Use o StorageGRID

StorageGRID

NetApp
March 12, 2025

Índice

Use o StorageGRID

Use uma conta de locatário

Use uma conta de locatário: Visão geral

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

O que é uma conta de locatário?

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

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

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

  > Se você usar o protocolo cliente S3, também poderá usar buckets e políticas de bucket do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa criar contas de locatário separadas. Consulte Instruções para a implementação de aplicativos cliente S3.

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

Como criar uma conta de locatário

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

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

sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.

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

Configurar locatários do S3

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

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

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

Configurar os locatários Swift

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

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

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

Use o Gerenciador do Locatário

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

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

Como entrar e sair

Inicie sessão no Tenant Manager

Você acessa o Gerenciador do Locatário inserindo o URL do locatário na barra de

endereços de um navegador da web suportado.

O que você vai precisar

- Tem de ter as suas credenciais de início de sessão.
- Você deve ter um URL para acessar o Gerenciador do Locatário, conforme fornecido pelo administrador da grade. O URL será parecido com um destes exemplos:

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

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

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

  O URL sempre contém o nome de domínio totalmente qualificado (FQDN) ou o endereço IP usado para acessar um nó de administração e, opcionalmente, também pode incluir um número de porta, o ID da conta de locatário de 20 dígitos ou ambos.

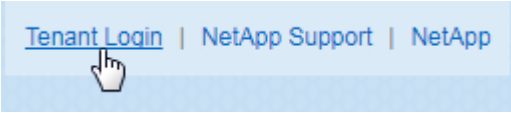
- Se o URL não incluir o ID de conta de 20 dígitos do locatário, você deve ter esse ID de conta.
- Você deve estar usando um navegador da web suportado.
- Os cookies devem estar ativados no seu navegador.
- Você deve ter permissões de acesso específicas.

Passos

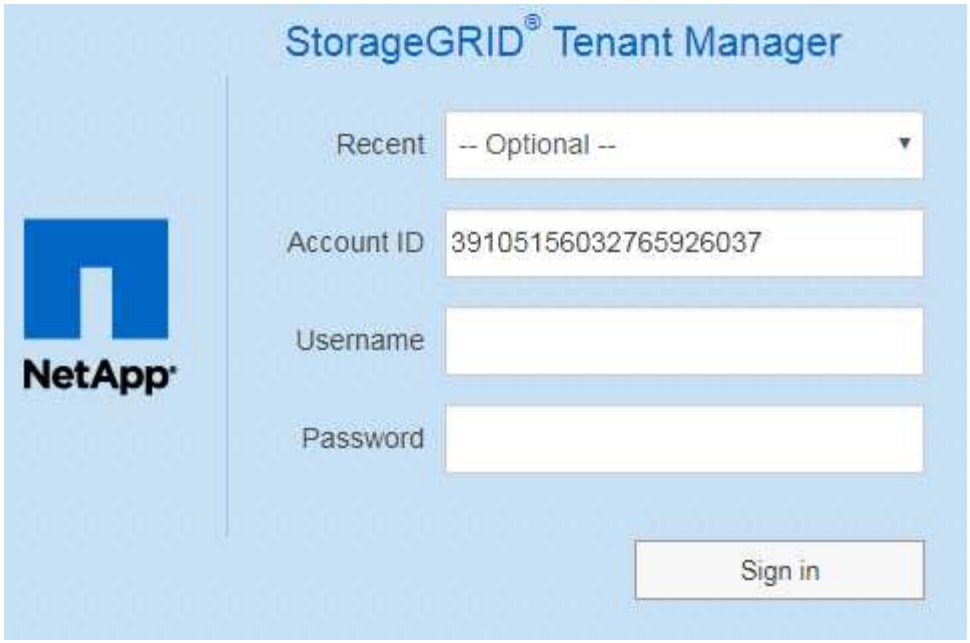
1. Inicie um navegador da web suportado.
2. Na barra de endereços do navegador, insira o URL para acessar o Gerenciador de locatários.
3. Se for solicitado um alerta de segurança, instale o certificado usando o assistente de instalação do navegador.
4. Inicie sessão no Gestor do Locatário.

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

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

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



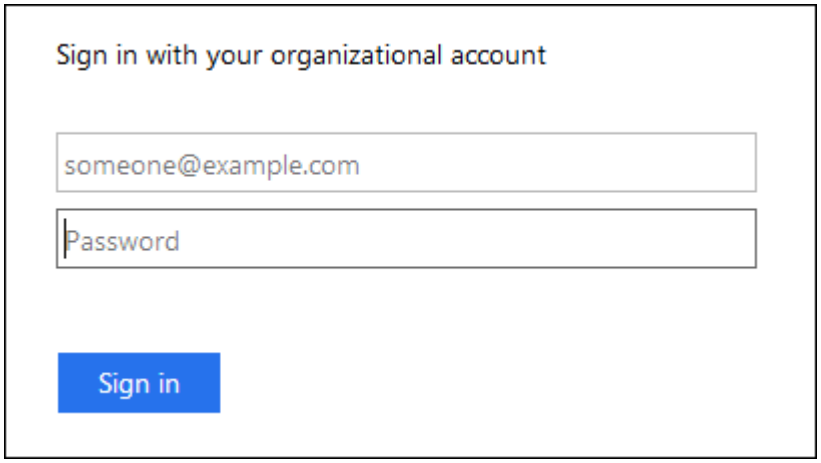
i. Se o ID da conta de 20 dígitos do locatário não for exibido, selecione o nome da conta do locatário se ele aparecer na lista de contas recentes ou insira o ID da conta.

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

iii. Clique em **entrar**.

É apresentado o Painel do Gestor do Locatário.

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



Insira suas credenciais SSO padrão e clique em **entrar**.

◦ A página de login SSO do Tenant Manager.

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

ii. Clique em **entrar**.

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

É apresentado o Painel do Gestor do Locatário.

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

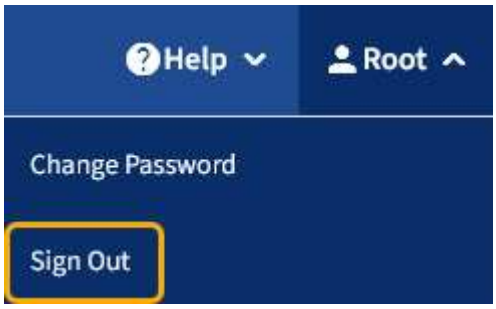
> Se o SSO estiver ativado para o sistema StorageGRID, você não poderá alterar sua senha do Gerenciador do Locatário.

Sair do Tenant Manager

Quando terminar de trabalhar com o Gestor do Locatário, tem de terminar sessão para garantir que os utilizadores não autorizados não conseguem aceder ao sistema StorageGRID. Fechar seu navegador pode não sair do sistema, com base nas configurações de cookies do navegador.

Passos

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



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

   ◦ Se o SSO não estiver em uso:

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

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

- Se o SSO estiver ativado:

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

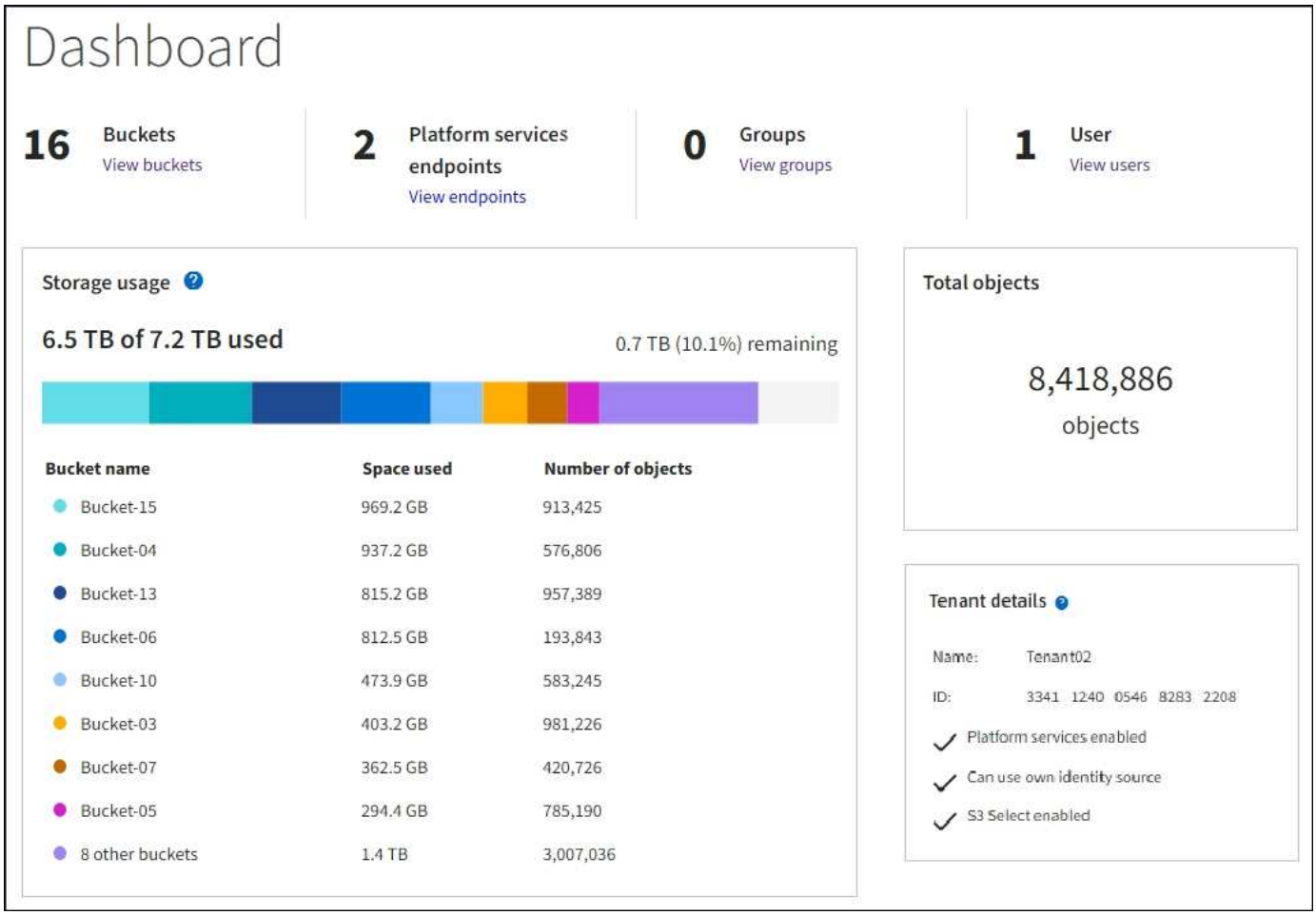
> Se o SSO estiver ativado e você também estiver conetado ao Gerenciador de Grade, você também deverá sair do Gerenciador de Grade para sair do SSO.

Entenda o Painel do Tenant Manager

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

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

Quando os objetos tiverem sido carregados, o Painel de Controle se parece com o seguinte exemplo:



Resumo da conta do locatário

A parte superior do Painel contém as seguintes informações:

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

Pode selecionar as ligações para ver os detalhes.

O lado direito do painel contém as seguintes informações:

- O número total de objetos para o locatário.

  Para uma conta do S3, se nenhum objeto tiver sido ingerido e você tiver a permissão de acesso root, as diretrizes de introdução aparecerão em vez do número total de objetos.

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

Uso de storage e cota

O painel uso do armazenamento contém as seguintes informações:

- A quantidade de dados de objeto para o locatário.

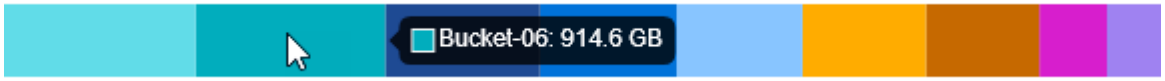
Esse valor indica a quantidade total de dados de objeto carregados e não representa o espaço usado para armazenar cópias desses objetos e seus metadados.

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

A utilização de quotas baseia-se em estimativas internas e pode ser ultrapassada em alguns casos. Por exemplo, o StorageGRID verifica a cota quando um locatário começa a carregar objetos e rejeita novos ingere se o locatário tiver excedido a cota. No entanto, o StorageGRID não leva em conta o tamanho do upload atual ao determinar se a cota foi excedida. Se os objetos forem excluídos, um locatário poderá ser temporariamente impedido de carregar novos objetos até que a utilização da cota seja recalculada. Os cálculos de utilização de cotas podem levar 10 minutos ou mais.

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

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



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

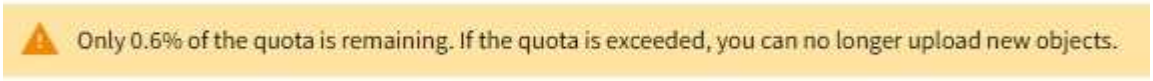
Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

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

Alertas de uso de cota

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

Se 90% ou mais da cota de um locatário tiver sido usada, o alerta **uso de cota de locatário alto** será acionado. Para obter mais informações, consulte a referência de alertas nas instruções para monitoramento e solução de problemas do StorageGRID.

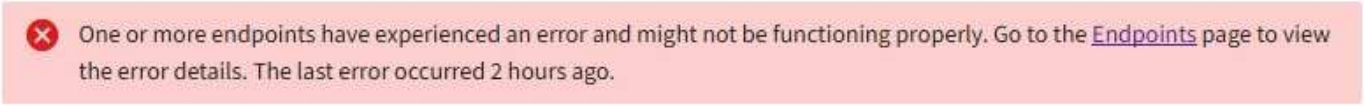


Se você exceder sua cota, não poderá carregar novos objetos.

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

Erros de endpoint

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



Para ver detalhes sobre um erro de endpoint, selecione Endpoints para exibir a página Endpoints.

Informações relacionadas

Solucionar erros de endpoint dos serviços da plataforma

Monitorar e solucionar problemas

API de gerenciamento do locatário

Entenda a API de gerenciamento do locatário

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

A API de gerenciamento do locatário:

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

- Utiliza controle de versão para dar suporte a atualizações sem interrupções.

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

Passos

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

Operações da API

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

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

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

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

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

- **Config** — operações relacionadas à versão do produto e versões da API de Gerenciamento do locatário. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **Containers** — operações em baldes S3 ou contentores Swift, como segue:

  S3

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

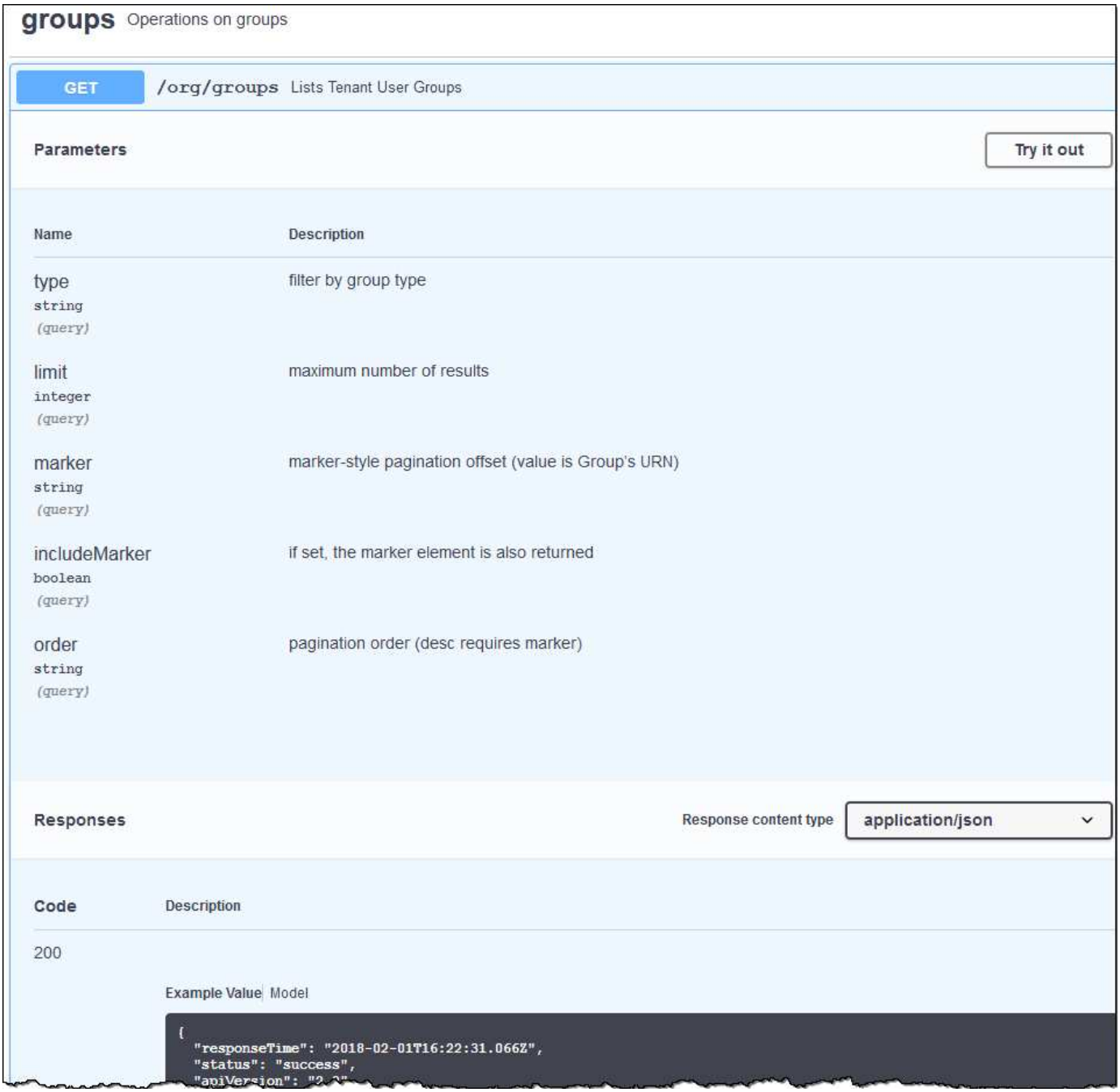
  Swift: Defina o nível de consistência usado para contentores

- **Disabled-features** — operações para visualizar recursos que podem ter sido desativados.
- **Endpoints** — operações para gerenciar um endpoint. Os endpoints permitem que um bucket do S3 use um serviço externo para replicação, notificações ou integração de pesquisa do StorageGRID CloudMirror.

- **Groups** — operações para gerenciar grupos de locatários locais e recuperar grupos de locatários federados de uma origem de identidade externa.
- **Identity-source** — operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo federado e de usuário.
- **Regions** — operações para determinar quais regiões foram configuradas para o sistema StorageGRID.
- **S3** — operações para gerenciar chaves de acesso S3 para usuários arrendatários.
- **S3-object-lock** — operações em configurações globais de bloqueio de objetos S3D, usadas para suportar a conformidade regulamentar.
- **Usuários** — operações para visualizar e gerenciar usuários de inquilinos.

Detalhes da operação

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



Emitir solicitações de API

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

Passos

1. Selecione a ação HTTP para ver os detalhes da solicitação.
2. Determine se a solicitação requer parâmetros adicionais, como um grupo ou ID de usuário. Em seguida, obtenha esses valores. Talvez você precise emitir uma solicitação de API diferente primeiro para obter as informações de que precisa.
3. Determine se você precisa modificar o corpo de solicitação de exemplo. Em caso afirmativo, você pode selecionar **modelo** para aprender os requisitos para cada campo.

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

Controle de versão da API de gerenciamento de locatário

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

Por exemplo, este URL de solicitação especifica a versão 3 da API.

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

A versão principal da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que são ***not compatible*** com versões mais antigas. A versão menor da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que ***are compatíveis*** com versões mais antigas. As alterações compatíveis incluem a adição de novos endpoints ou novas propriedades. O exemplo a seguir ilustra como a versão da API é carregada com base no tipo de alterações feitas.

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

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

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Deprecated: True"
- O corpo de resposta JSON inclui "obsoleto": True

Determine quais versões de API são suportadas na versão atual

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

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

Especifique a versão da API para solicitação

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

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

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Proteger contra falsificação de solicitação entre locais (CSRF)

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

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

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

Para ativar a funcionalidade, defina o `csrfToken` parâmetro para `true` durante a autenticação. A predefinição é `false`.

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

Quando verdadeiro, um `GridCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Grade, e o `AccountCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Tenant.

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

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

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

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

Gerenciar o acesso ao sistema

Use a federação de identidade

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

Configure a federação de identidade para o Gerenciador do Locatário

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

O que você vai precisar

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

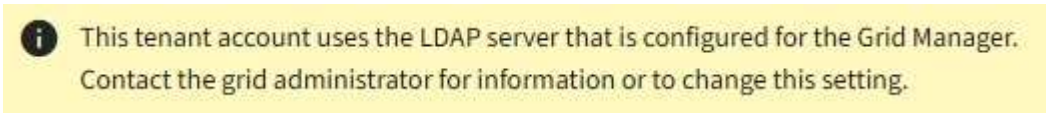
  > Se pretender utilizar um serviço LDAP v3 que não esteja listado, contacte o suporte técnico.

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

Sobre esta tarefa

Se você pode configurar um serviço de federação de identidade para seu locatário depende de como sua conta de locatário foi configurada. Seu locatário pode compartilhar o serviço de federação de identidade configurado para o Gerenciador de Grade. Se você vir essa mensagem ao acessar a página Federação de

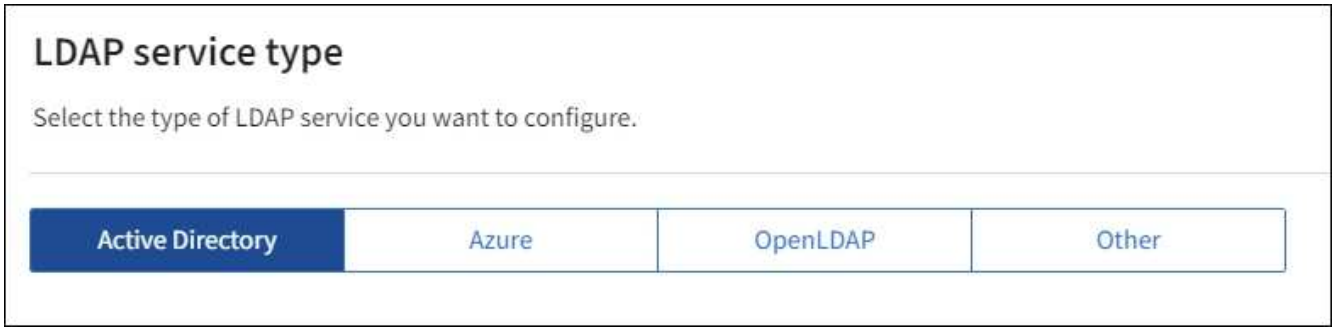
identidade, não será possível configurar uma origem de identidade federada separada para esse locatário.



Introduza a configuração

Passos

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



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

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

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

- **Nome de usuário**: O caminho completo do nome distinto (DN) para o usuário que se conetará ao servidor LDAP.

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

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

  - `sAMAccountName` ou `uid`
  - `objectGUID`, `entryUUID`, ou `nsuniqueid`
  - `cn`
  - `memberOf` ou `isMemberOf`
  - **Ative Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, E `userPrincipalName`
  - **Azure**: `accountEnabled` E. `userPrincipalName`
- **Senha**: A senha associada ao nome de usuário.
- **Group base DN**: O caminho completo do nome distinto (DN) para uma subárvore LDAP que você deseja pesquisar grupos. No exemplo do ative Directory (abaixo), todos os grupos cujo Nome distinto é relativo ao DN base (DC-StorageGRID,DC-com) podem ser usados como grupos federados.

