substituir um objeto. Quando definida como Negar, a permissão PutOverwriteObject funciona da seguinte maneira:
  - Se um objeto existente for encontrado no mesmo caminho:
    - Os dados do objeto, os metadados definidos pelo usuário ou a marcação de objetos S3 não podem ser substituídos.
    - Todas as operações de ingestão em andamento são canceladas e um erro é retornado.
    - Se o controle de versão do S3 estiver habilitado, a configuração Negar impedirá que as operações PutObjectTagging ou DeleteObjectTagging modifiquem o TagSet de um objeto e suas versões não atuais.
  - Se um objeto existente não for encontrado, esta permissão não terá efeito.
- Quando essa permissão não está presente, o efeito é o mesmo que se Permitir estivesse definido.

> ⓘ Se a política atual do S3 permitir a substituição e a permissão PutOverwriteObject estiver definida como Negar, o cliente não poderá substituir os dados de um objeto, os metadados definidos pelo usuário ou a marcação de objetos. Além disso, se a caixa de seleção **Impedir modificação do cliente** estiver marcada (**CONFIGURAÇÃO** > **Configurações de segurança** > **Rede e objetos**), essa configuração substituirá a configuração da permissão PutOverwriteObject.

Especificar condições em uma política

As condições definem quando uma política estará em vigor. As condições consistem em operadores e pares chave-valor.

As condições usam pares chave-valor para avaliação. Um elemento Condition pode conter várias condições, e cada condição pode conter vários pares chave-valor. O bloco de condição usa o seguinte formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

No exemplo a seguir, a condição IpAddress usa a chave de condição SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Operadores de condição suportados

Os operadores de condição são categorizados da seguinte forma:

- Corda
- Numérico
- Booleano
- Endereço IP
- Verificação nula

Operadores de condição	Descrição
StringEquals	Compara uma chave a um valor de string com base na correspondência exata (diferencia maiúsculas de minúsculas).
StringNotEquals	Compara uma chave a um valor de string com base na correspondência negada (diferencia maiúsculas de minúsculas).
StringEqualsIgnoreCase	Compara uma chave a um valor de string com base na correspondência exata (ignora maiúsculas e minúsculas).
StringNotEqualsIgnoreCase	Compara uma chave a um valor de string com base na correspondência negada (ignora maiúsculas e minúsculas).
StringLike	Compara uma chave a um valor de string com base na correspondência exata (diferencia maiúsculas de minúsculas). Pode incluir caracteres curinga * e ?.
StringNotLike	Compara uma chave a um valor de string com base na correspondência negada (diferencia maiúsculas de minúsculas). Pode incluir caracteres curinga * e ?.
NumericEquals	Compara uma chave a um valor numérico com base na correspondência exata.
NuméricoNãoIgual	Compara uma chave a um valor numérico com base na correspondência negada.

Operadores de condição	Descrição
NuméricoMaiorQue	Compara uma chave a um valor numérico com base na correspondência "maior que".
NuméricoMaiorQueIgual	Compara uma chave a um valor numérico com base na correspondência "maior ou igual a".
NuméricoMenorQue	Compara uma chave a um valor numérico com base na correspondência "menor que".
NuméricoMenorQueIgual	Compara uma chave a um valor numérico com base na correspondência "menor ou igual a".
Bool	Compara uma chave a um valor booleano com base na correspondência "verdadeiro ou falso".
Endereço IP	Compara uma chave a um endereço IP ou intervalo de endereços IP.
Não Endereço IP	Compara uma chave a um endereço IP ou intervalo de endereços IP com base na correspondência negada.
Nulo	Verifica se uma chave de condição está presente no contexto de solicitação atual.

Chaves de condição suportadas

Chaves de condição	Ações	Descrição
aws:SourceIp	Operadores de IP	Será comparado ao endereço IP de onde a solicitação foi enviada. Pode ser usado para operações de bucket ou objeto. **Observação:** Se a solicitação S3 foi enviada por meio do serviço Load Balancer nos nós de administração e nos nós de gateway, isso será comparado ao endereço IP upstream do serviço Load Balancer. **Observação**: se um balanceador de carga de terceiros não transparente for usado, isso será comparado ao endereço IP desse balanceador de carga. Qualquer `X-Forwarded-For` O cabeçalho será ignorado porque sua validade não pode ser verificada.
aws:nome de usuário	Recurso/Identidade	Será comparado ao nome de usuário do remetente de onde a solicitação foi enviada. Pode ser usado para operações de bucket ou objeto.

Chaves de condição	Ações	Descrição
s3:delimitador	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro delimitador especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:ExistingObjectTag/<chave-tag>	s3:ExcluirMarcaçãoDeObjeto s3:ExcluirMarcaçãoDeVersãoDoObjeto s3:ObterObjeto s3:ObterAclDeObjeto 3: Obter marcação de objeto s3:ObterVersãoDoObjeto s3:ObterVersãoDoObjetoAcl s3:ObterTag deVersão do Objeto s3:ColocarObjetoAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Exigirá que o objeto existente tenha a chave e o valor de tag específicos.
s3:max-chaves	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro max-keys especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:object-lock-remaining-retention-days	s3:ColocarObjeto	Compara com a data de retenção especificada no `x-amz-object-lock-retain-until-date` cabeçalho de solicitação ou calculado a partir do período de retenção padrão do bucket para garantir que esses valores estejam dentro do intervalo permitido para as seguintes solicitações: • ColocarObjeto • CopiarObjeto • CriarMultipartUpload

Chaves de condição	Ações	Descrição
s3:object-lock-remaining-retention-days	s3:PutObjectRetention	Compara com a data de retenção especificada na solicitação PutObjectRetention para garantir que esteja dentro do intervalo permitido.
s3:prefix	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro de prefixo especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:RequestObjectTag/<chave-tag>	s3:ColocarObjeto s3:PutObjectTagging s3:PutObjectVersionTagging	Exigirá uma chave de tag e um valor específicos quando a solicitação de objeto incluir marcação.

Especificar variáveis em uma política

Você pode usar variáveis em políticas para preencher informações de políticas quando elas estiverem disponíveis. Você pode usar variáveis de política no `Resource` elemento e em comparações de strings no `Condition` elemento.

Neste exemplo, a variável `${aws:username}` faz parte do elemento Recurso:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

Neste exemplo, a variável `${aws:username}` faz parte do valor da condição no bloco de condição:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variável	Descrição
`${aws:SourceIp}`	Usa a chave SourceIp como a variável fornecida.
`${aws:username}`	Usa a chave de nome de usuário como a variável fornecida.
`${s3:prefix}`	Usa a chave de prefixo específica do serviço como a variável fornecida.

Variável	Descrição
`${s3:max-keys}`	Usa a chave max-keys específica do serviço como a variável fornecida.
`${*}`	Caractere especial. Usa o caractere como um caractere * literal.
`${?}`	Caractere especial. Usa o caractere como um caractere literal ?.
`${$}`	Caractere especial. Usa o caractere como um caractere $ literal.

Crie políticas que exijam tratamento especial

Às vezes, uma política pode conceder permissões que são perigosas para a segurança ou perigosas para operações contínuas, como bloquear o usuário root da conta. A implementação da API REST do StorageGRID S3 é menos restritiva durante a validação de políticas do que a Amazon, mas igualmente rigorosa durante a avaliação de políticas.

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento do StorageGRID
Negar a si mesmo quaisquer permissões para a conta root	Balde	Válido e aplicado, mas a conta do usuário root mantém a permissão para todas as operações de política do bucket S3	Mesmo
Negar a si mesmo quaisquer permissões para usuário/grupo	Grupo	Válido e aplicado	Mesmo
Permitir qualquer permissão a um grupo de contas estrangeiras	Balde	Principal inválido	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro 405 Método Não Permitido quando permitidas por uma política
Permitir que uma conta estrangeira root ou usuário tenha qualquer permissão	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro 405 Método Não Permitido quando permitidas por uma política	Mesmo

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento do StorageGRID
Permitir que todos tenham permissão para todas as ações	Balde	Válido, mas as permissões para todas as operações de política do bucket S3 retornam um erro 405 Método Não Permitido para a raiz da conta estrangeira e usuários	Mesmo
Negar a todos permissões para todas as ações	Balde	Válido e aplicado, mas a conta do usuário root mantém a permissão para todas as operações de política do bucket S3	Mesmo
Principal é um usuário ou grupo inexistente	Balde	Principal inválido	Válido
O recurso é um bucket S3 inexistente	Grupo	Válido	Mesmo
Principal é um grupo local	Balde	Principal inválido	Válido
A política concede a uma conta não proprietária (incluindo contas anônimas) permissões para colocar objetos.	Balde	Válido. Os objetos são de propriedade da conta do criador e a política de bucket não se aplica. A conta do criador deve conceder permissões de acesso ao objeto usando ACLs de objeto.	Válido. Os objetos são de propriedade da conta do proprietário do bucket. Aplica-se a política de balde.