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

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

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

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

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

  Introduza um destes padrões:

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

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

6. Na seção Transport Layer Security (TLS), selecione uma configuração de segurança.

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

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

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

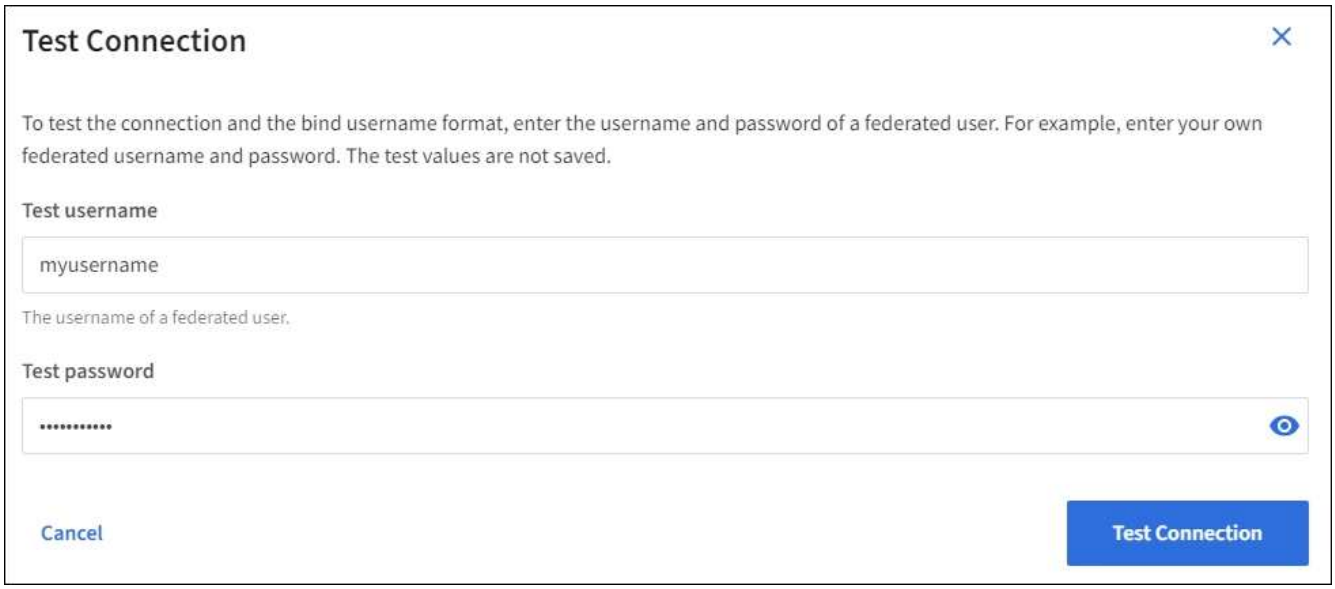
     Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

Teste a conexão e salve a configuração

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

1. Selecione **Test Connection**.
2. Se você não forneceu um formato de nome de usuário do BIND:
   - Uma mensagem ""Teste de conexão bem-sucedida"" aparece se as configurações de conexão forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - Uma mensagem "'test Connection could not be established'" (não foi possível estabelecer ligação) é apresentada se as definições de ligação forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.
3. Se você tiver fornecido um formato de nome de usuário do BIND, insira o nome de usuário e a senha de um usuário federado válido.

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



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

Forçar a sincronização com a fonte de identidade

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

Passos

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

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

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

Desativar a federação de identidade

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

Sobre esta tarefa

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

- Os utilizadores federados não poderão iniciar sessão.
- Os usuários federados que estiverem conetados no momento manterão o acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.

- A sincronização entre o sistema StorageGRID e a origem da identidade não ocorrerá e os alertas ou alarmes não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Ativar federação de identidade** será desativada se o logon único (SSO) estiver definido como **habilitado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade. Desative o logon únicoConsulte .

Passos

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

Diretrizes para configurar o servidor OpenLDAP

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

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

Sobreposições de Memberof e refint

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

Indexação

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

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

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

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

Gerenciar grupos

Crie grupos para um locatário do S3

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

O que você vai precisar

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

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

Para obter informações sobre o S3, Use S3consulte .

Passos

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

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

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

4. Introduza o nome do grupo.
   - **Local group**: Insira um nome de exibição e um nome exclusivo. Pode editar o nome de apresentação mais tarde.
   - **Federated group**: Insira o nome exclusivo. Para o ative Directory, o nome exclusivo é o nome associado ao `sAMAccountName` atributo. Para OpenLDAP, o nome exclusivo é o nome associado ao `uid` atributo.
5. Selecione **continuar**.
6. Selecione um modo de acesso. Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como somente leitura, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.
   - **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do Tenant e gerenciar a configuração do locatário.

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

7. Selecione as permissões de grupo para este grupo.

   Consulte as informações sobre permissões de gerenciamento de locatários.

8. Selecione **continuar**.
9. Selecione uma política de grupo para determinar quais permissões de acesso S3 os membros deste grupo terão.
   - **No S3 Access**: Padrão. Os usuários deste grupo não têm acesso a recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar essa opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
   - **Acesso somente leitura**: Os usuários deste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo somente leitura aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
   - **Acesso total**: Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo de acesso total aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
   - **Custom**: Os usuários do grupo recebem as permissões que você especificar na caixa de texto. Consulte as instruções para implementar um aplicativo cliente S3 para obter informações detalhadas sobre políticas de grupo, incluindo sintaxe de linguagem e exemplos.
10. Se você selecionou **Personalizado**, digite a política de grupo. Cada política de grupo tem um limite de tamanho de 5.120 bytes. Você deve inserir uma string formatada JSON válida.

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

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

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

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

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

13. Selecione **Finish**.

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

Crie grupos para um locatário Swift

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

O que você vai precisar

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

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

Passos

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

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

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

4. Introduza o nome do grupo.
   - **Local group**: Insira um nome de exibição e um nome exclusivo. Pode editar o nome de apresentação mais tarde.
   - **Federated group**: Insira o nome exclusivo. Para o ative Directory, o nome exclusivo é o nome associado ao `sAMAccountName` atributo. Para OpenLDAP, o nome exclusivo é o nome associado ao `uid` atributo.
5. Selecione **continuar**.
6. Selecione um modo de acesso. Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como somente leitura, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.
   - **Leitura-escrita** (padrão): Os usuários podem fazer login no Gerenciador do Tenant e gerenciar a configuração do locatário.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações nem executar nenhuma operação no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. Os usuários locais só de leitura podem alterar suas próprias senhas.

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

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

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

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

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

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

12. Selecione **Finish**.

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

Informações relacionadas

Permissões de gerenciamento do locatário

Use Swift

Permissões de gerenciamento do locatário

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

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

- Visualizar o painel de instrumentos

- Alterar sua própria senha (para usuários locais)

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

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

Pode atribuir as seguintes permissões a um grupo. Observe que S3 locatários e locatários Swift têm permissões de grupo diferentes. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Permissão	Descrição
Acesso à raiz	Fornece acesso total ao Gerenciador do Locatário e à API de Gerenciamento do Locatário. **Observação:** os usuários do Swift devem ter permissão de acesso root para entrar na conta do locatário.
Administrador	Apenas inquilinos Swift. Fornece acesso total aos contentores e objetos Swift para essa conta de locatário **Observação:** os usuários do Swift devem ter a permissão Swift Administrator para executar qualquer operação com a Swift REST API.
Gerencie suas próprias credenciais S3	Apenas S3 inquilinos. Permite que os usuários criem e removam suas próprias chaves de acesso S3. Os usuários que não têm essa permissão não veem a opção de menu **ARMAZENAMENTO (S3) My S3 Access Keys**.
Gerenciar todos os baldes	• S3 locatários: Permite que os usuários usem o Gerenciador do locatário e a API de gerenciamento do locatário para criar e excluir buckets do S3 e gerenciar as configurações de todos os buckets do S3 na conta do locatário, independentemente das políticas de bucket ou grupo do S3. Os usuários que não têm essa permissão não veem a opção de menu **Buckets**. • Swift tenants: Permite que usuários Swift controlem o nível de consistência para contentores Swift usando a API de Gerenciamento do locatário. **Observação:** você só pode atribuir a permissão Gerenciar todos os buckets a grupos Swift a partir da API de Gerenciamento de locatário. Você não pode atribuir essa permissão a grupos Swift usando o Gerenciador de inquilinos.

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

Informações relacionadas

Use S3

Use Swift

Ver e editar detalhes do grupo

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

O que você vai precisar

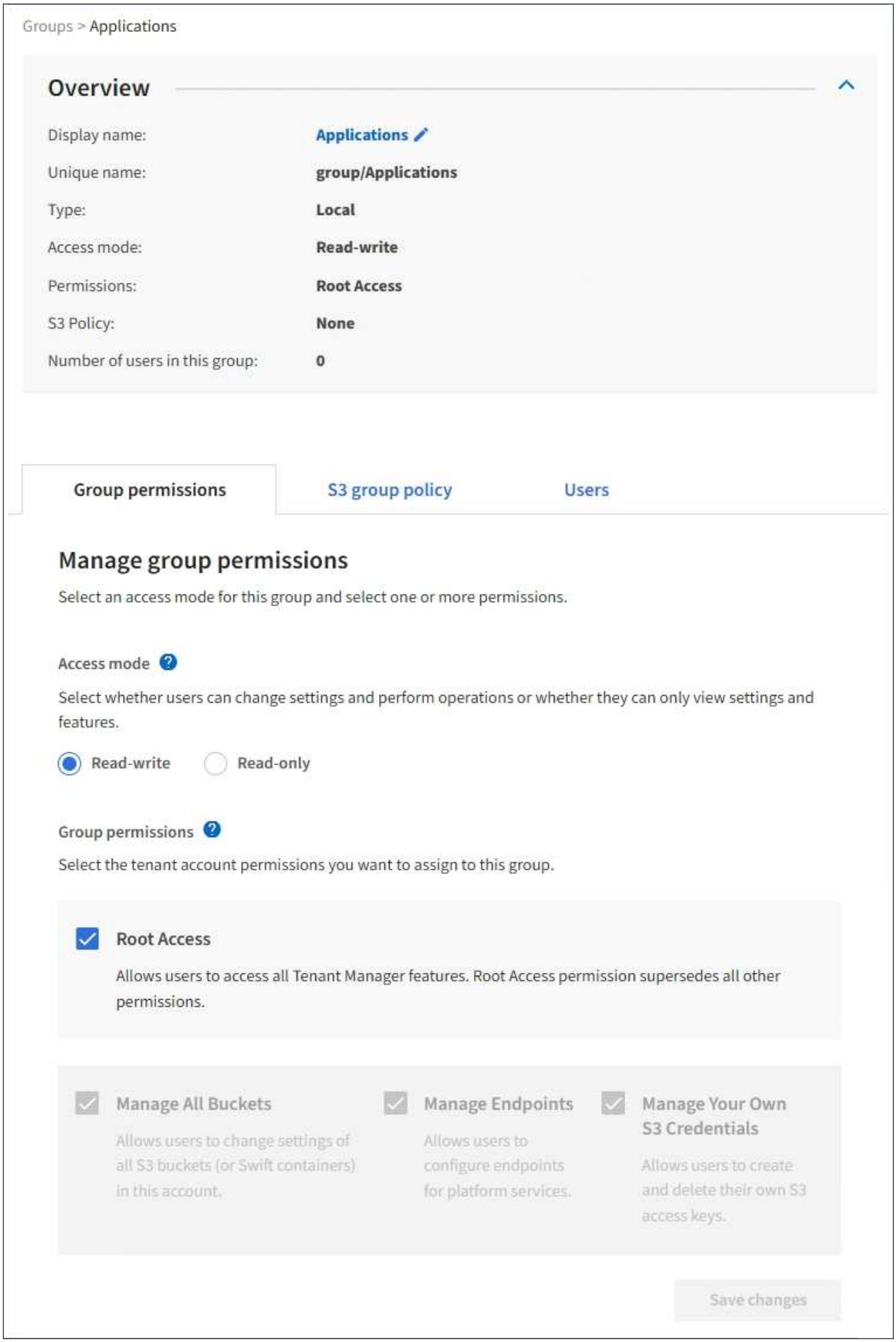
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

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

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

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


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

3. Faça alterações nas definições do grupo conforme necessário.

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

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

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

   b. Opcionalmente, atualize as permissões.

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

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

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

   d. Opcionalmente, adicione ou remova usuários.

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

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

Informações relacionadas

Criar grupos para S3 inquilino

Crie grupos para o locatário Swift

Adicione usuários a um grupo local

Você pode adicionar usuários a um grupo local conforme necessário.

O que você vai precisar

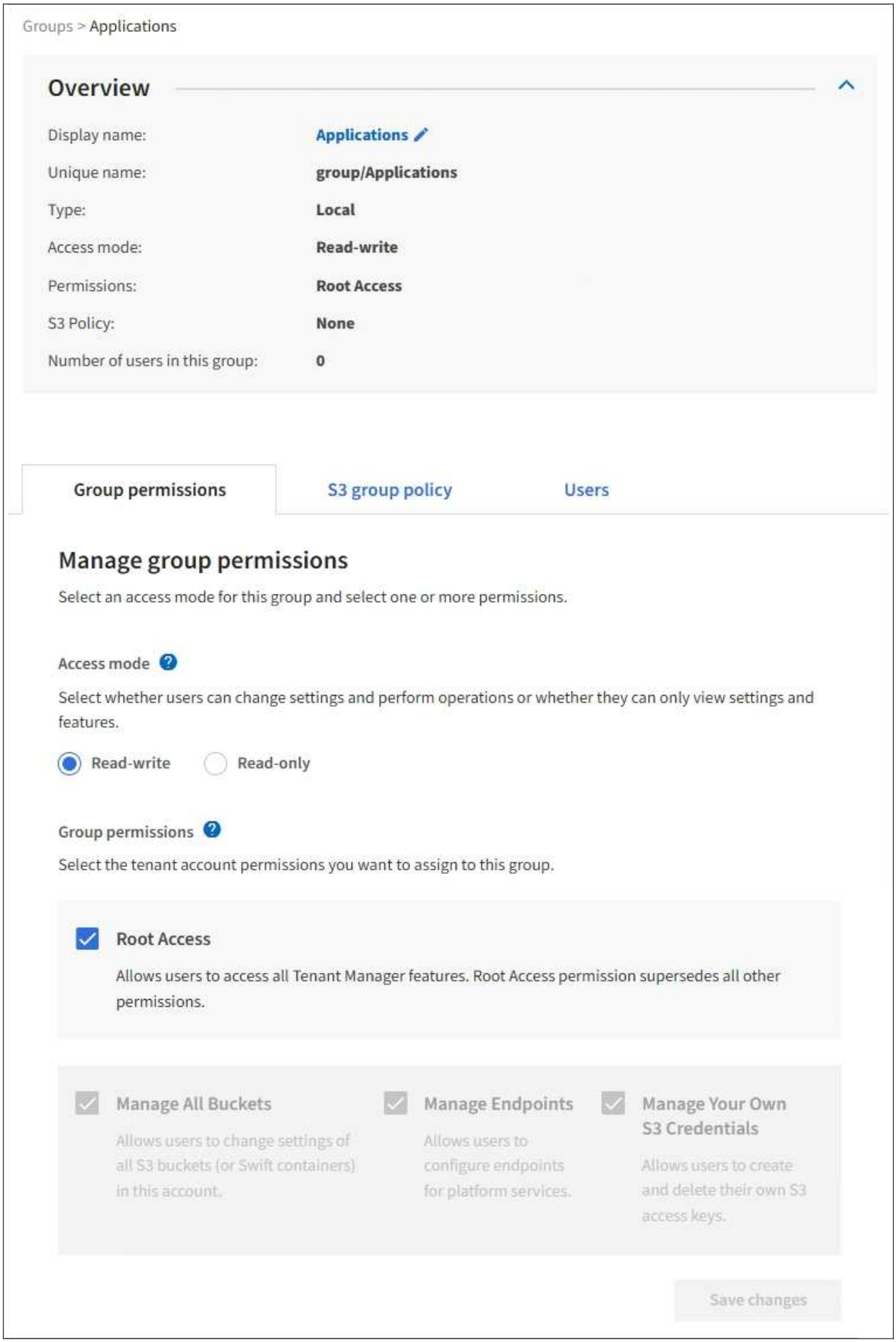
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve pertencer a um grupo de usuários que tenha a permissão de acesso root.

Passos

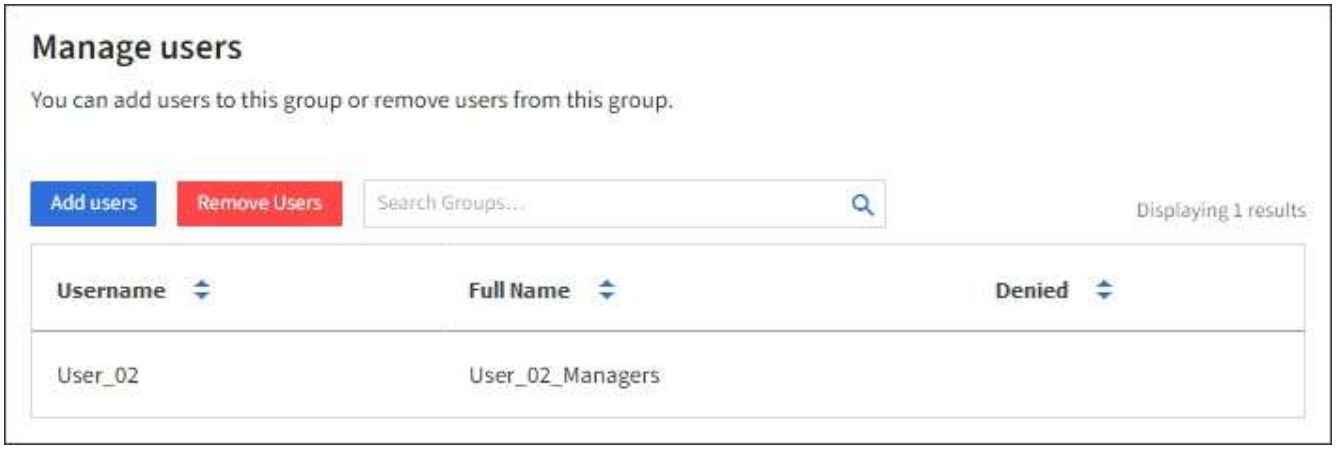
1. Selecione **GERENCIAMENTO DE ACESSO grupos**.
2. Selecione o nome do grupo local ao qual deseja adicionar usuários.

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

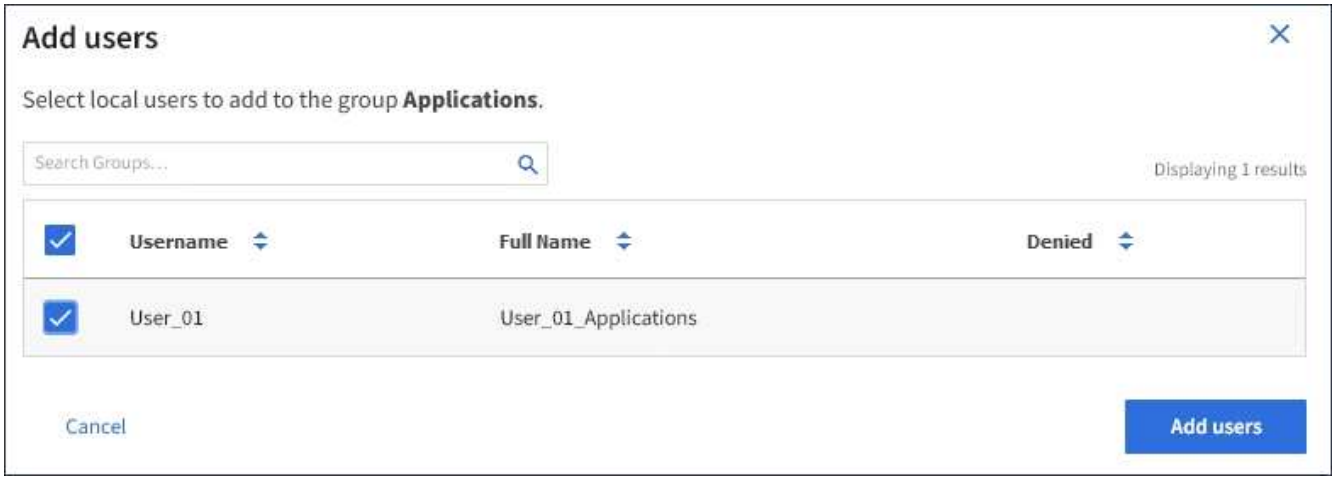
   A página de detalhes do grupo é exibida.


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

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



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



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

Editar nome do grupo

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

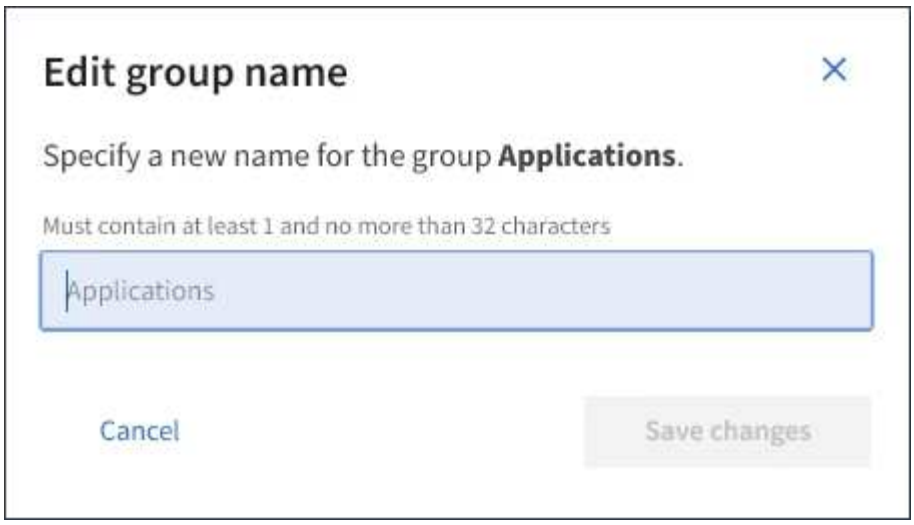
O que você vai precisar

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

Passos

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

   A caixa de diálogo Editar nome do grupo é exibida.



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

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

5. Selecione **Salvar alterações**.

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

Grupo duplicado

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

O que você vai precisar

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

Passos

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

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

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

associado ao `sAMAccountName` atributo. Para OpenLDAP, o nome exclusivo é o nome associado ao `uid` atributo.

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

Eliminar grupo

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

O que você vai precisar

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

Passos

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

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

   É apresentada uma mensagem de confirmação.

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

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

Gerenciar usuários locais

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

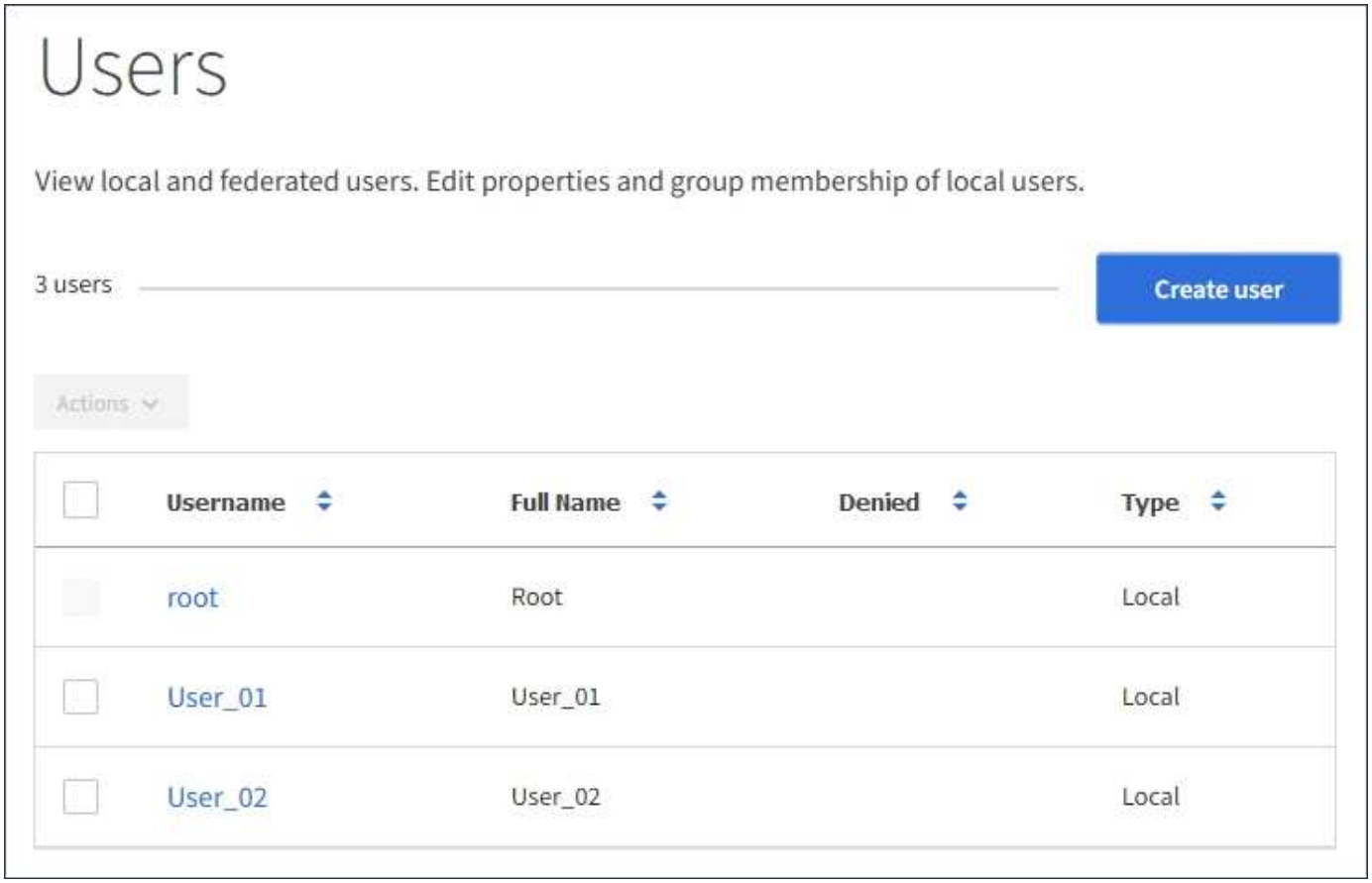
O que você vai precisar

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

> Se o logon único (SSO) estiver habilitado para o seu sistema StorageGRID, os usuários locais não poderão fazer login no Gerenciador do Locatário ou na API de Gerenciamento do Locatário, embora possam usar aplicativos cliente S3 ou Swift para acessar os recursos do locatário, com base nas permissões de grupo.

Acesse a página usuários

Selecione **GERENCIAMENTO DE ACESSO usuários**.



Crie usuários locais

Você pode criar usuários locais e atribuí-los a um ou mais grupos locais para controlar suas permissões de acesso.

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

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

Passos

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

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

   Os usuários que não pertencem a nenhum grupo não terão permissões de gerenciamento. As permissões são cumulativas. Os usuários terão todas as permissões para todos os grupos aos quais pertencem.
5. Selecione **criar usuário**.

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

Editar detalhes do utilizador

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

Passos

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

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

Você não pode alterar o nome de usuário.

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

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

Duplicar usuários locais

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

Passos

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

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

   Os usuários que não pertencem a nenhum grupo não terão permissões de gerenciamento. As permissões são cumulativas. Os usuários terão todas as permissões para todos os grupos aos quais pertencem.
6. Selecione **criar usuário**.

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

Eliminar utilizadores locais

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

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

Passos

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

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

Gerenciar contas de locatários do S3

Gerenciar S3 chaves de acesso

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

Sobre esta tarefa

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

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

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

Crie suas próprias chaves de acesso S3

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

O que você vai precisar

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

Sobre esta tarefa

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

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

- Defina um tempo de expiração para que suas chaves limitem seu acesso a um determinado período de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco se o ID da chave de acesso e a

chave de acesso secreta forem acidentalmente expostos. As chaves expiradas são removidas automaticamente.

- Se o risco de segurança em seu ambiente for baixo e você não precisar criar novas chaves periodicamente, não será necessário definir um tempo de expiração para suas chaves. Se você decidir mais tarde criar novas chaves, exclua as chaves antigas manualmente.

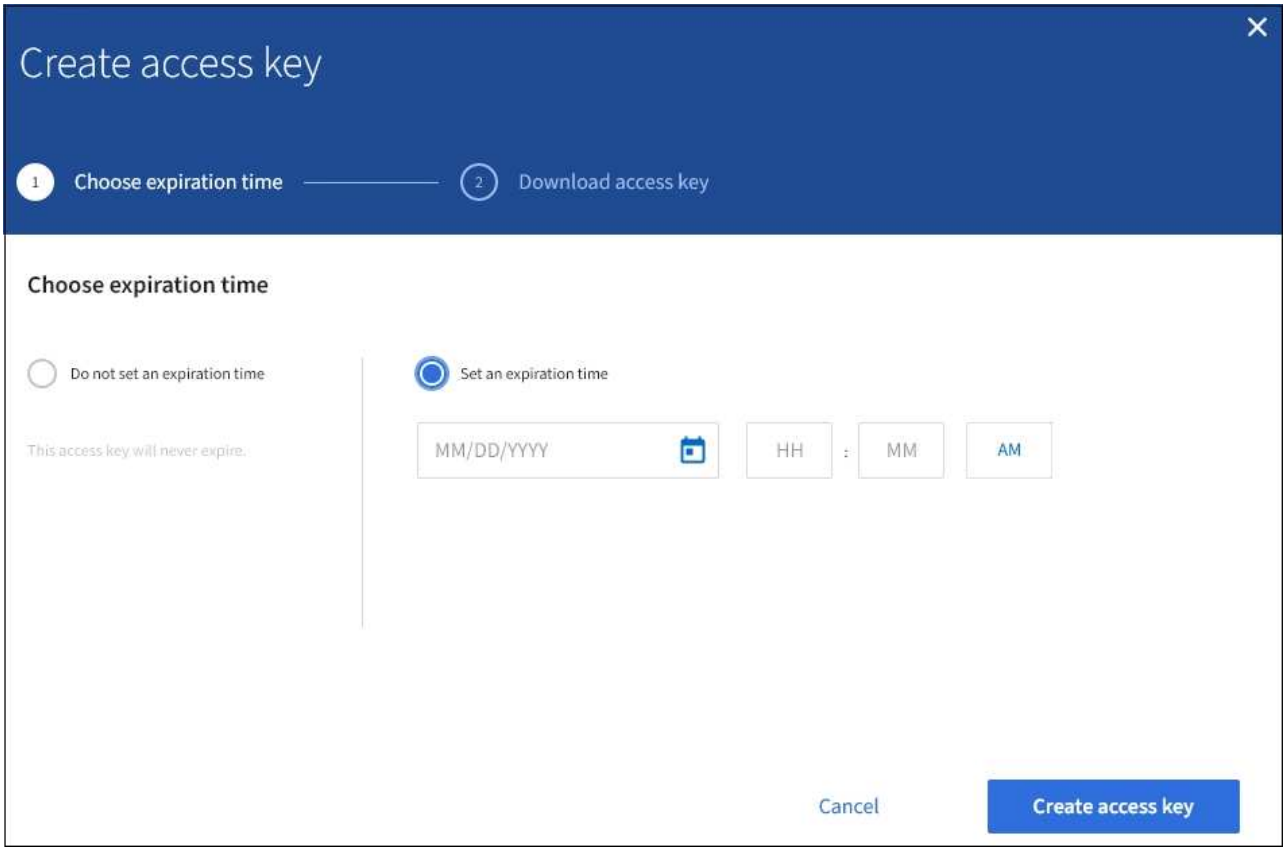
> Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidos para a sua conta no Gerenciador do Locatário. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Gire as chaves de acesso regularmente, remova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

Passos

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

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

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

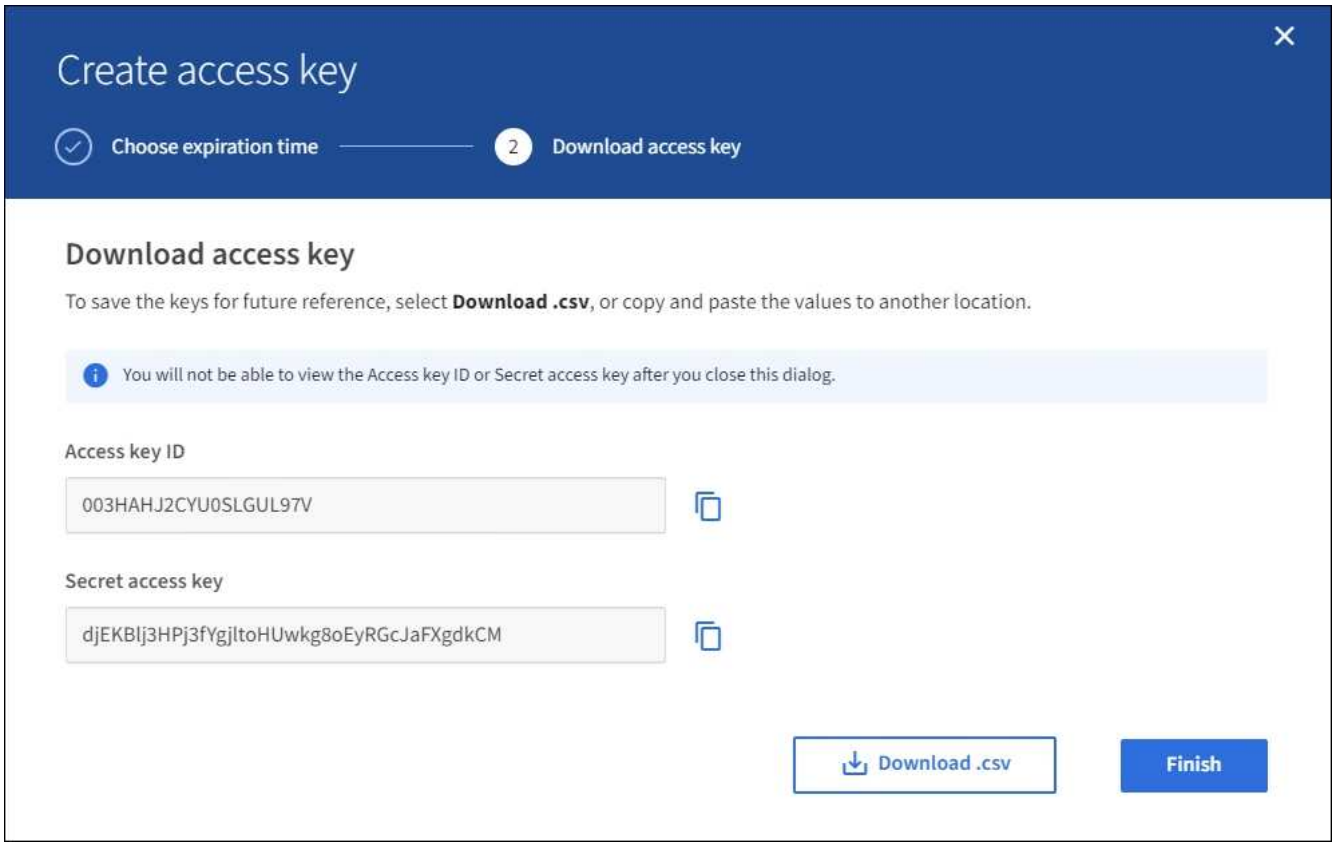


4. Selecione **criar chave de acesso**.

   A caixa de diálogo Download Access Key (Transferir chave de acesso) é exibida, listando o ID da chave de acesso e a chave de acesso secreta.

5. Copie o ID da chave de acesso e a chave de acesso secreta para um local seguro ou selecione **Transferir .csv** para guardar um ficheiro de folha de cálculo que contenha a ID da chave de acesso e a chave de acesso secreta.

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



6. Selecione **Finish**.

   A nova chave está listada na página Minhas chaves de acesso. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Veja as suas teclas de acesso S3

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

O que você vai precisar

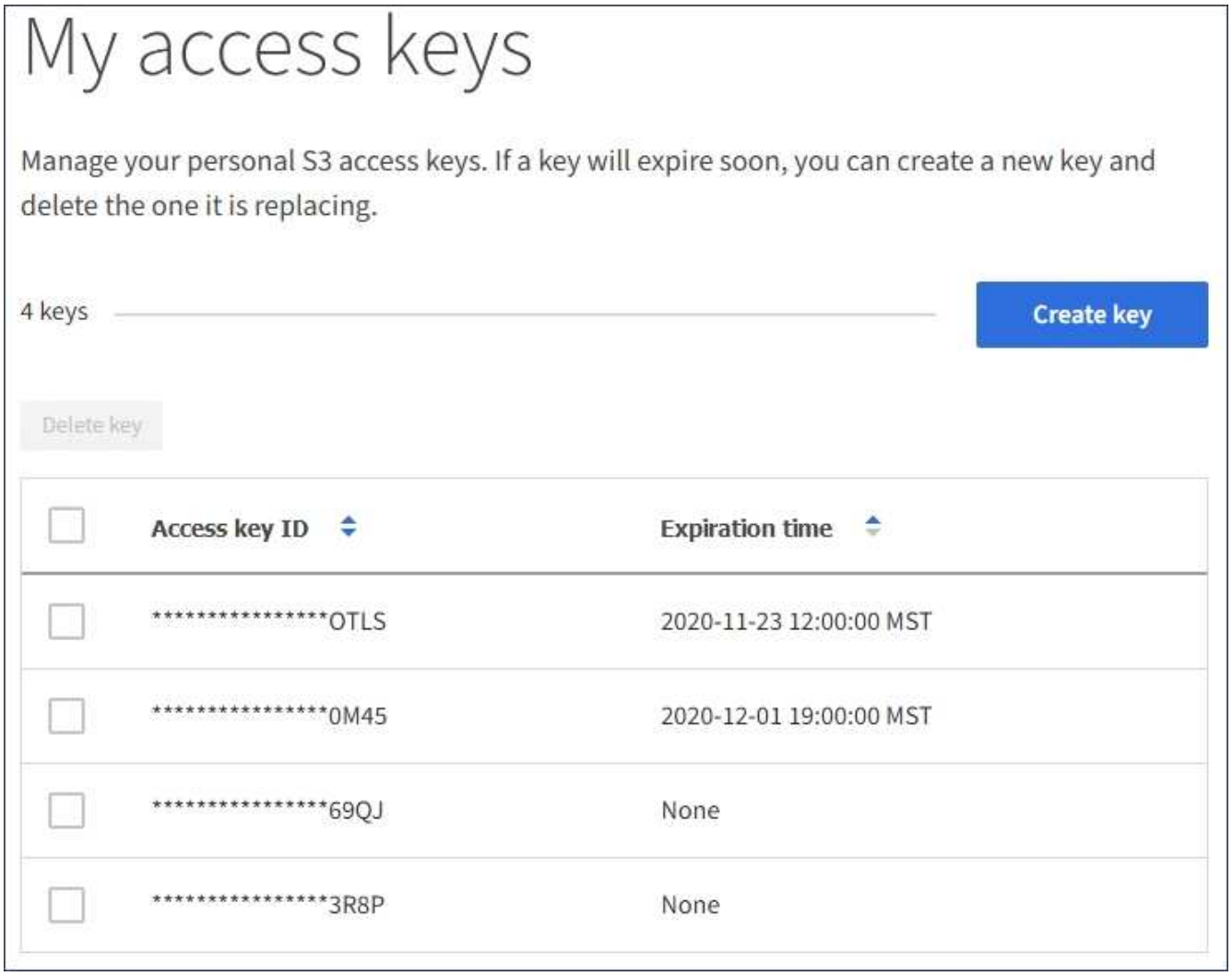
- Você deve estar conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você deve ter a permissão Gerenciar suas próprias credenciais do S3.

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

Passos

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

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



2. Classifique as chaves por **tempo de expiração** ou **ID da chave de acesso**.
3. Conforme necessário, crie novas chaves e exclua manualmente as chaves que você não está mais usando.

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

   As chaves expiradas são removidas automaticamente.

Informações relacionadas

Crie suas próprias chaves de acesso S3

Elimine as suas próprias chaves de acesso S3

Elimine as suas próprias chaves de acesso S3

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

O que você vai precisar

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

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

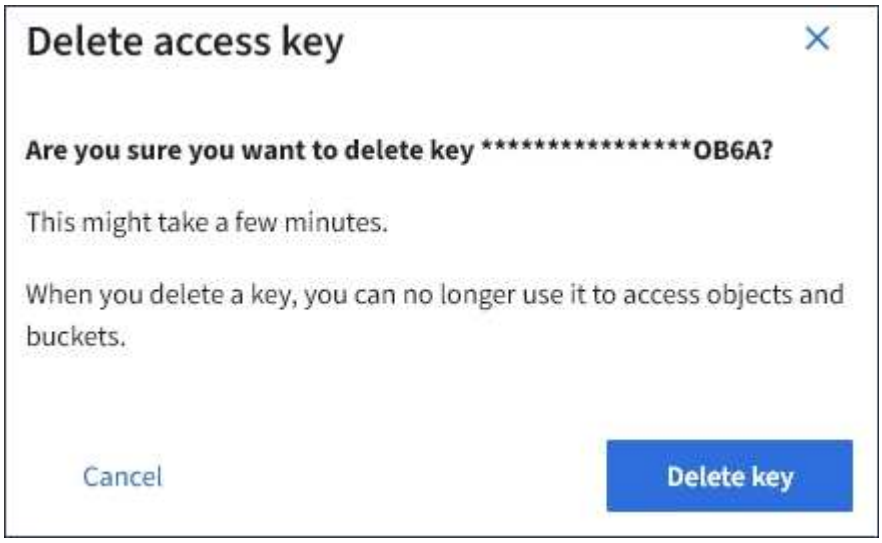
Passos

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

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

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

   É apresentada uma caixa de diálogo de confirmação.



4. Selecione **Delete key**.

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

Crie as chaves de acesso S3 de outro usuário

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

O que você vai precisar

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

Sobre esta tarefa

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

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

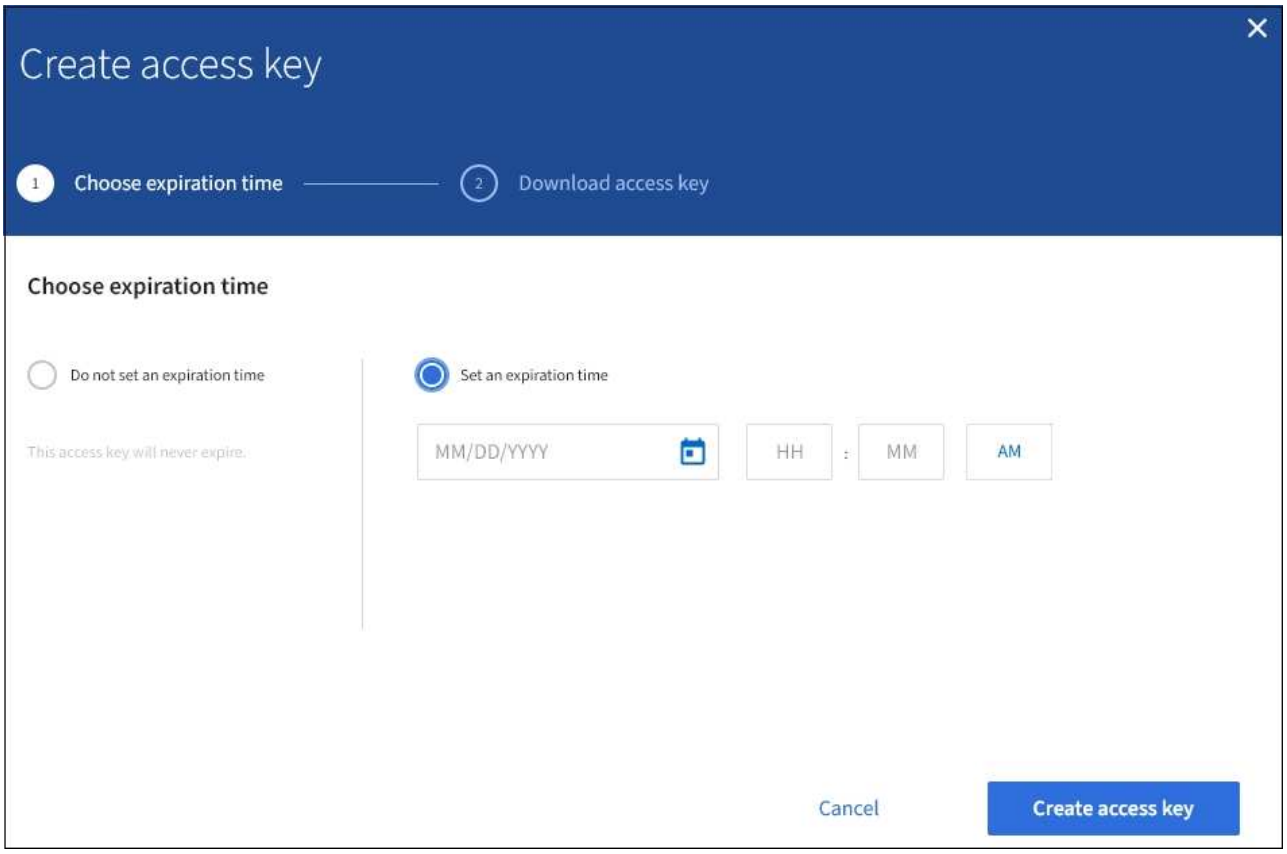
- Defina um tempo de expiração para as teclas para limitar o acesso do usuário a um determinado período de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco se o ID da chave de acesso e a chave de acesso secreta forem acidentalmente expostos. As chaves expiradas são removidas automaticamente.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

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

Passos

1. Selecione **GERENCIAMENTO DE ACESSO usuários**.
2. Selecione o usuário cujas chaves de acesso S3 você deseja gerenciar.

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

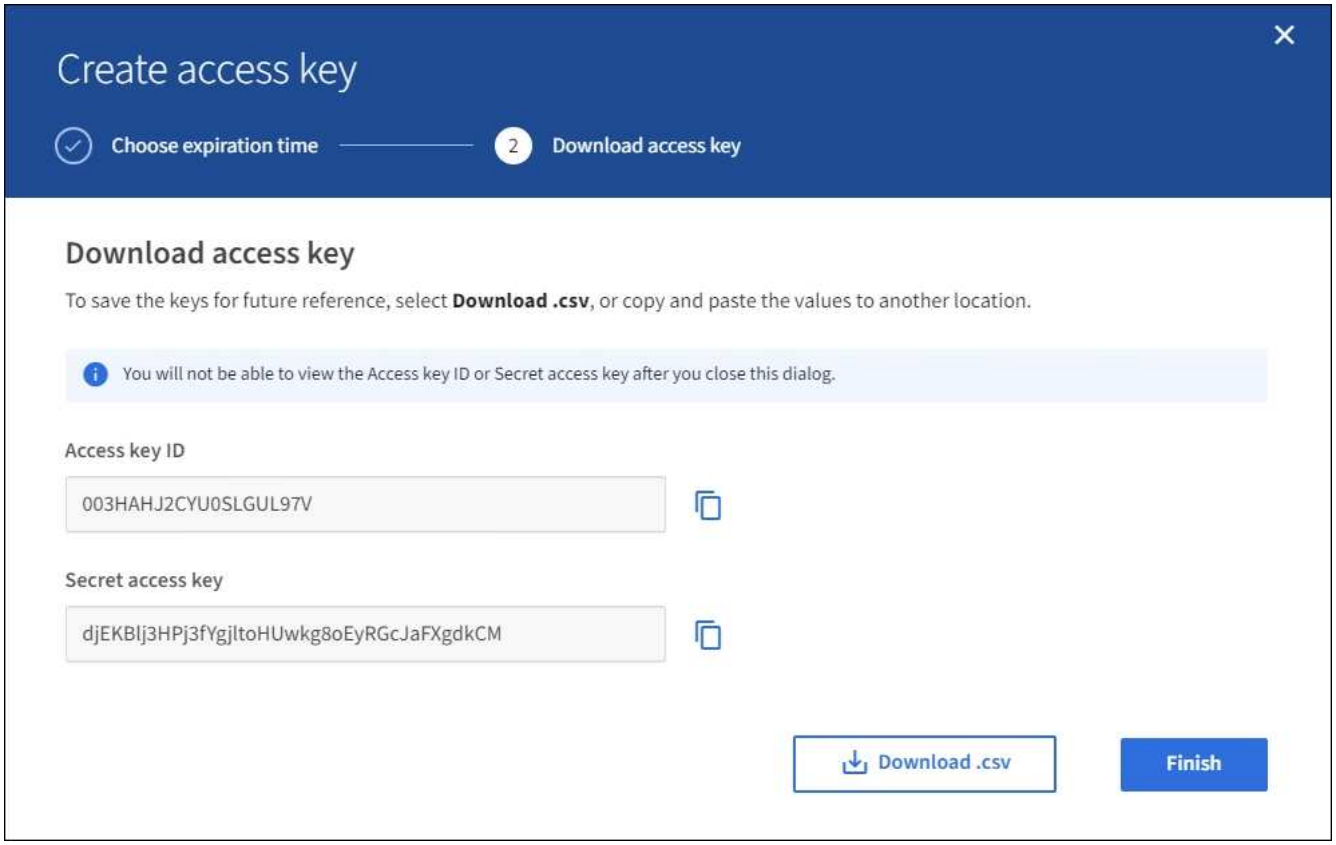


5. Selecione **criar chave de acesso**.

   A caixa de diálogo Download Access Key (Transferir chave de acesso) é exibida, listando o ID da chave de acesso e a chave de acesso secreta.

6. Copie o ID da chave de acesso e a chave de acesso secreta para um local seguro ou selecione **Transferir .csv** para guardar um ficheiro de folha de cálculo que contenha a ID da chave de acesso e a chave de acesso secreta.

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



7. Selecione **Finish**.

   A nova chave está listada na guia teclas de acesso da página de detalhes do usuário. As alterações podem levar até 15 minutos para entrar em vigor devido ao armazenamento em cache.