Proteção WORM (gravação única e leitura múltipla)

Você pode criar buckets WORM (write-once-read-many) para proteger dados, metadados de objetos definidos pelo usuário e marcação de objetos do S3. Configure os buckets WORM para permitir a criação de novos objetos e evitar substituições ou exclusões de conteúdo existente. Use uma das abordagens descritas aqui.

Para garantir que as substituições sejam sempre negadas, você pode:

- No Grid Manager, vá para **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança** > **Rede e objetos** e marque a caixa de seleção **Impedir modificação do cliente**.
- Aplique as seguintes regras e políticas do S3:
  - Adicione uma operação PutOverwriteObject DENY à política S3.
  - Adicione uma operação DeleteObject DENY à política S3.
  - Adicione uma operação PutObject ALLOW à política S3.

Definir DeleteObject como DENY em uma política do S3 não impede que o ILM exclua objetos quando existe uma regra como "zero cópias após 30 dias".

Mesmo quando todas essas regras e políticas são aplicadas, elas não protegem contra gravações simultâneas (veja Situação A). Eles protegem contra sobrescritas sequenciais concluídas (veja Situação B).

Situação A: Gravações simultâneas (não protegidas)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situação B: Substituições sequenciais concluídas (protegidas contra)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Informações relacionadas

- "Como as regras do StorageGRID ILM gerenciam objetos"
- "Exemplos de políticas de bucket"
- "Exemplo de políticas de grupo"
- "Gerenciar objetos com ILM"
- "Use uma conta de inquilino"

Exemplos de políticas de bucket

Use os exemplos nesta seção para criar políticas de acesso do StorageGRID para buckets.

As políticas de bucket especificam as permissões de acesso para o bucket ao qual a política está anexada. Você configura uma política de bucket usando a API PutBucketPolicy do S3 por meio de uma destas ferramentas:

- "Gerente de inquilinos" .
- AWS CLI usando este comando (consulte"Operações em baldes"):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Exemplo: permitir que todos tenham acesso somente leitura a um bucket

Neste exemplo, todos, incluindo anônimos, têm permissão para listar objetos no bucket e executar operações GetObject em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que esta

política pode não ser particularmente útil porque ninguém, exceto o root da conta, tem permissão para gravar no bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Exemplo: permitir que todos em uma conta tenham acesso total e todos em outra conta tenham acesso somente leitura a um bucket

Neste exemplo, todos em uma conta especificada têm permissão para acesso total a um bucket, enquanto todos em outra conta especificada têm permissão apenas para listar o bucket e executar operações GetObject em objetos no bucket começando com o `shared/` prefixo de chave de objeto.

> No StorageGRID, os objetos criados por uma conta não proprietária (incluindo contas anônimas) são de propriedade da conta do proprietário do bucket. A política de bucket se aplica a esses objetos.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Exemplo: permitir que todos tenham acesso somente leitura a um bucket e acesso total ao grupo especificado

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar operações GetObject em todos os objetos no bucket, enquanto apenas os usuários pertencentes ao grupo `Marketing` na conta especificada têm acesso total.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemplo: permitir que todos tenham acesso de leitura e gravação a um bucket se o cliente estiver no intervalo de IP

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar quaisquer operações de objeto em todos os objetos no bucket, desde que as solicitações venham de um intervalo de IP especificado (54.240.143.0 a 54.240.143.255, exceto 54.240.143.188). Todas as outras operações serão negadas, e todas as solicitações fora do intervalo de IP serão negadas.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Exemplo: permitir acesso total a um bucket exclusivamente por um usuário federado especificado

Neste exemplo, o usuário federado Alex tem acesso total ao `examplebucket` balde e seus objetos. Todos os outros usuários, incluindo `root', têm todas as operações explicitamente negadas. Observe, no entanto, que` root' nunca tem permissões negadas para Put/Get/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemplo: permissão PutOverwriteObject

Neste exemplo, o `Deny` O efeito para PutOverwriteObject e DeleteObject garante que ninguém possa substituir ou excluir os dados do objeto, os metadados definidos pelo usuário e a marcação de objetos do S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Exemplo de políticas de grupo

Use os exemplos nesta seção para criar políticas de acesso do StorageGRID para grupos.