Informações relacionadas

Permissões de gerenciamento do locatário

Veja as S3 chaves de acesso de outro usuário

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

O que você vai precisar

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

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

Passos

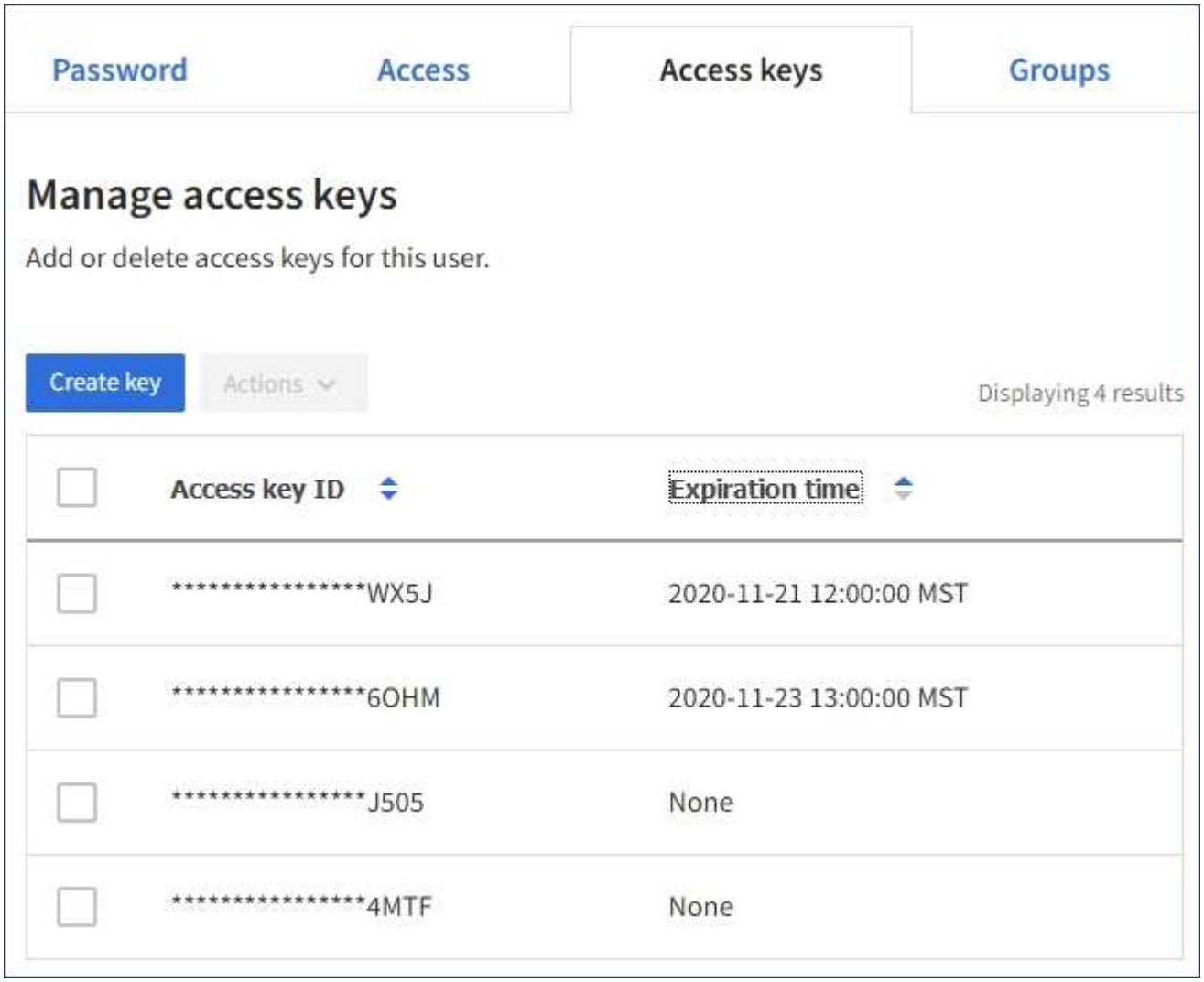
1. Selecione **GERENCIAMENTO DE ACESSO usuários**.

   A página usuários é exibida e lista os usuários existentes.

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

   É apresentada a página Detalhes do utilizador.

3. Selecione **teclas de acesso**.



4. Classifique as chaves por **tempo de expiração** ou **ID da chave de acesso**.
5. Conforme necessário, crie novas chaves e exclua manualmente as chaves que não estiverem mais em uso.

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

   As chaves expiradas são removidas automaticamente.

Informações relacionadas

Crie as chaves de acesso S3 de outro usuário

Eliminar as S3 chaves de acesso de outro utilizador

Exclua as S3 chaves de acesso de outro usuário

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

O que você vai precisar

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

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

Passos

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

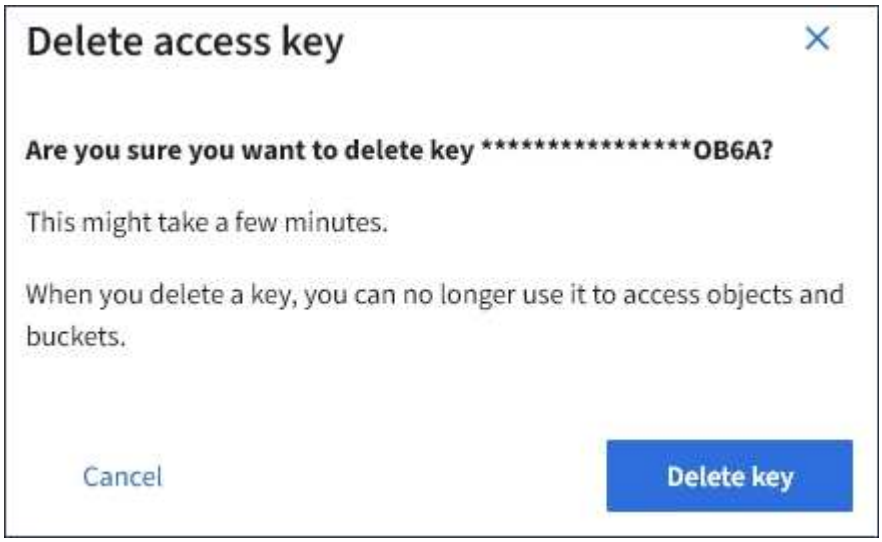
   A página usuários é exibida e lista os usuários existentes.

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

   É apresentada a página Detalhes do utilizador.

3. Selecione **teclas de acesso** e, em seguida, marque a caixa de seleção para cada chave de acesso que deseja excluir.
4. Selecione **ações Excluir tecla selecionada**.

   É apresentada uma caixa de diálogo de confirmação.



5. Selecione **Delete key**.

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

Gerenciar buckets do S3

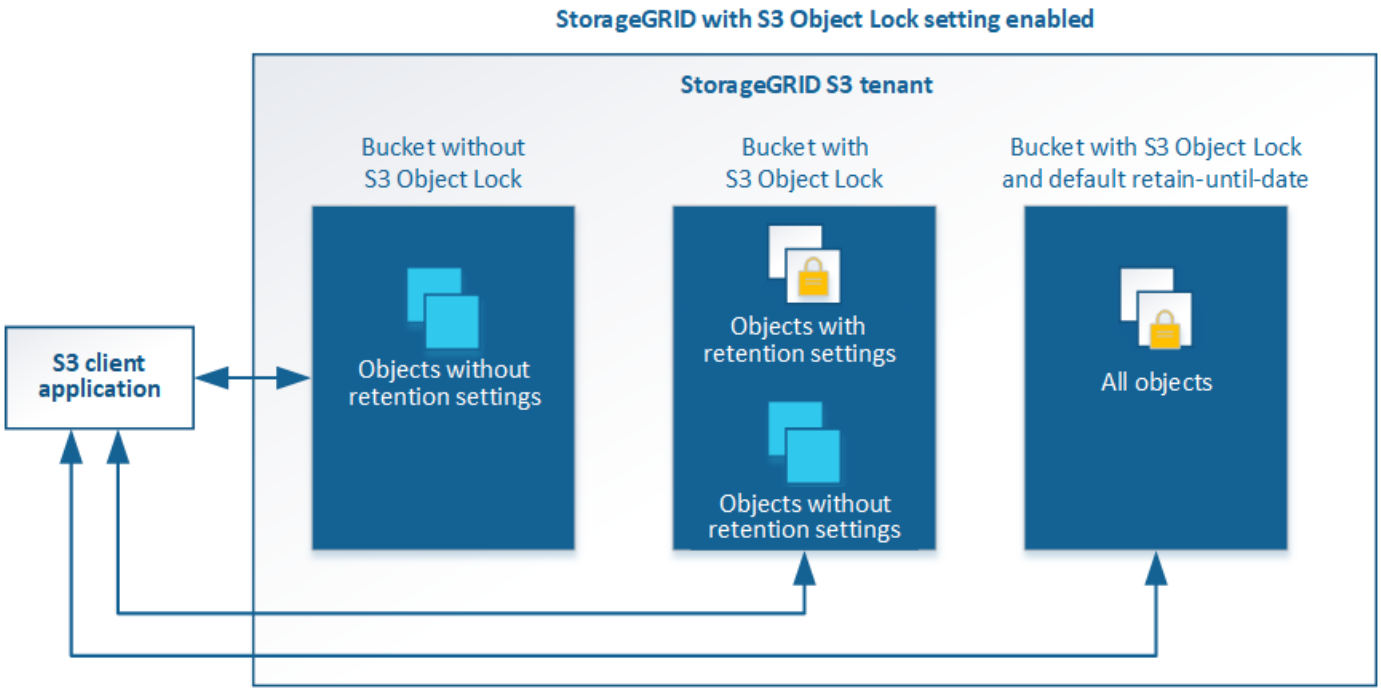
Use o bloqueio de objetos S3 com locatários

Você pode usar o recurso bloqueio de objetos S3 no StorageGRID se seus objetos precisarem cumprir com os requisitos regulamentares para retenção.

O que é S3 Object Lock?

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

Como mostrado na figura, quando a configuração global de bloqueio de objeto S3D está ativada para um sistema StorageGRID, uma conta de locatário S3D pode criar buckets com ou sem bloqueio de objeto S3D ativado. Se um bucket tiver o bloqueio de objeto S3 ativado, os aplicativos cliente S3 podem, opcionalmente, especificar configurações de retenção para qualquer versão de objeto nesse bucket. Uma versão de objeto deve ter configurações de retenção especificadas para ser protegida pelo bloqueio de objeto S3.



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

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

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

- **Retenção legal**: Aplicar uma retenção legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar colocar uma retenção legal em um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até que seja explicitamente removida. As obrigações legais são independentes da retenção até à data.

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

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

Gerenciar buckets em conformidade com o legado

O recurso bloqueio de objetos S3 substitui o recurso de conformidade que estava disponível nas versões anteriores do StorageGRID. Se você criou buckets compatíveis usando uma versão anterior do StorageGRID, poderá continuar gerenciando as configurações desses buckets. No entanto, não será mais possível criar novos buckets compatíveis. Para obter instruções, consulte o artigo da base de dados de Conhecimento da NetApp.

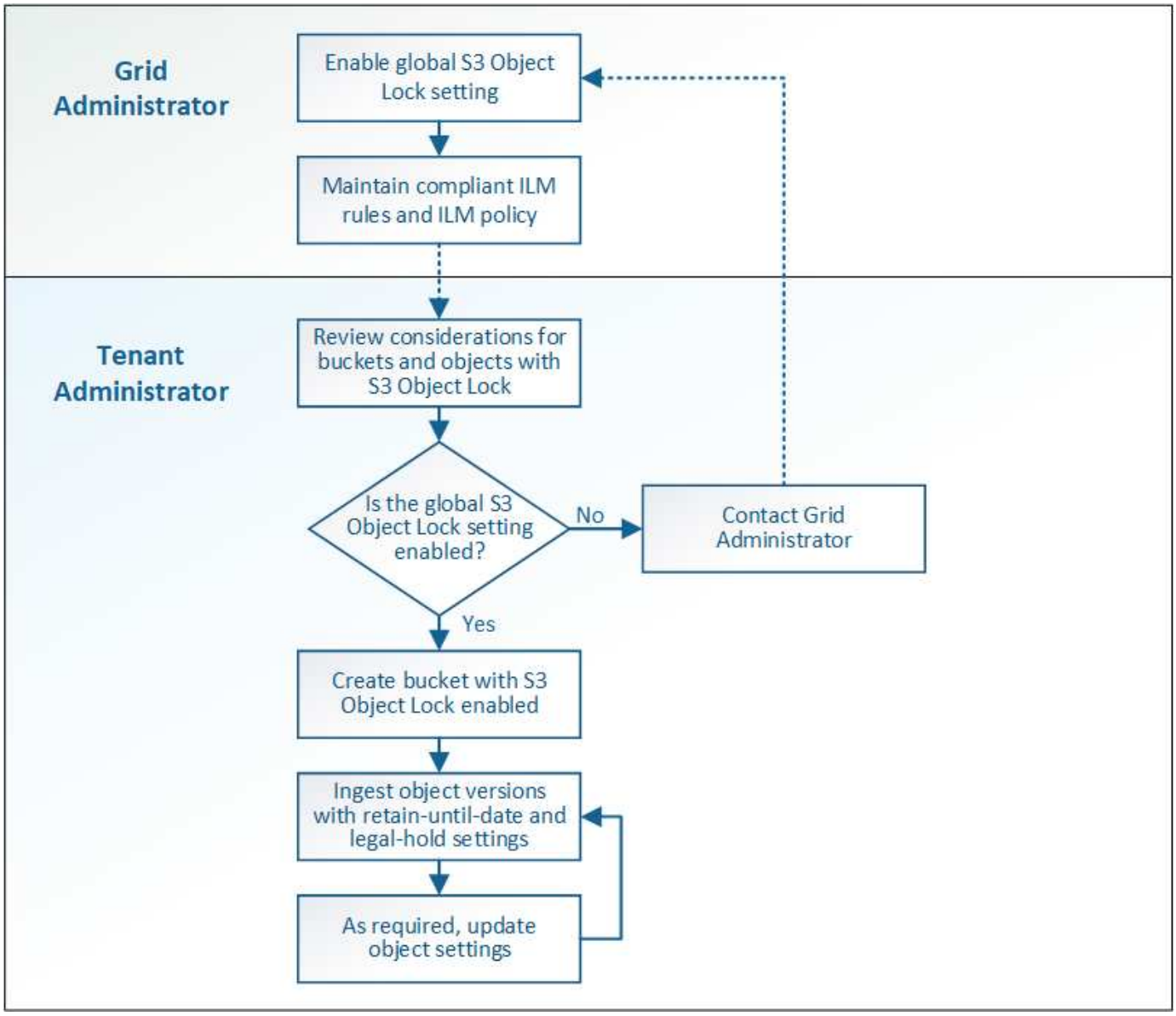
"Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

S3 fluxo de trabalho Object Lock

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

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

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



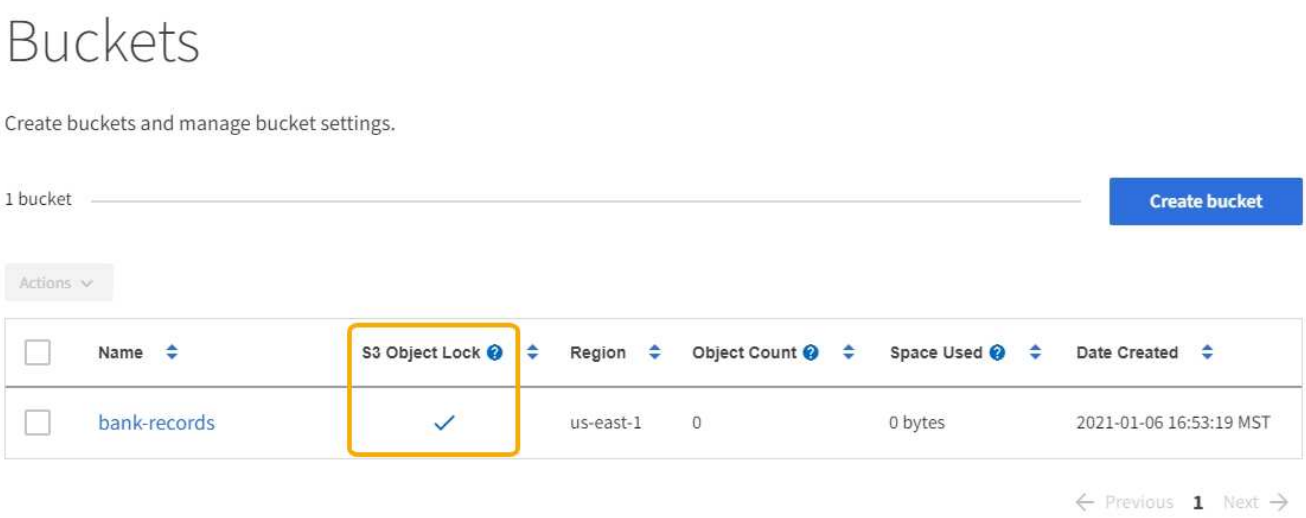
Requisitos para o bloqueio de objetos S3

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

Requisitos para buckets com bloqueio de objeto S3 ativado

- Se a configuração global de bloqueio de objeto S3 estiver ativada para o sistema StorageGRID, você poderá usar o Gerenciador de locatário, a API de gerenciamento de locatário ou a API REST S3 para criar buckets com o bloqueio de objeto S3 ativado.

  Este exemplo do Gerenciador do Locatário mostra um bucket com o bloqueio de objeto S3 ativado.



- Se você planeja usar o bloqueio de objetos S3D, você deve ativar o bloqueio de objetos S3D ao criar o bucket. Não é possível ativar o bloqueio de objetos S3D para um bucket existente.
- O controle de versão do bucket é necessário com o S3 Object Lock. Quando o bloqueio de objeto S3 está ativado para um bucket, o StorageGRID ativa automaticamente o controle de versão desse bucket.
- Depois de criar um bucket com o bloqueio de objetos S3 ativado, não é possível desativar o bloqueio de objetos S3 ou suspender o controle de versão desse bucket.
- Opcionalmente, você pode configurar a retenção padrão para um bucket. Quando uma versão de objeto é carregada, a retenção padrão é aplicada à versão do objeto. Você pode substituir o intervalo padrão especificando um modo de retenção e manter até a data na solicitação para carregar uma versão de objeto.
- A configuração do ciclo de vida do bucket é compatível com buckets do ciclo de vida do objeto do S3.
- A replicação do CloudMirror não é compatível com buckets com o S3 Object Lock ativado.

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

- Para proteger uma versão de objeto, o aplicativo cliente S3 deve configurar a retenção padrão de bucket ou especificar configurações de retenção em cada solicitação de upload.
- Você pode aumentar a data de retenção até uma versão de objeto, mas nunca pode diminuir esse valor.
- Se você for notificado de uma ação legal pendente ou investigação regulatória, poderá preservar informações relevantes colocando uma retenção legal em uma versão de objeto. Quando uma versão de objeto está sob uma retenção legal, esse objeto não pode ser excluído do StorageGRID, mesmo que tenha atingido sua data de retenção até. Assim que a retenção legal for levantada, a versão do objeto pode ser excluída se a data de retenção for atingida.
- S3 Object Lock requer o uso de buckets versionados. As configurações de retenção se aplicam a versões de objetos individuais. Uma versão de objeto pode ter uma configuração de retenção de data e de retenção legal, uma mas não a outra, ou nenhuma. Especificar uma configuração reter-até-data ou retenção legal para um objeto protege apenas a versão especificada na solicitação. Você pode criar novas versões do objeto, enquanto a versão anterior do objeto permanece bloqueada.

Ciclo de vida dos objetos em buckets com o bloqueio de objetos S3 ativado

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

1. * Ingestão de objetos*

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

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

Crie um balde S3D.

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

O que você vai precisar

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

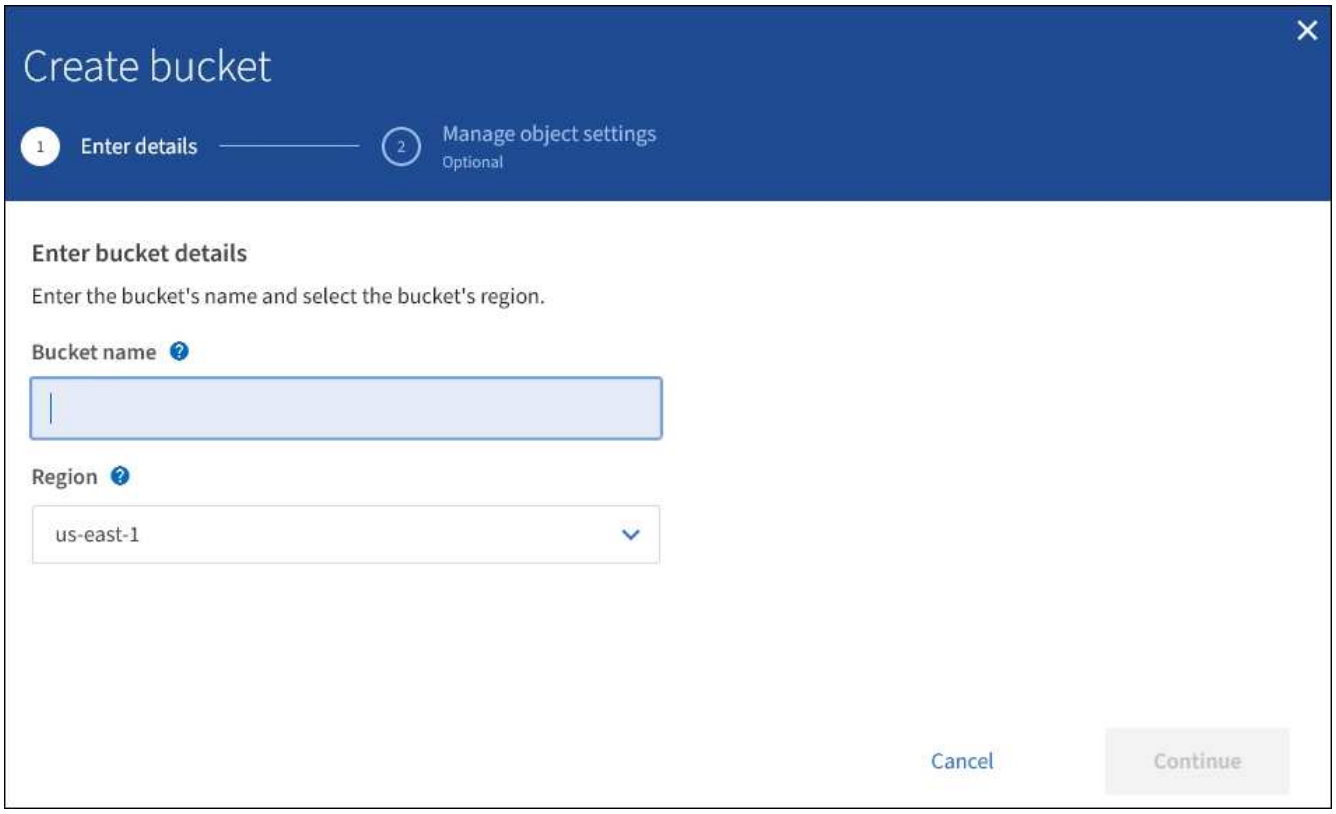
> As permissões para definir ou modificar as propriedades de bloqueio de objetos S3D de buckets ou objetos podem ser concedidas pelo política de bucket ou política de grupo.

- Se você planeja criar um bucket com o bloqueio de objeto S3, ativou a configuração global de bloqueio de objeto S3 para o sistema StorageGRID e revisou os requisitos para buckets e objetos do bloqueio de objeto S3.

  Use o bloqueio de objetos S3D.

Passos

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



3. Introduza um nome exclusivo para o intervalo.

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

   Os nomes dos buckets devem cumprir com estas regras:

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

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

4. Selecione a região para este intervalo.

   O administrador do StorageGRID gerencia as regiões disponíveis. A região de um bucket pode afetar a política de proteção de dados aplicada a objetos. Por padrão, todos os buckets são criados na `us-east-1` região.

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

5. Selecione **continuar**.
6. Opcionalmente, habilite o controle de versão de objetos para o bucket.

Ative o controle de versão de objetos se você quiser armazenar todas as versões de cada objeto neste intervalo. Em seguida, você pode recuperar versões anteriores de um objeto, conforme necessário.

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

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

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

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

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

8. Selecione **criar bucket**.

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

Informações relacionadas

Gerenciar objetos com ILM

Entenda a API de gerenciamento do locatário

Use S3

Veja os detalhes do balde S3

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

O que você vai precisar

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

Passos

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

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

2. Reveja as informações de cada balde.

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

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

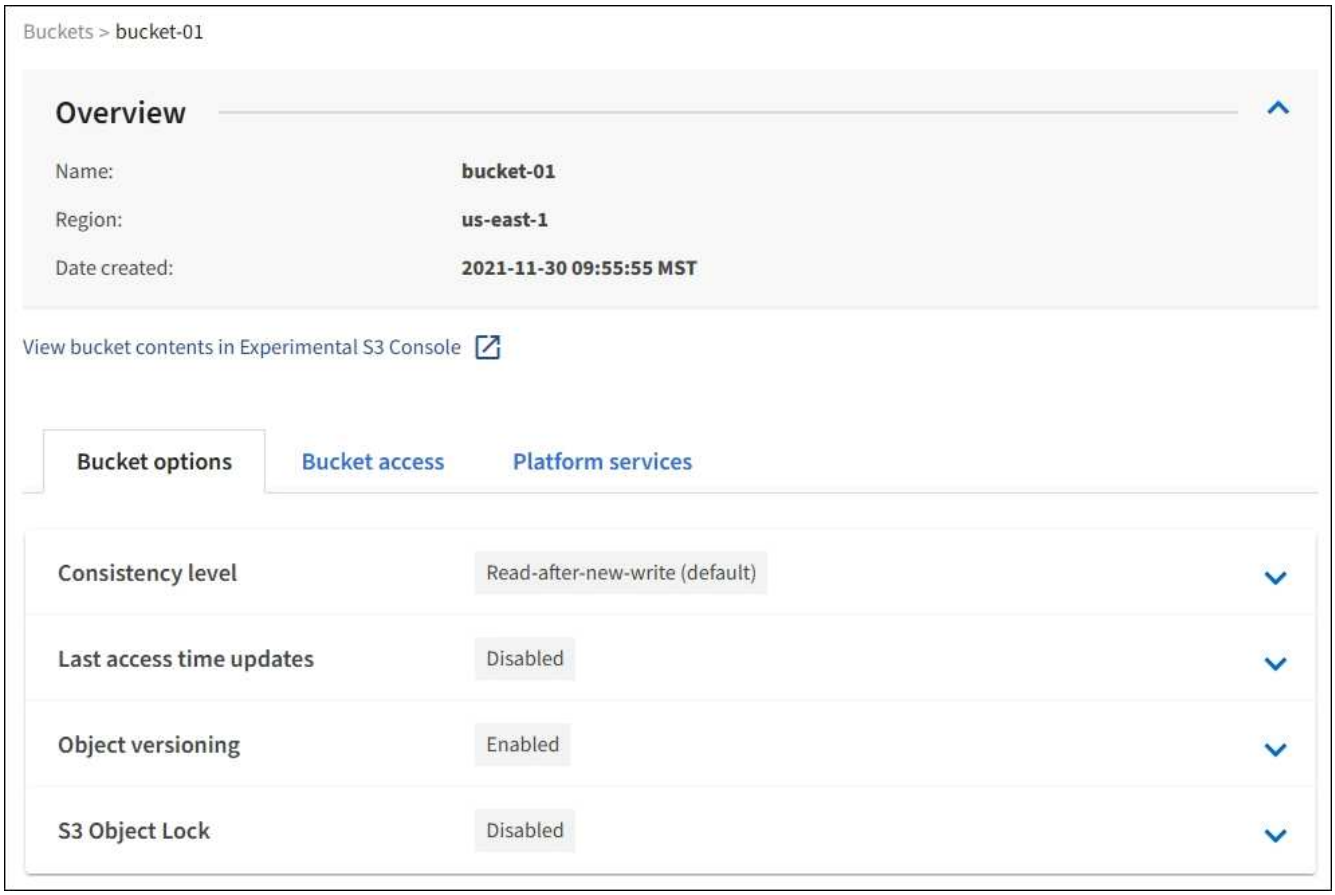
     Esta coluna não será exibida se a configuração global de bloqueio de objetos S3D estiver desativada. Esta coluna também mostra informações para quaisquer buckets em conformidade com o legado.

   - Região: A região do balde, que não pode ser alterada.
   - Contagem de objetos: O número de objetos neste intervalo.
   - Espaço usado: O tamanho lógico de todos os objetos neste intervalo. O tamanho lógico não inclui o espaço real necessário para cópias replicadas ou codificadas para apagamento ou metadados de objetos.
   - Data de criação: A data e a hora em que o intervalo foi criado.

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

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

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



Altere o nível de consistência

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

O que você vai precisar

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

Sobre esta tarefa

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

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

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

Passos

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

   É apresentada a página de detalhes do balde.

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

Ative ou desative as atualizações da última hora de acesso

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

Estas instruções aplicam-se apenas a sistemas StorageGRID que incluam pelo menos uma regra ILM que utilize a opção **último tempo de acesso** nas instruções de colocação. Você pode ignorar essas instruções se o seu sistema StorageGRID não incluir essa regra.

O que você vai precisar

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

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

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

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

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

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

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

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

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

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

Tipo de solicitação	Comportamento se a última hora de acesso estiver desativada (predefinição)		Comportamento se a última hora de acesso estiver ativada	
	Último tempo de acesso atualizado?	Objeto adicionado à fila de avaliação ILM?	Último tempo de acesso atualizado?	Objeto adicionado à fila de avaliação ILM?
Solicitação para recuperar um objeto, sua lista de controle de acesso ou seus metadados	Não	Não	Sim	Sim
Solicitação para atualizar os metadados de um objeto	Sim	Sim	Sim	Sim
Solicitação para copiar um objeto de um bucket para outro	• Não, para a cópia de origem • 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

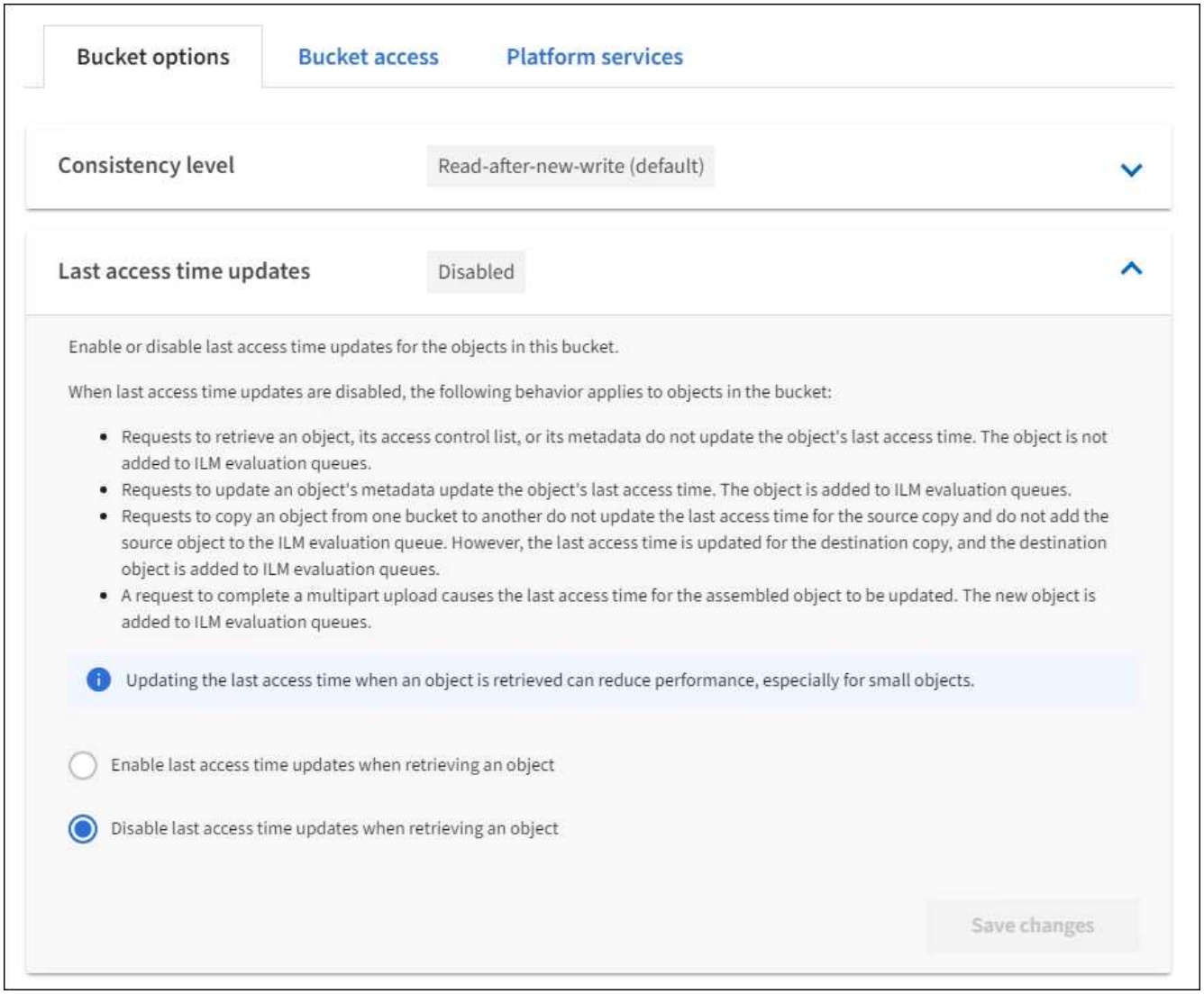
Pedido para concluir um carregamento multipart	Sim, para o objeto montado	Sim, para o objeto montado	Sim, para o objeto montado	Sim, para o objeto montado

Passos

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

   É apresentada a página de detalhes do balde.

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



5. Selecione **Salvar alterações**.

Informações relacionadas

Permissões de gerenciamento do locatário

Gerenciar objetos com ILM

Alterar o controle de versão de objetos para um bucket

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

O que você vai precisar

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

  Permissões de gerenciamento do locatário

Sobre esta tarefa

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

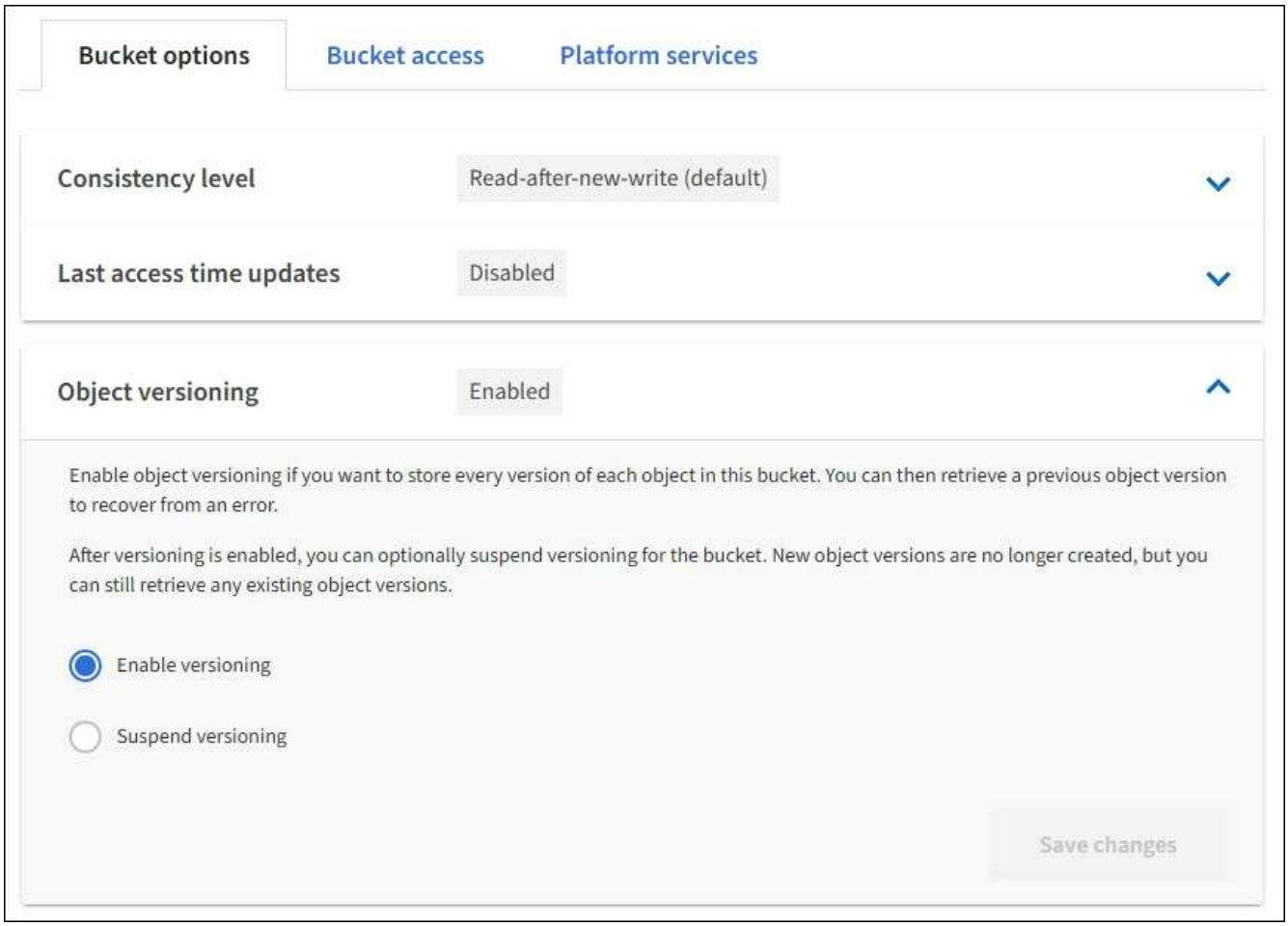
- Desativado: O controle de versão nunca foi habilitado
- Habilitado: O controle de versão está habilitado
- Suspenso: O controle de versão foi ativado anteriormente e está suspenso

Controle de versão de objeto S3

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

Passos

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



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

> Se o bloqueio de objeto S3 ou a conformidade legada estiver ativada, as opções **versão de objeto** serão desativadas.

Opção	Descrição
Habilite o controle de versão	Ative o controle de versão de objetos se você quiser armazenar todas as versões de cada objeto neste intervalo. Em seguida, você pode recuperar versões anteriores de um objeto, conforme necessário. Os objetos que já estavam no bucket serão versionados quando forem modificados por um usuário.
Suspenda o controle de versão	Suspenda o controle de versão do objeto se você não quiser mais criar novas versões de objeto. Você ainda pode recuperar quaisquer versões de objetos existentes.

5. Selecione **Salvar alterações**.

Configurar a partilha de recursos entre origens (CORS)

Você pode configurar o Compartilhamento de recursos entre origens (CORS) para um bucket do S3 se quiser que esse bucket e objetos nesse bucket estejam acessíveis a

aplicativos da Web em outros domínios.

O que você vai precisar

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

Sobre esta tarefa

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

Passos

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

   Este exemplo mostra o XML usado para ativar o CORS para um bucket S3. Esse XML permite que qualquer domínio envie SOLICITAÇÕES GET para o bucket, mas só permite que o `http://www.example.com` domínio envie SOLICITAÇÕES POST e EXCLUA. Todos os cabeçalhos de solicitação são permitidos.

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

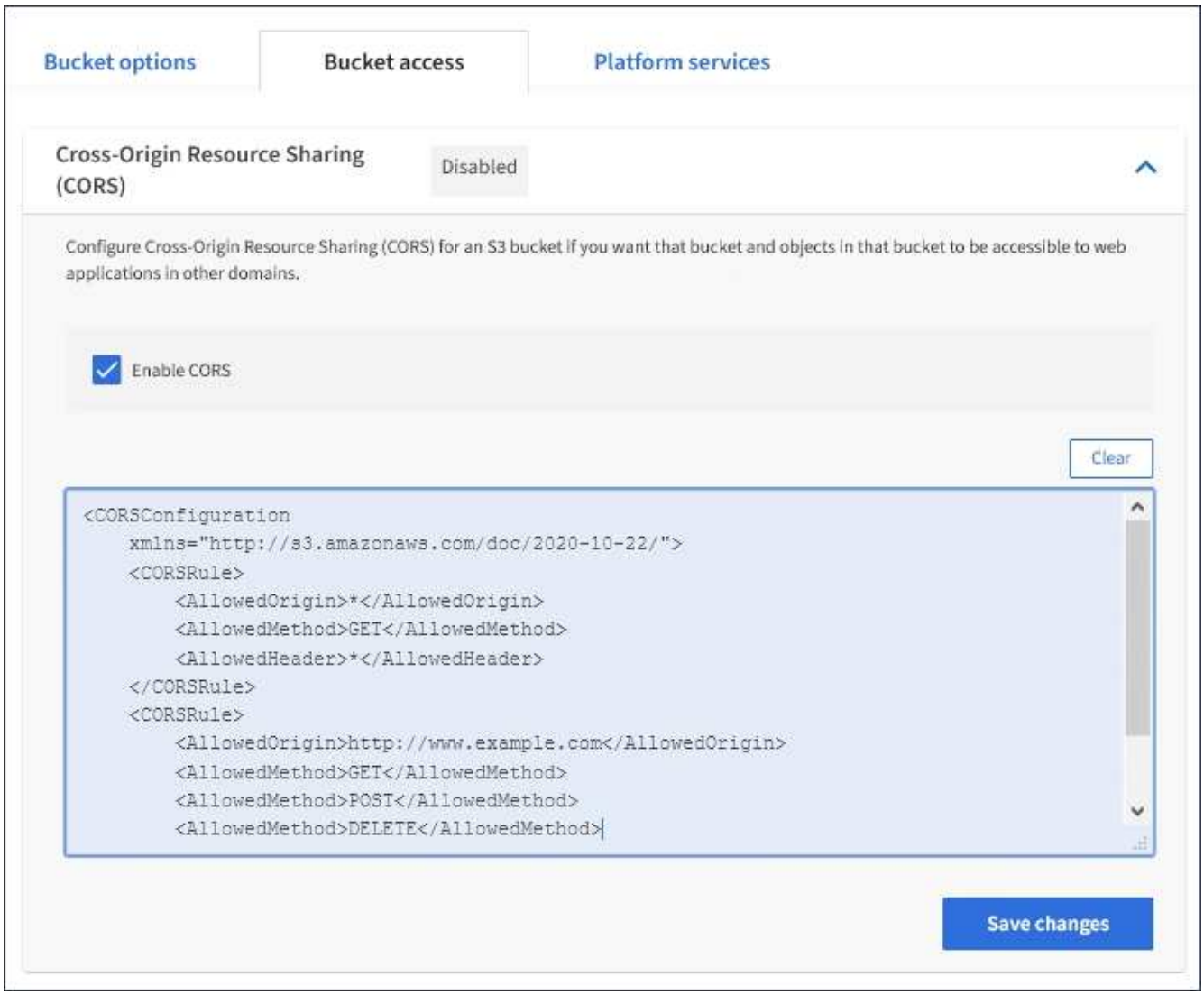
   Para obter mais informações sobre o XML de configuração do CORS, "Documentação do Amazon Web Services (AWS): Guia do desenvolvedor do Amazon Simple Storage Service" consulte .

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

   É apresentada a página de detalhes do balde.

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

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



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

Eliminar o balde S3

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

O que você vai precisar

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

Sobre esta tarefa

Estas instruções descrevem como excluir um bucket do S3 usando o Gerenciador do locatário. Também é possível excluir buckets do S3 usando o API de gerenciamento do locatário ou o S3 API REST.

Não é possível excluir um bucket do S3 se ele contiver objetos ou versões de objetos não atuais. Para obter informações sobre como os objetos com versão S3 são excluídos, consulte instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Passos

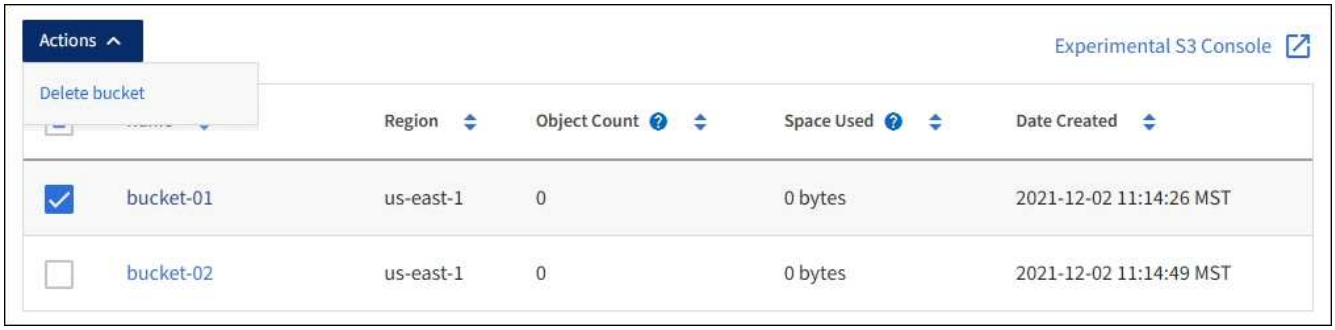
1. Selecione **STORAGE (S3)** > **Buckets**.

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

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

   O menu ações está ativado.

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



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

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

Se um balde não estiver vazio, é apresentada uma mensagem de erro. Você deve excluir todos os objetos antes de excluir um bucket.

Use o experimental S3 Console

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

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

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

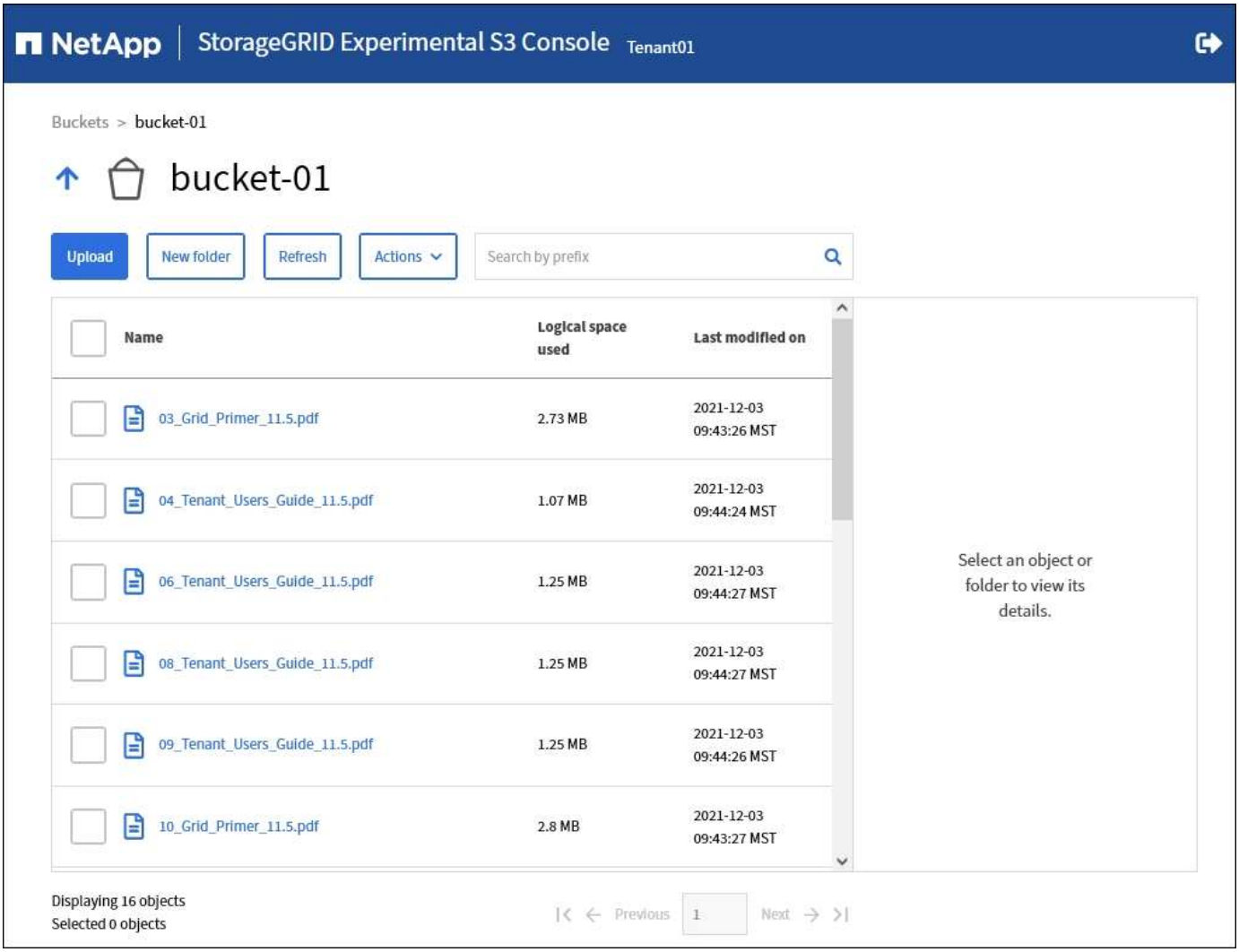
> O console S3 não foi totalmente testado e está marcado como "experimental". Não se destina ao gerenciamento em massa de objetos ou para uso em um ambiente de produção. Os locatários só devem usar o Console S3 ao executar funções para um pequeno número de objetos, como ao carregar objetos para simular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

O que você vai precisar

- Você está conetado ao Gerenciador do Locatário usando um navegador da web suportado.
- Você tem a permissão Gerenciar suas próprias credenciais S3.
- Você criou um bucket.
- Você sabe o ID da chave de acesso do usuário e a chave de acesso secreta. Opcionalmente, você tem um `.csv` arquivo contendo essas informações. Consulte instruções para criar chaves de acesso.