As políticas de grupo especificam as permissões de acesso para o grupo ao qual a política está anexada. Não há `Principal` elemento na política porque está implícito. As políticas de grupo são configuradas usando o Gerenciador de Tenants ou a API.

Exemplo: definir política de grupo usando o Gerenciador de Tenants

Ao adicionar ou editar um grupo no Gerenciador de Tenants, você pode selecionar uma política de grupo para determinar quais permissões de acesso ao S3 os membros desse grupo terão. Ver "Criar grupos para um locatário S3" .

- **Sem acesso S3**: opção padrão. Os usuários neste grupo não têm acesso aos recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar esta opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
- **Acesso somente leitura**: os usuários neste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários neste grupo podem listar objetos e ler dados de objetos, metadados e tags. Quando você seleciona esta opção, a string JSON para uma política de grupo somente leitura aparece na caixa de texto. Você não pode editar esta sequência.
- **Acesso total**: os usuários neste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona esta opção, a string JSON para uma política de grupo de acesso total aparece na caixa de texto. Você não pode editar esta sequência.
- **Mitigação de ransomware**: esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários neste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que tenham o controle de versão de objetos habilitado.

  Usuários do Tenant Manager que têm a permissão Gerenciar todos os buckets podem substituir esta política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação Multifator (MFA) quando disponível.

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

Exemplo: permitir acesso total do grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm permissão de acesso total a todos os buckets de propriedade da conta do locatário, a menos que seja explicitamente negado pela política de bucket.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemplo: permitir acesso somente leitura do grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm acesso somente leitura aos recursos do S3, a menos que explicitamente negado pela política de bucket. Por exemplo, os usuários neste grupo podem listar objetos e ler dados de objetos, metadados e tags.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemplo: permitir que os membros do grupo tenham acesso total apenas à sua "pasta" em um bucket

Neste exemplo, os membros do grupo só têm permissão para listar e acessar sua pasta específica (prefixo de chave) no bucket especificado. Observe que as permissões de acesso de outras políticas de grupo e da política de bucket devem ser consideradas ao determinar a privacidade dessas pastas.

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

Operações S3 rastreadas nos logs de auditoria

As mensagens de auditoria são geradas pelos serviços do StorageGRID e armazenadas em arquivos de log de texto. Você pode revisar as mensagens de auditoria específicas do S3 no log de auditoria para obter detalhes sobre as operações de bucket e objeto.

Operações de bucket rastreadas nos logs de auditoria

- CriarBucket
- ExcluirBucket
- ExcluirBucketTagging
- ExcluirObjetos
- Obter marcação de balde
- Balde de cabeça
- Objetos de Lista
- Versões do objeto de lista
- Conformidade do PUT Bucket
- Colocar marcação de balde
- Versão PutBucket

Operações de objetos rastreadas nos logs de auditoria

- Upload completo de várias partes
- CopiarObjeto
- ExcluirObjeto
- ObterObjeto
- CabeçaObjeto
- ColocarObjeto
- RestaurarObjeto
- SelecionarObjeto
- UploadPart (quando uma regra ILM usa ingestão balanceada ou restrita)
- UploadPartCopy (quando uma regra ILM usa ingestão balanceada ou estrita)

Informações relacionadas

- "Arquivo de log de auditoria de acesso"
- "O cliente escreve mensagens de auditoria"
- "O cliente leu mensagens de auditoria"

Use a API REST do Swift (fim da vida útil)

Usar a API REST do Swift

O suporte para a API Swift chegou ao fim e será removido em uma versão futura.

Os detalhes do Swift foram removidos desta versão do site de documentação. Ver "StorageGRID 11.8: Use a API REST do Swift" .

Informações sobre direitos autorais

Informações sobre marcas comerciais