Passos

1. Selecione **baldes**.
2. Experimental S3 Console Selecione . Você também pode acessar este link a partir da página de detalhes do bucket.
3. Na página experimental de login do Console S3, cole o ID da chave de acesso e a chave de acesso secreta nos campos. Caso contrário, selecione **carregar chaves de acesso** e selecione o seu `.csv` ficheiro.
4. Selecione **entrar**.
5. Gerencie objetos conforme necessário.



Gerenciar os serviços da plataforma S3

O que são serviços de plataforma?

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

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

- **Replicação do CloudMirror**: O Serviço de replicação do StorageGRID CloudMirror é usado para espelhar objetos específicos de um bucket do StorageGRID para um destino externo especificado.

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

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

- **Notificações**: Notificações de eventos por bucket São usadas para enviar notificações sobre ações específicas executadas em objetos para um Amazon Simple Notification Service (SNS) externo especificado.

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

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

- **Serviço de integração de pesquisa**: O serviço de integração de pesquisa é usado para enviar metadados de objetos S3 para um índice Elasticsearch especificado, onde os metadados podem ser pesquisados ou analisados usando o serviço externo.

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

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

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

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

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

Como os serviços de plataforma são configurados

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

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

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

1. Se você quiser que todos os objetos cujas chaves comecem por `/images` ser replicados em um bucket do Amazon S3, adicione uma configuração de replicação ao bucket de origem.
2. Se você também quiser enviar notificações quando esses objetos estiverem armazenados no bucket, adicione uma configuração de notificações.

3. Finalmente, se você quiser indexar os metadados para esses objetos, adicione a configuração de notificação de metadados usada para implementar a integração de pesquisa.

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

Serviço de plataforma	S3 API REST
Replicação do CloudMirror	• OBTER replicação do bucket • COLOQUE a replicação do balde
Notificações	• OBTER notificação Bucket • COLOCAR notificação de balde
Integração de pesquisa	• OBTER configuração de notificação de metadados do bucket • COLOQUE a configuração de notificação de metadados do bucket Essas operações são personalizadas para o StorageGRID.

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

Informações relacionadas

Considerações sobre o uso de serviços de plataforma

Use S3

Serviço de replicação do CloudMirror

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

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

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

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

No StorageGRID, é possível replicar os objetos em um único bucket em vários buckets do destino. Para fazer isso, especifique o destino para cada regra no XML de configuração de replicação. Você não pode replicar um

objeto para mais de um bucket ao mesmo tempo.

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

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

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

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

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

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

Entenda as notificações para buckets

Você pode ativar a notificação de eventos para um bucket do S3 se quiser que o StorageGRID envie notificações sobre eventos especificados para um SNS (Serviço de notificação simples) do Amazon de destino.

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

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

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

Notificações e mensagens suportadas

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

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

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

Compreender o serviço de integração de pesquisa

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

O serviço de integração de pesquisa é um serviço StorageGRID personalizado que envia automaticamente e assincronamente metadados de objetos S3 para um endpoint de destino sempre que um objeto ou seus metadados são atualizados. Depois, você pode usar ferramentas sofisticadas de pesquisa, análise de dados, visualização ou aprendizado de máquina fornecidas pelo serviço de destino para pesquisar, analisar e obter insights a partir dos dados do objeto.

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

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

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

As notificações são geradas e enfileiradas para entrega sempre que:

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

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

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

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

Informações relacionadas

Configuração XML para integração de pesquisa

Metadados de objetos incluídos nas notificações de metadados

JSON gerado pelo serviço de integração de pesquisa

Configurar o serviço de integração de pesquisa

Considerações sobre o uso de serviços de plataforma

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

Para obter informações sobre o S3, Use S3consulte .

Considerações sobre o uso de serviços de plataforma

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

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

Considerações para usar o serviço de replicação do CloudMirror

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

Consideração	Detalhes
Tamanho do objeto	O tamanho máximo para objetos que podem ser replicados para um bucket de destino pelo serviço de replicação do CloudMirror é 5 TIB, o que é o mesmo que o tamanho máximo de objeto *suportado*. **Nota**: O tamanho máximo *recomendado* para uma operação de um único objeto PUT é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multipart.
Controle de versão do bucket e IDs de versão	Se o bucket S3 de origem no StorageGRID tiver o controle de versão ativado, você também deverá habilitar o controle de versão para o bucket de destino. Ao usar o controle de versão, observe que o pedido de versões de objetos no intervalo de destino é o melhor esforço e não é garantido pelo serviço CloudMirror, devido às limitações no protocolo S3. **Nota**: Os IDs de versão para o bucket de origem no StorageGRID não estão relacionados com os IDs de versão para o bucket de destino.
Marcação para versões de objetos	O serviço CloudMirror não replica nenhuma solicitação de marcação PUT Object ou EXCLUI solicitações de marcação de objetos que forneçam um ID de versão, devido a limitações no protocolo S3. Como os IDs de versão para a origem e destino não estão relacionados, não há como garantir que uma atualização de tag para uma ID de versão específica seja replicada. Em contraste, o serviço CloudMirror replica solicitações de marcação DE objetos ou EXCLUI solicitações de marcação de objetos que não especificam um ID de versão. Essas solicitações atualizam as tags para a chave mais recente (ou a versão mais recente se o bucket for versionado). Inests normais com tags (não marcando atualizações) também são replicados.
Carregamentos e valores multiparte `ETag`	Ao espelhar objetos que foram carregados usando um upload multipart, o serviço CloudMirror não preserva as peças. Como resultado, o `ETag` valor para o objeto espelhado será diferente do valor do objeto `ETag` original.
Objetos criptografados com SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente)	O serviço CloudMirror não suporta objetos que são criptografados com SSE-C. se você tentar ingerir um objeto no bucket de origem para replicação do CloudMirror e a solicitação incluir os cabeçalhos de solicitação SSE-C, a operação falhará.
Balde com bloqueio de objetos S3 ativado	Se o bucket S3 de destino para replicação do CloudMirror tiver o bloqueio de objetos S3 ativado, a tentativa de configurar a replicação de bucket (PUT Bucket replicação) falhará com um erro AccessDenied.

Configurar endpoints de serviços de plataforma

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

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

O que é um endpoint de serviços de plataforma?

Ao criar um endpoint de serviços de plataforma, você especifica as informações que o StorageGRID precisa para acessar o destino externo.

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

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

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

Endpoints para replicação do CloudMirror

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

Endpoints para notificações

O StorageGRID oferece suporte a pontos de extremidade do Serviço de notificação simples (SNS). Os endpoints do Simple Queue Service (SQS) ou do AWS Lambda não são suportados.

Endpoints para o serviço de integração de pesquisa

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

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

Informações relacionadas

Administrar o StorageGRID

Especifique URN para endpoint de serviços de plataforma

Ao criar um endpoint de serviços de plataforma, você deve especificar um Nome de recurso exclusivo (URN). Você usará a URN para referenciar o endpoint quando criar

XML de configuração para o serviço da plataforma. A URNA para cada endpoint deve ser única.

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

URNA elementos

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

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

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

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

Serviço	Tipo
Replicação do CloudMirror	s3
Notificações	sns
Integração de pesquisa	es

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

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

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

Urnas para serviços hospedados na AWS e no GCP

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

- Replicação do CloudMirror:

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

- Notificações:

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

- Integração de pesquisa:

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

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

Urnas para serviços hospedados localmente

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

- Replicação do CloudMirror:

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

  Para um endpoint do CloudMirror hospedado no StorageGRID, você pode especificar uma URNA válida que começa com `urn:sgws`:

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

- Notificações:

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

- Integração de pesquisa:

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

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

Criar endpoint de serviços de plataforma

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

O que você vai precisar

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

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

  - Nome de recurso único (URN)

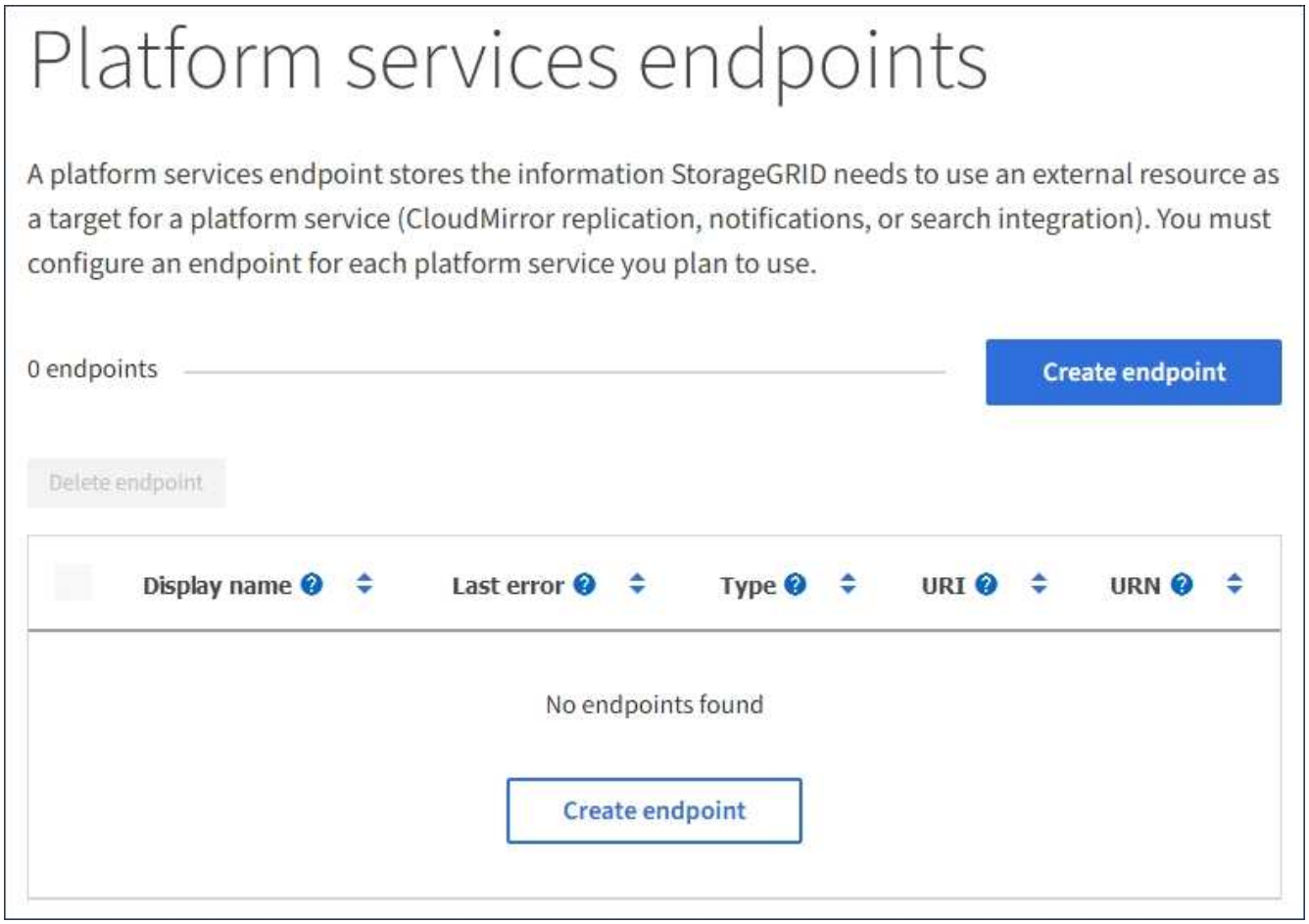
    Especifique URN para endpoint de serviços de plataforma

  - Credenciais de autenticação (se necessário):
    - Chave de acesso: ID da chave de acesso e chave de acesso secreta
    - HTTP básico: Nome de usuário e senha
    - CAP (Portal de Acesso C2S): URL de credenciais temporárias, certificados de servidor e cliente, chaves de cliente e uma senha de chave privada do cliente opcional.
  - Certificado de segurança (se estiver usando um certificado de CA personalizado)

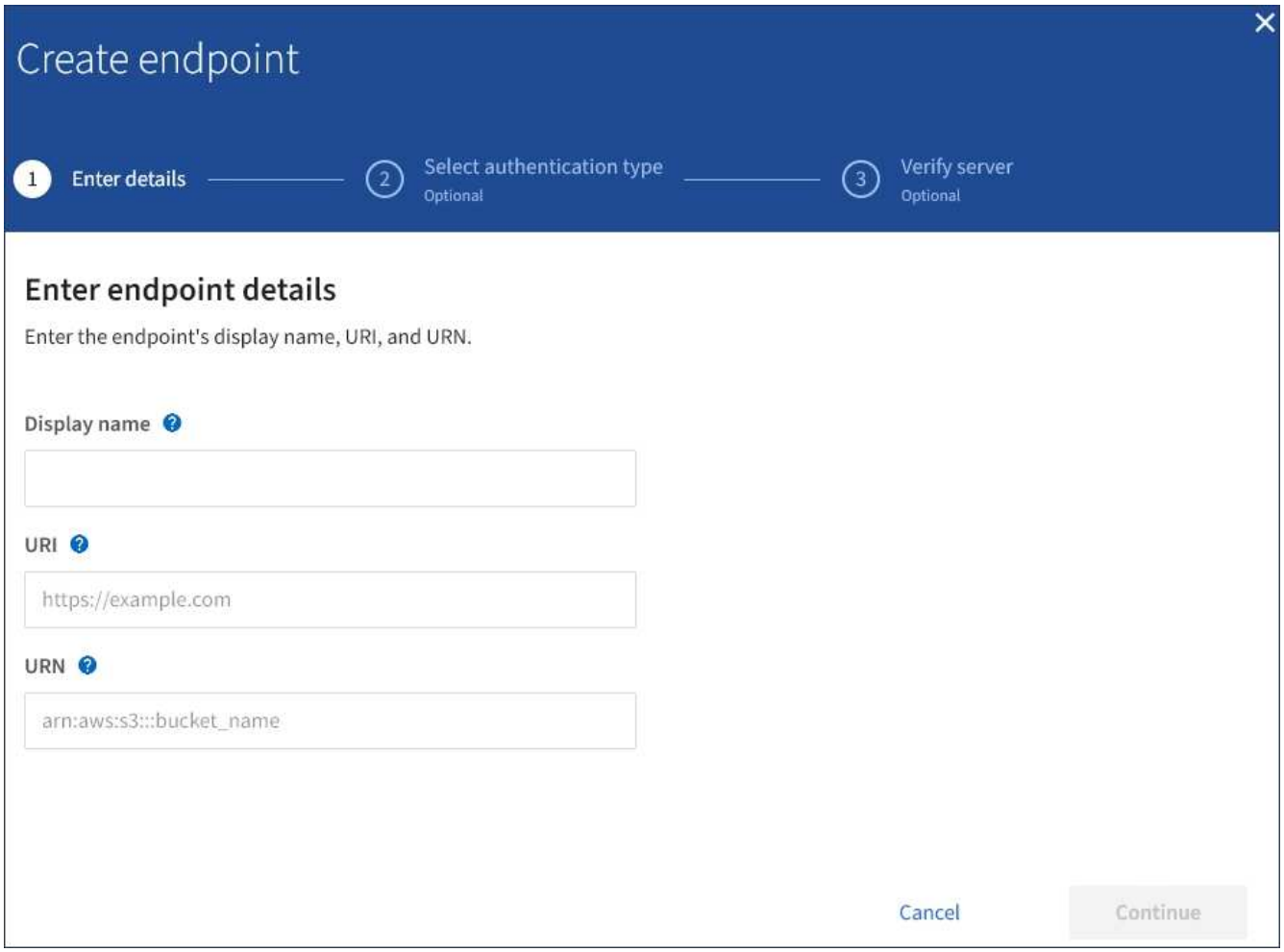
Passos

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

   A página de endpoints dos serviços da plataforma é exibida.



2. Selecione **criar endpoint**.



3. Introduza um nome de apresentação para descrever brevemente o ponto final e a respetiva finalidade.

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

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

   Use um dos seguintes formatos:

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

   Se você não especificar uma porta, a porta 443 será usada para URIs HTTPS e a porta 80 será usada para URIs HTTP.

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

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

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

balanceador de carga.

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

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

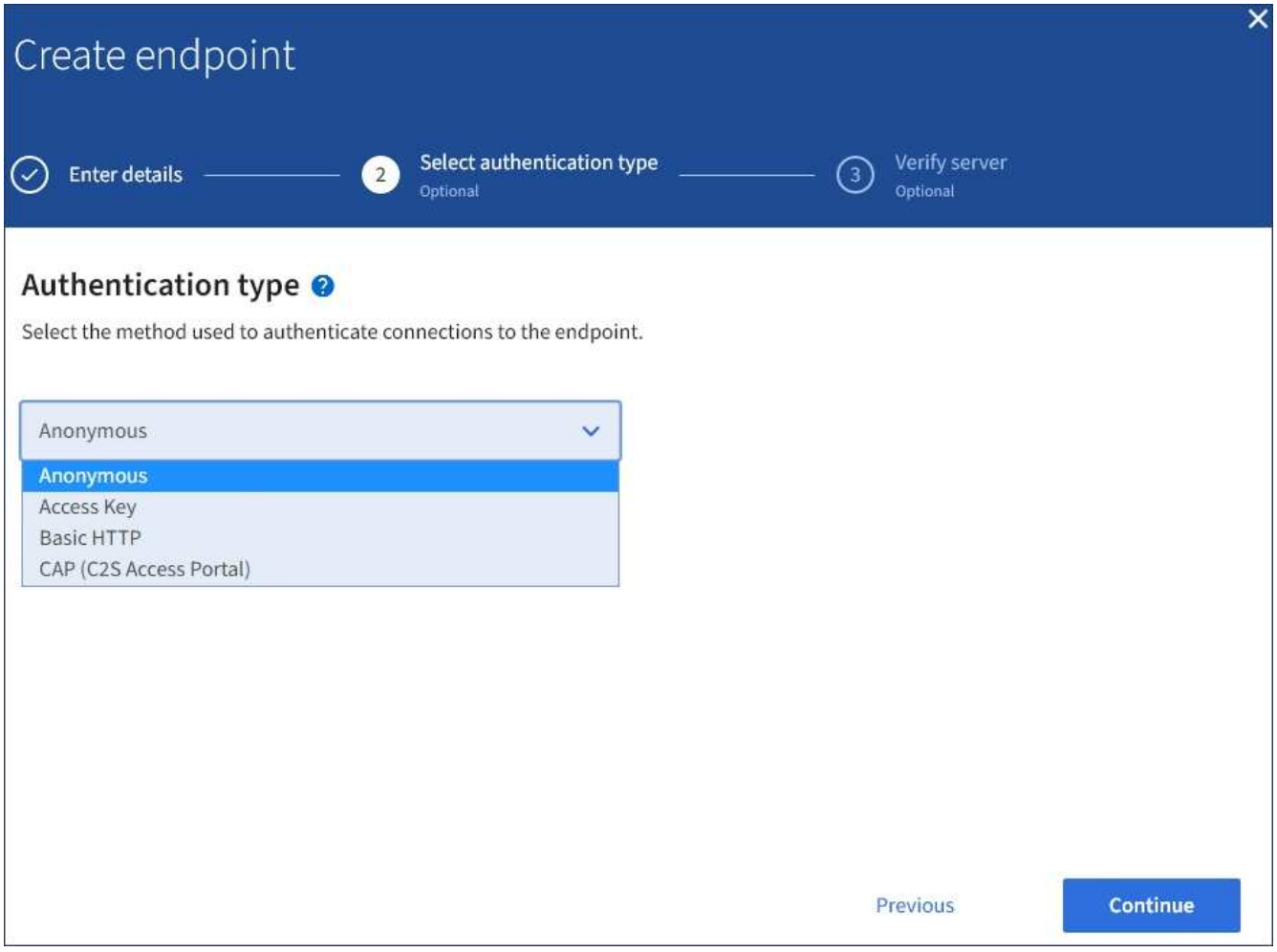
```
https://s3-aws-region.amazonaws.com
```

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

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

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

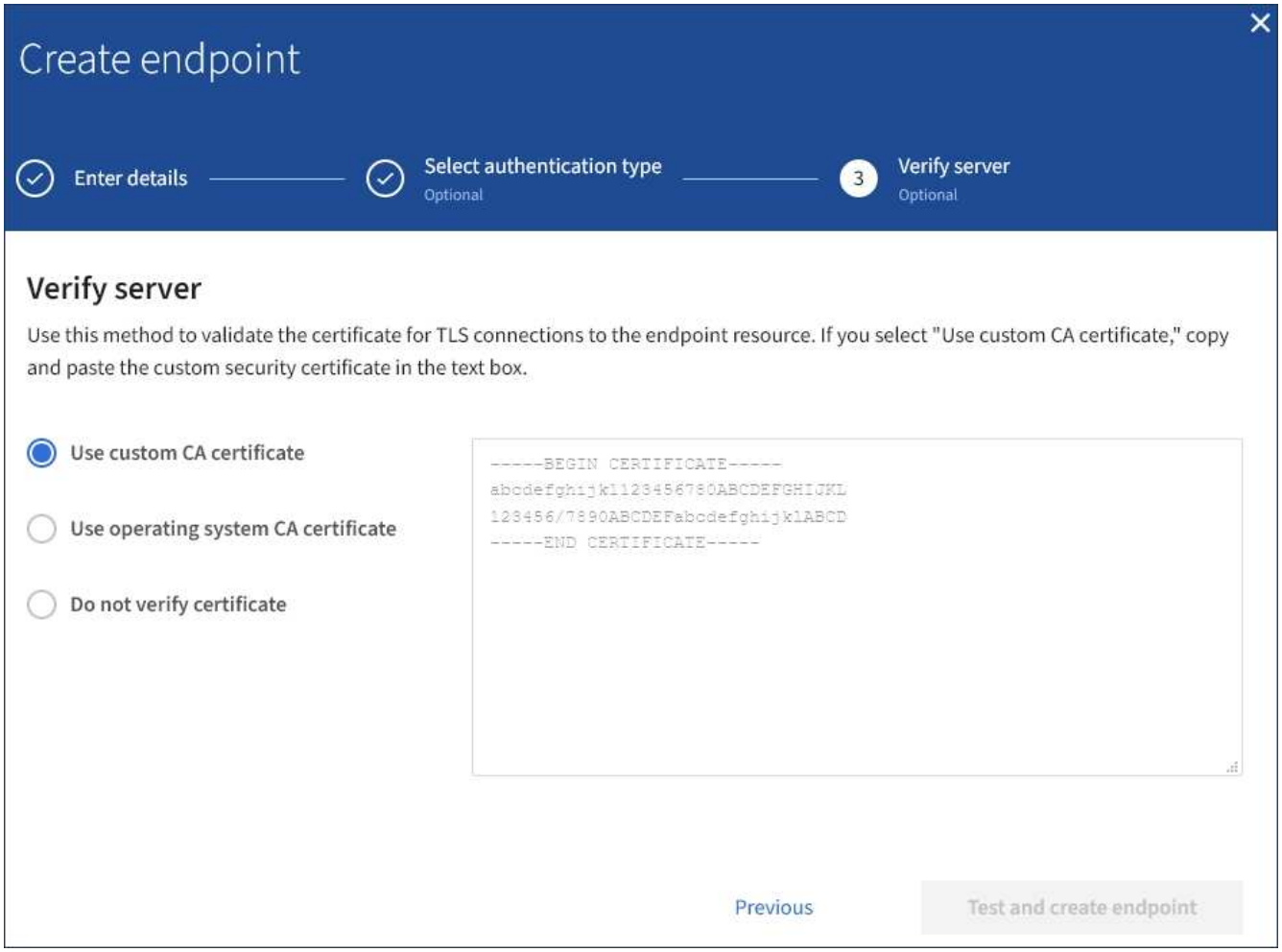
6. Selecione **continuar**.
7. Selecione um valor para **tipo de autenticação** e insira ou carregue as credenciais necessárias.



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

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints que têm a segurança desativada.	Sem autenticação.
Chave de acesso	Usa credenciais de estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreto
HTTP básico	Usa um nome de usuário e senha para autenticar conexões com o destino.	• Nome de utilizador • Palavra-passe
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 de cliente (upload de arquivo PEM) • Chave privada do cliente (upload de arquivo PEM, formato criptografado OpenSSL ou formato de chave privada não criptografado) • Senha de chave privada do cliente (opcional)

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



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

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

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

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

Informações relacionadas

Especifique URN para endpoint de serviços de plataforma

Configurar a replicação do CloudMirror

Configurar notificações de eventos

Configurar o serviço de integração de pesquisa

Teste a conexão para endpoint de serviços de plataforma

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

O que você vai precisar

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

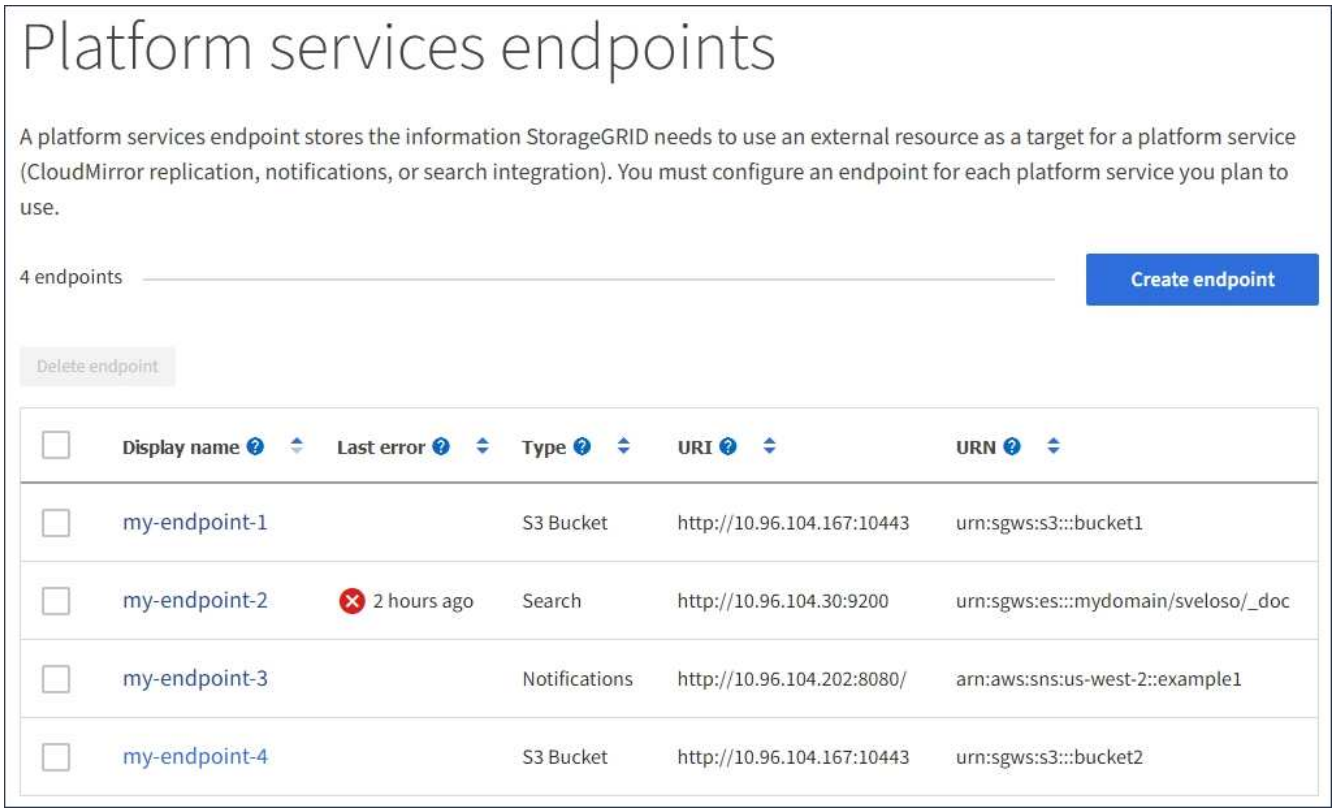
Sobre esta tarefa

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

Passos

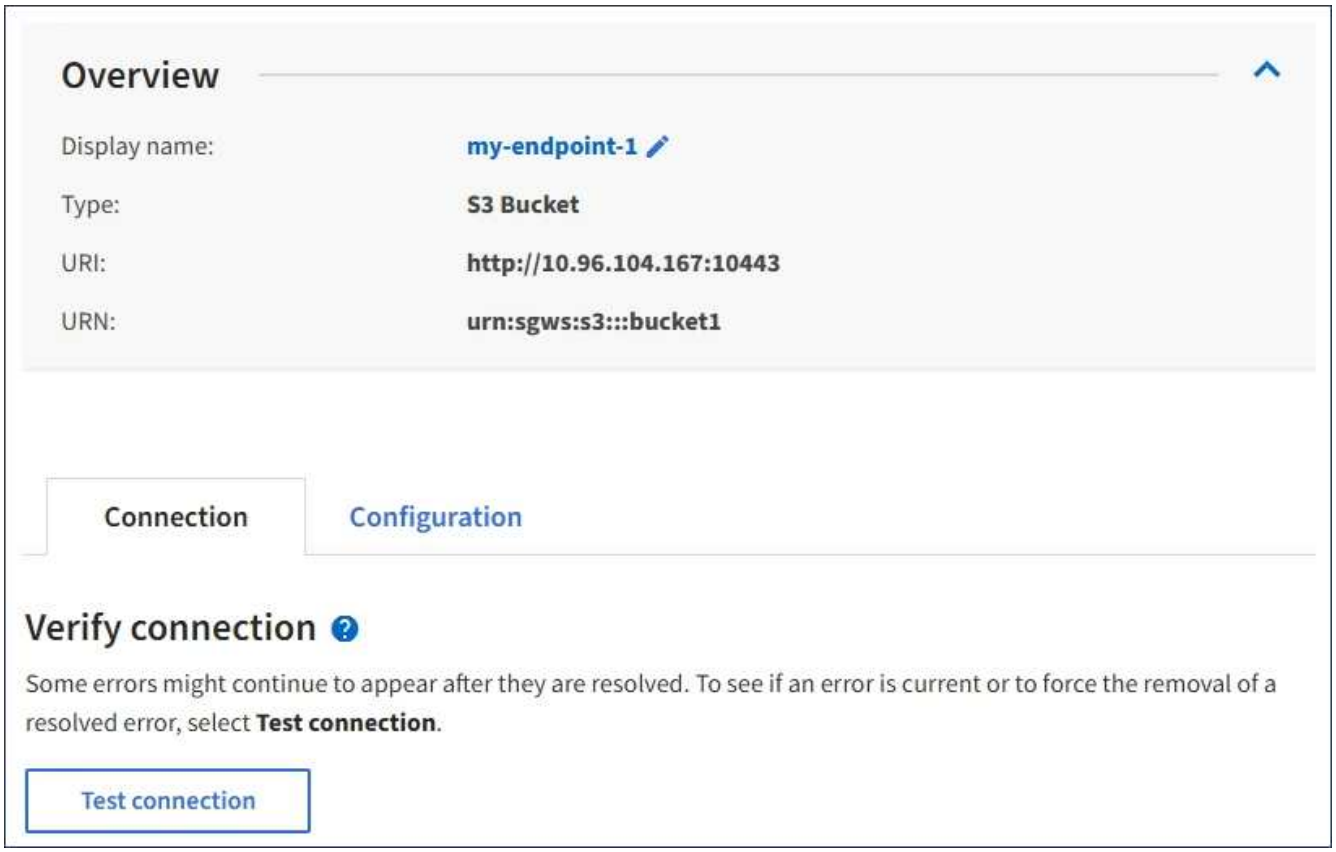
1. Selecione **STORAGE (S3) endpoints de serviços de plataforma**.

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



2. Selecione o ponto final cuja ligação pretende testar.

   A página de detalhes do ponto final é exibida.



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

Editar endpoint de serviços de plataforma

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

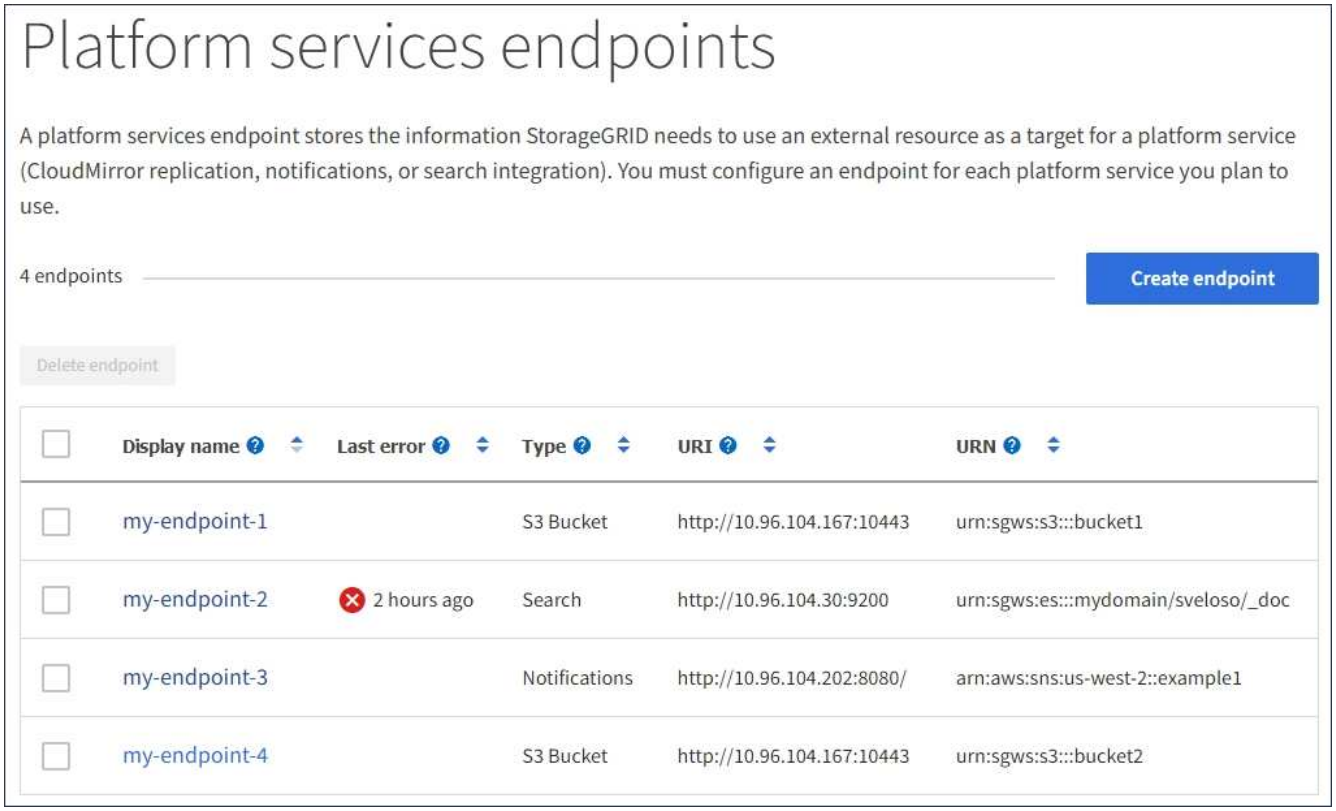
O que você vai precisar

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

Passos

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

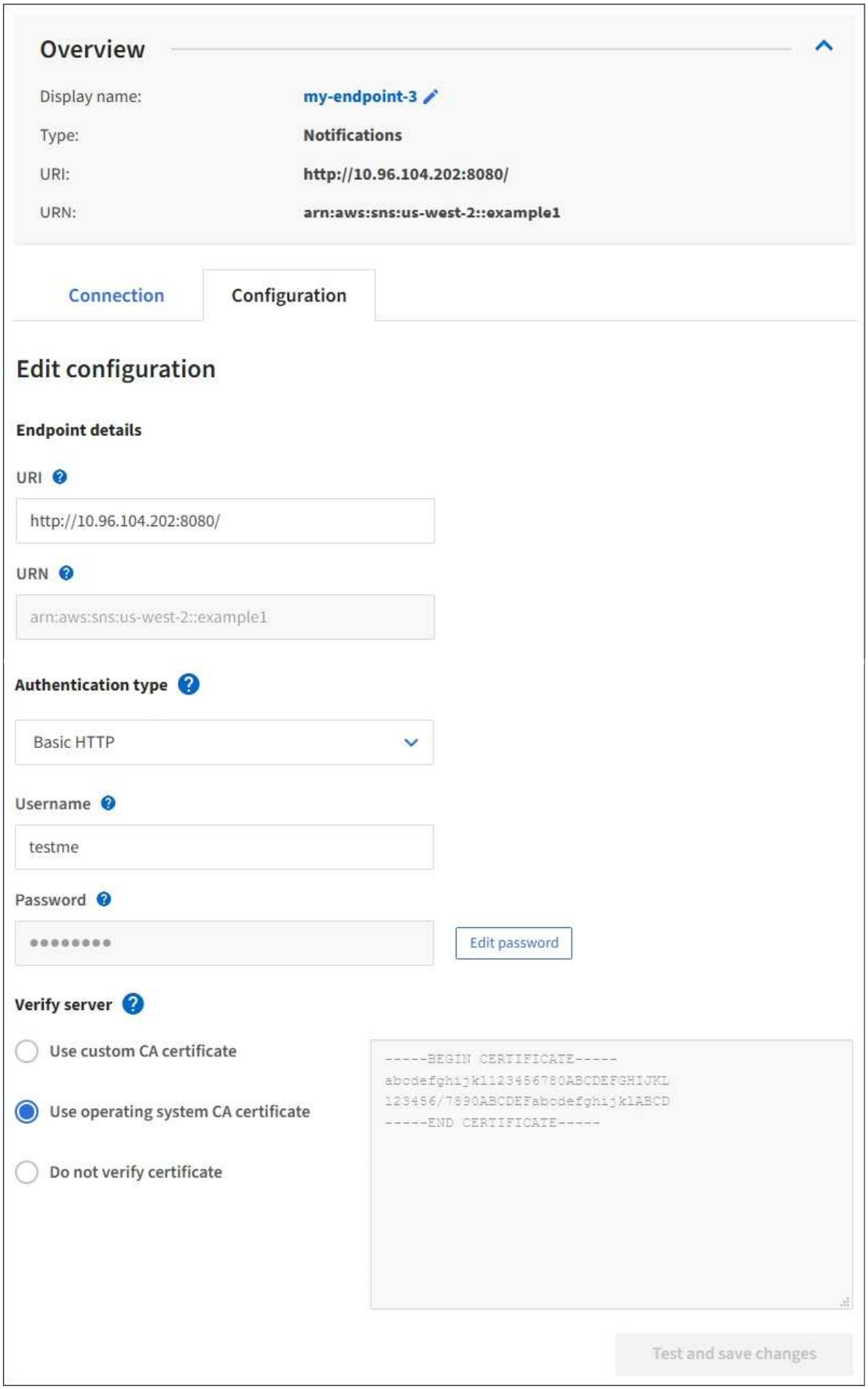
A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.



2. Selecione o ponto de extremidade que pretende editar.

   A página de detalhes do ponto final é exibida.

3. Selecione **Configuração**.


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

4. Conforme necessário, altere a configuração do endpoint.

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

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

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

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

Excluir endpoint de serviços de plataforma

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

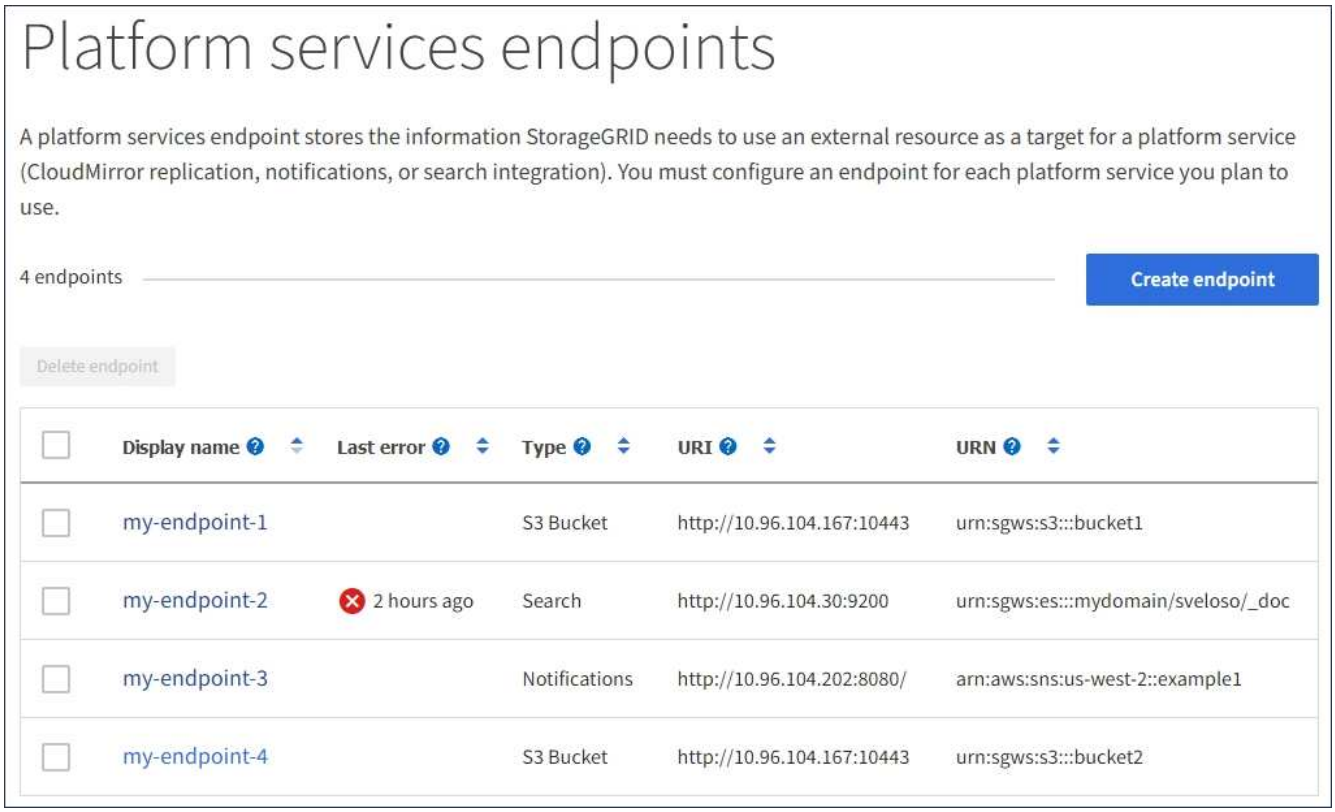
O que você vai precisar

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

Passos

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

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

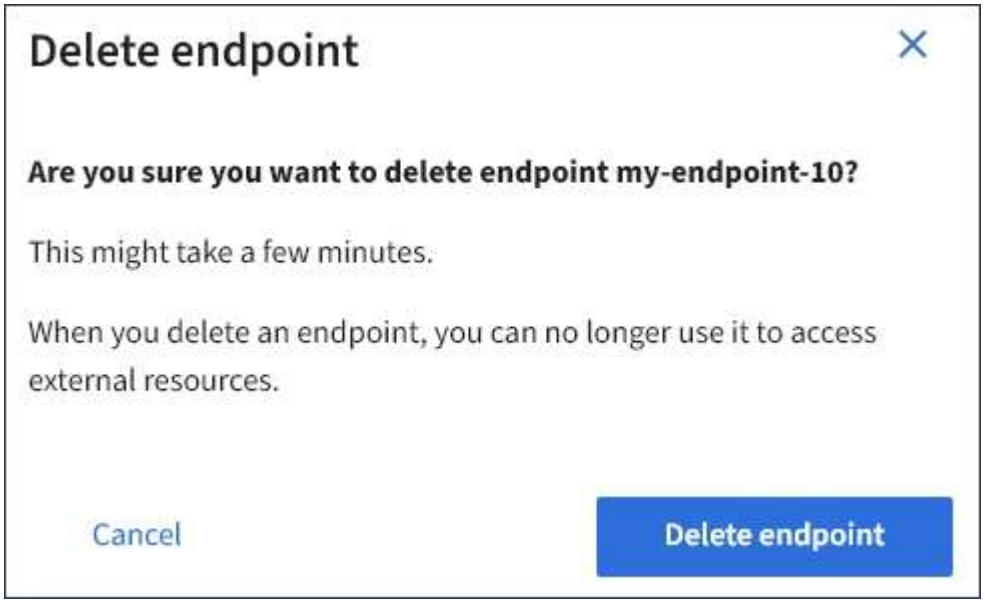


2. Marque a caixa de seleção para cada ponto de extremidade que deseja excluir.

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

3. Selecione **ações Excluir endpoint**.

   É apresentada uma mensagem de confirmação.



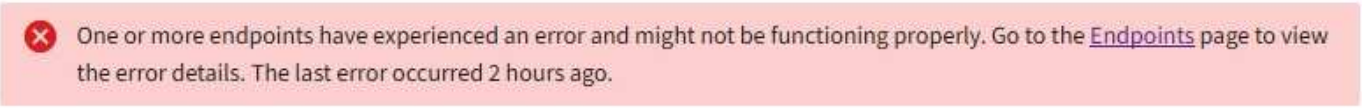
4. Selecione **Excluir endpoint**.

Solucionar erros de endpoint dos serviços da plataforma

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

Determine se ocorreu um erro

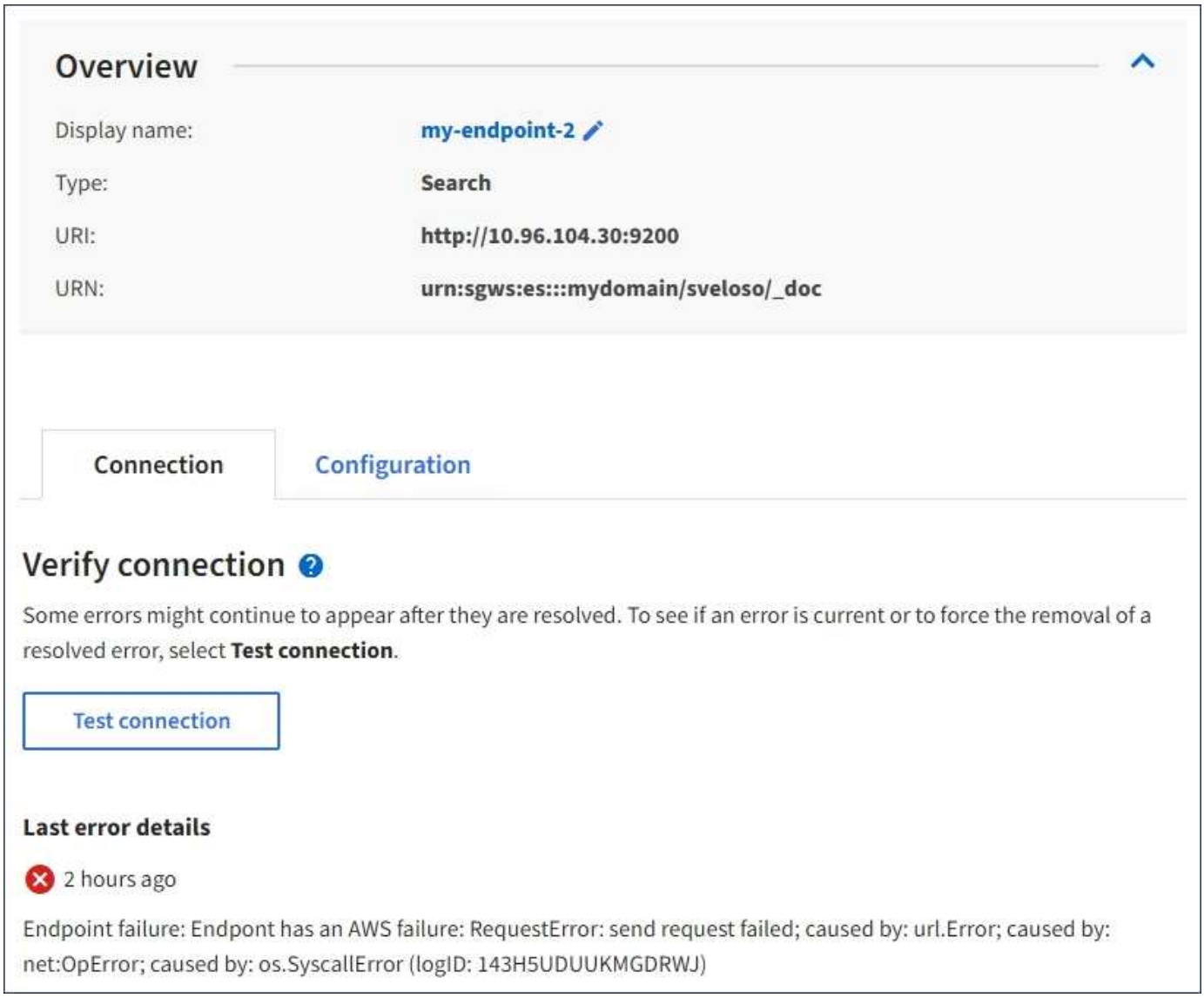
Se algum erro de endpoint de serviços de plataforma tiver ocorrido nos últimos 7 dias, o Painel do Gerenciador do Locatário exibirá uma mensagem de alerta. Você pode acessar a página de endpoints dos serviços da plataforma para ver mais detalhes sobre o erro.



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

Passos

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



Verifique se o erro ainda está atual

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

Passos

1. Selecione o ponto final.

   A página de detalhes do ponto final é exibida.

2. Selecione **Connection Test Connection**.

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

Resolver erros de endpoint

Você pode usar a mensagem **último erro** na página de detalhes do endpoint para ajudar a determinar o que está causando o erro. Alguns erros podem exigir que você edite o endpoint para resolver o problema. Por

exemplo, um erro de espelhamento de nuvem pode ocorrer se o StorageGRID não conseguir acessar o bucket do destino S3 porque ele não tem as permissões de acesso corretas ou a chave de acesso expirou. A mensagem é "as credenciais do endpoint ou o acesso ao destino precisa ser atualizado", e os detalhes são "AccessDenied" ou "InvalidAccessKeyId".

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

Passos

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

Credenciais de endpoint com permissões insuficientes

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

Solução de problemas de serviços de plataforma adicionais

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

Administrar o StorageGRID

Informações relacionadas

Criar endpoint de serviços de plataforma

Teste a conexão para endpoint de serviços de plataforma

Editar endpoint de serviços de plataforma

Configurar a replicação do CloudMirror

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

O que você vai precisar

- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você já deve ter criado um bucket para agir como a origem da replicação.
- O endpoint que você pretende usar como destino para a replicação do CloudMirror já deve existir, e você deve ter sua URN.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root, que permite gerenciar as configurações de todos os buckets do S3 em sua conta de locatário.

Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador do locatário.

Sobre esta tarefa

A replicação do CloudMirror copia objetos de um bucket de origem para um bucket de destino especificado em um endpoint. Para ativar a replicação do CloudMirror para um bucket, você deve criar e aplicar XML de configuração de replicação de bucket válida. O XML de configuração de replicação deve usar a URN de um endpoint de bucket do S3 para cada destino.

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

Para obter informações gerais sobre replicação de bucket e como configurá-la, consulte a documentação do Amazon Simple Storage Service (S3) sobre replicação entre regiões (CRR). Para obter informações sobre como o StorageGRID implementa a API de configuração de replicação de bucket do S3, consulte o Instruções para a implementação de aplicativos cliente S3.

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

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

Passos

1. Habilite a replicação para o bucket de origem:

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

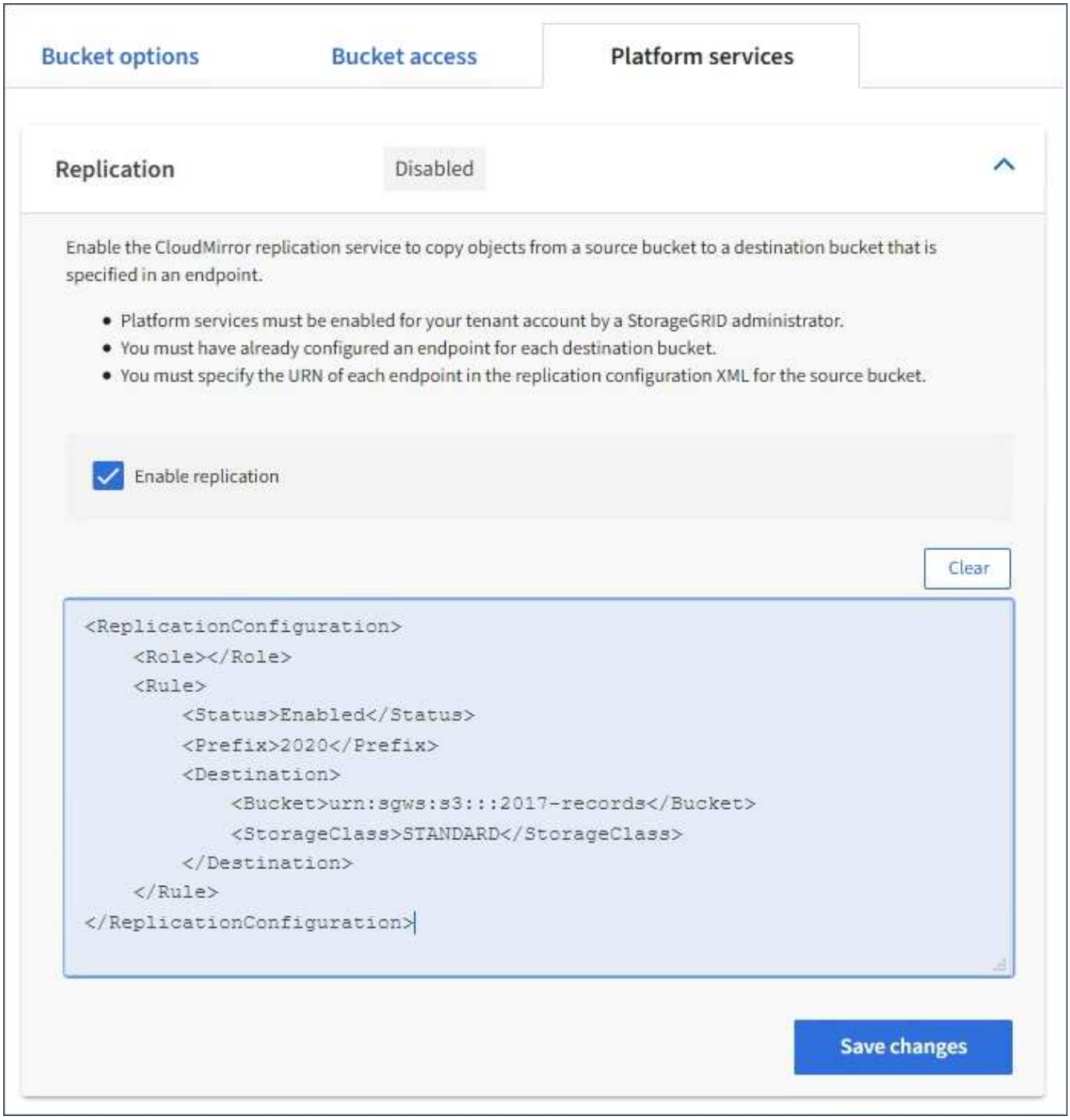
   - Observe que o StorageGRID só suporta V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue convenções V1 para exclusão de versões de objetos. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes.
   - Use a URNA de um endpoint de bucket S3 como o destino.
   - Opcionalmente, adicione o `<StorageClass>` elemento e especifique uma das seguintes opções:
     - `STANDARD`: A classe de armazenamento padrão. Se você não especificar uma classe de armazenamento ao carregar um objeto, a `STANDARD` classe de armazenamento será usada.
     - `STANDARD_IA`: (Standard - Acesso não frequente.) Use essa classe de storage para dados acessados com menos frequência, mas que ainda exigem acesso rápido quando necessário.
     - `REDUCED_REDUNDANCY`: Use esta classe de armazenamento para dados não críticos e reprodutíveis que podem ser armazenados com menos redundância do que a `STANDARD` classe de armazenamento.
   - Se você especificar um `Role` no XML de configuração, ele será ignorado. Este valor não é utilizado pelo StorageGRID.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

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

   É apresentada a página de detalhes do balde.

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



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

7. Verifique se a replicação está configurada corretamente:
   a. Adicione um objeto ao bucket de origem que atenda aos requisitos de replicação, conforme especificado na configuração de replicação.

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

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

Para objetos pequenos, a replicação acontece rapidamente.

Informações relacionadas

Use S3

Criar endpoint de serviços de plataforma

Configurar notificações de eventos

O serviço de notificações é um dos três serviços da plataforma StorageGRID. Você pode habilitar notificações de um bucket para enviar informações sobre eventos especificados para um serviço de destino compatível com o AWS Simple Notification Service (SNS).

O que você vai precisar

- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você já deve ter criado um bucket para agir como a fonte das notificações.
- O endpoint que você pretende usar como destino para notificações de eventos já deve existir, e você deve ter sua URNA.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root, que permite gerenciar as configurações de todos os buckets do S3 em sua conta de locatário. Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador do locatário.

Sobre esta tarefa

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

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

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

Passos

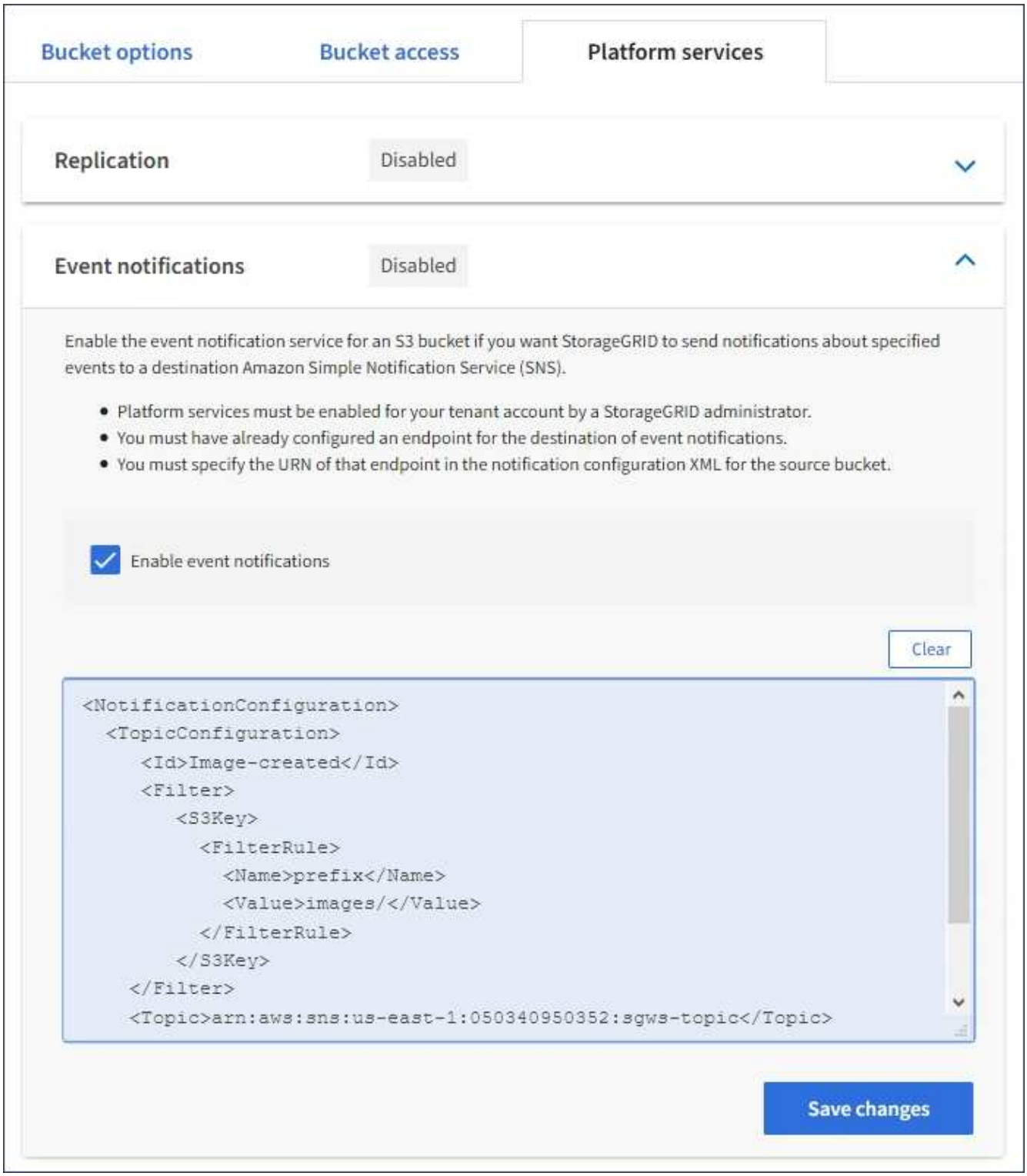
1. Ativar notificações para o intervalo de origem:
    - Use um editor de texto para criar a configuração de notificação XML necessário para habilitar notificações de eventos, conforme especificado na API de notificação S3.
    - Ao configurar o XML, use a URNA de um endpoint de notificações de eventos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

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

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

   É apresentada a página de detalhes do balde.

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



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

7. Verifique se as notificações de eventos estão configuradas corretamente:

   a. Execute uma ação em um objeto no bucket de origem que atenda aos requisitos para acionar uma notificação conforme configurado no XML de configuração.

No exemplo, uma notificação de evento é enviada sempre que um objeto é criado com o `images/` prefixo.

b. Confirme se uma notificação foi entregue ao tópico SNS de destino.

Por exemplo, se o tópico de destino estiver hospedado no AWS Simple Notification Service (SNS), você poderá configurar o serviço para enviar um e-mail quando a notificação for entregue.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

Se a notificação for recebida no tópico de destino, você configurou com êxito o bucket de origem para

notificações do StorageGRID.

Informações relacionadas

Entenda as notificações para buckets

Use S3

Criar endpoint de serviços de plataforma

Use o serviço de integração de pesquisa

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

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

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

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

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

Informações relacionadas

Configuração XML para integração de pesquisa

Metadados de objetos incluídos nas notificações de metadados

JSON gerado pelo serviço de integração de pesquisa

Configurar o serviço de integração de pesquisa

Use S3

Configuração XML para integração de pesquisa

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

Os objetos podem ser filtrados no prefixo do nome do objeto. Por exemplo, você pode enviar metadados para

objetos com o prefixo `images` para um destino e metadados para objetos com o prefixo `videos` para outro. As configurações que têm prefixos sobrepostos não são válidas e são rejeitadas quando são enviadas. Por exemplo, uma configuração que inclua uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não é permitida.

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

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

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

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

Nome	Descrição	Obrigatório
Estado	O estado pode ser "ativado" ou "Desativado". Nenhuma ação é tomada para regras que são desativadas. Incluído no elemento regra.	Sim
Prefixo	Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento regra.	Sim
Destino	Etiqueta de contentor para o destino de uma regra. Incluído no elemento regra.	Sim
Urna	URNA do destino onde os metadados do objeto são enviados. Deve ser a URNA de um endpoint StorageGRID com as seguintes propriedades: • `es` deve ser o terceiro elemento. • A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário `domain-name/myindex/mytype`. Os endpoints são configurados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário. Eles assumem a seguinte forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O endpoint deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. URNA está incluído no elemento destino.	Sim

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

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

Neste exemplo, metadados de objetos para todos os objetos são enviados para o mesmo destino.

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

Configuração de notificação de metadados com duas regras

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

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informações relacionadas

Use S3

Metadados de objetos incluídos nas notificações de metadados

JSON gerado pelo serviço de integração de pesquisa

Configurar o serviço de integração de pesquisa

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

O que você vai precisar

- Os serviços de plataforma devem estar habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você já deve ter criado um bucket do S3 cujo conteúdo você deseja indexar.
- O endpoint que você pretende usar como destino para o serviço de integração de pesquisa já deve existir, e você deve ter sua URNA.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root, que permite gerenciar as configurações de todos os buckets do S3 em sua conta de locatário. Essas permissões substituem as configurações de permissão nas políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador do locatário.

Sobre esta tarefa

Depois de configurar o serviço de integração de pesquisa para um bucket de origem, criar um objeto ou atualizar metadados ou tags de um objeto aciona metadados de objeto para serem enviados para o endpoint de destino. Se você ativar o serviço de integração de pesquisa para um bucket que já contém objetos, as notificações de metadados não serão enviadas automaticamente para objetos existentes. Você deve atualizar esses objetos existentes para garantir que seus metadados sejam adicionados ao índice de pesquisa de destino.

Passos

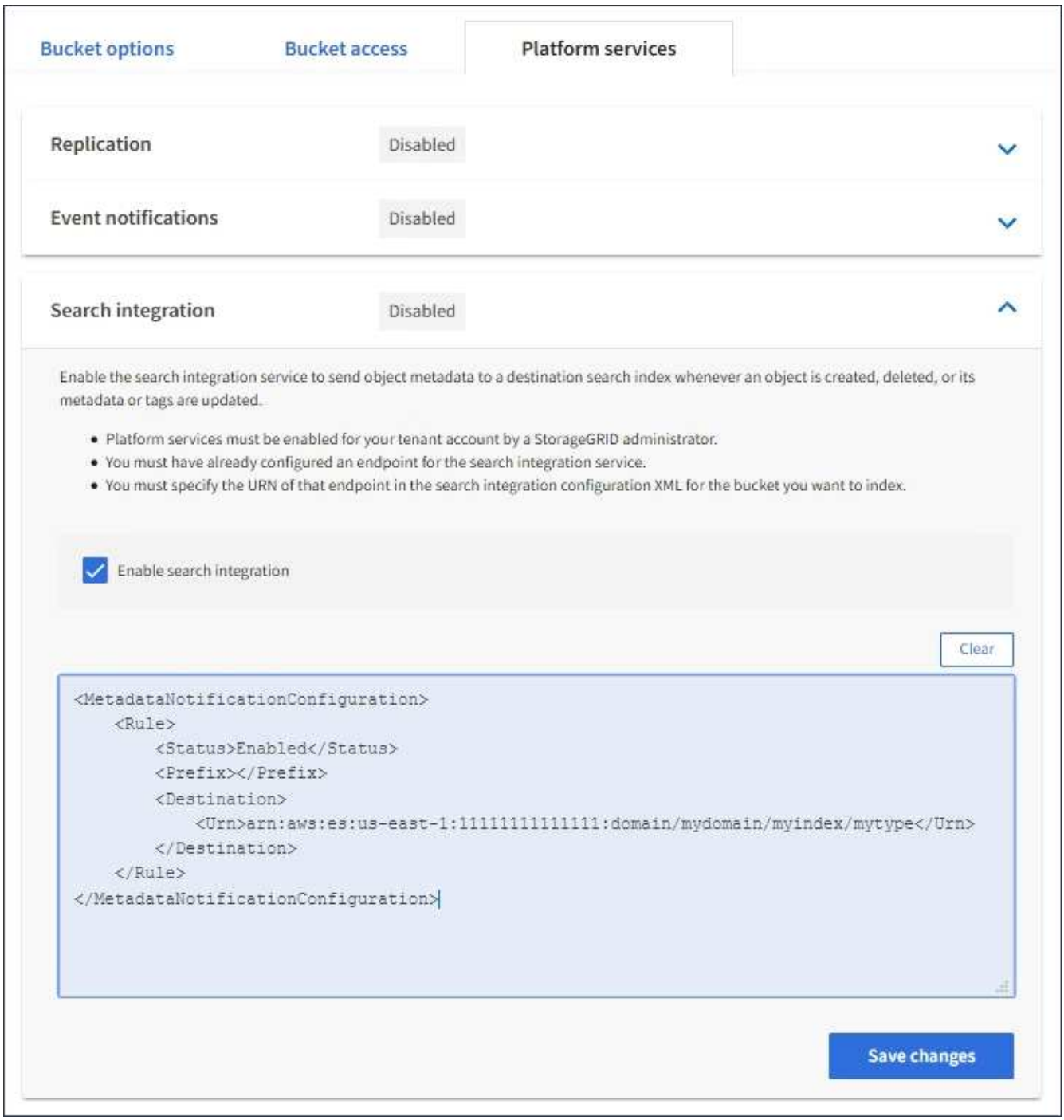
1. Use um editor de texto para criar o XML de notificação de metadados necessário para habilitar a integração de pesquisa.
   - Consulte as informações sobre o XML de configuração para integração de pesquisa.
   - Ao configurar o XML, use a URNA de um endpoint de integração de pesquisa como o destino.

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

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

   É apresentada a página de detalhes do balde.

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



Os serviços de plataforma devem estar habilitados para cada conta de locatário por um administrador do StorageGRID usando o Gerenciador de Grade ou a API de gerenciamento. Contacte o administrador do StorageGRID se ocorrer um erro ao guardar o XML de configuração.

7. Verifique se o serviço de integração de pesquisa está configurado corretamente:
   a. Adicione um objeto ao bucket de origem que atenda aos requisitos para acionar uma notificação de

metadados conforme especificado no XML de configuração.

No exemplo mostrado anteriormente, todos os objetos adicionados ao bucket acionam uma notificação de metadados.

b. Confirme se um documento JSON que contém metadados e tags do objeto foi adicionado ao índice de pesquisa especificado no endpoint.

Depois de terminar

Conforme necessário, você pode desativar a integração de pesquisa para um bucket usando um dos seguintes métodos:

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

Informações relacionadas

Compreender o serviço de integração de pesquisa

Configuração XML para integração de pesquisa

Use S3

Criar endpoint de serviços de plataforma

JSON gerado pelo serviço de integração de pesquisa

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

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

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

Metadados de objetos incluídos nas notificações de metadados

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

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

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

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

Use S3

Use S3: Visão geral

O StorageGRID oferece suporte à API Simple Storage Service (S3), que é implementada como um conjunto de serviços da Web de transferência de Estado representacional (REST). O suporte à API REST do S3 permite conectar aplicações orientadas a serviços desenvolvidas para serviços da Web do S3 ao storage de objetos no local que usa o sistema StorageGRID. Isso requer alterações mínimas no uso atual de chamadas de API REST do aplicativo cliente S3.

Alterações ao suporte à API REST do S3

Você deve estar ciente das alterações no suporte do sistema StorageGRID para a API REST do S3.

Solte	Comentários
11,6	• Adicionado suporte para o uso do `partNumber` parâmetro Request 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 bloqueio de objetos S3. • Adicionado suporte para a `s3:object-lock-remaining-retention-days` chave de condição de política para definir o intervalo de períodos de retenção permitidos para seus objetos. • O tamanho máximo *recommended* para uma única operação PUT Object é agora 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multipart. No StorageGRID 11,6, o tamanho máximo *suportado* para uma operação DE objeto PUT único permanece 5 TIB (5.497.558.138.880 bytes). No entanto, o alerta **S3 PUT Object Size too large** será acionado se você tentar fazer o upload de um objeto que exceda 5 GiB.

Solte	Comentários
11,5	• Adicionado suporte para gerenciar a criptografia de bucket. • Adicionado suporte para S3 Object Lock e solicitações de conformidade legadas obsoletas. • Adicionado suporte para o uso DE EXCLUIR vários objetos em buckets versionados. • O `Content-MD5` cabeçalho de solicitação agora é suportado corretamente.
11,4	• Adicionado suporte para EXCLUIR marcação de balde, OBTER marcação de balde e COLOCAR marcação de balde. As etiquetas 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 intervalo no `s3:ObjectRestore:Post` tipo de evento. • Os limites de tamanho da AWS para peças de várias partes agora são aplicados. Cada parte em um upload de várias partes deve estar entre 5 MIB e 5 GiB. A última parte pode ser menor do que 5 MIB. • Adicionado suporte para TLS 1,3 e lista atualizada de pacotes de criptografia TLS suportados. • O serviço CLB está obsoleto.
11,3	• Adicionado suporte para criptografia no lado do servidor de dados de objeto com chaves fornecidas pelo cliente (SSE-C). • Adicionado suporte para as operações DE ELIMINAÇÃO, OBTENÇÃO e COLOCAÇÃO do ciclo de vida do balde (apenas ação de expiração) e para o `x-amz-expiration` cabeçalho de resposta. • PUT Object, put Object - Copy e Multipart Upload atualizados para descrever o impactos das regras ILM que usam o posicionamento síncrono na ingestão. • Lista atualizada dos conjuntos de encriptação TLS suportados. As cifras TLS 1,1 não são mais suportadas.
11,2	Adicionado suporte para restauração PÓS-objeto para uso com Cloud Storage Pools. Adicionado suporte para o uso da sintaxe da AWS para ARN, chaves de condição de política e variáveis de política em políticas de grupo e bucket. As políticas de grupo e bucket existentes que usam a sintaxe StorageGRID continuarão a ser suportadas. **Observação:** os usos de ARN/URN em outra configuração JSON/XML, incluindo aqueles usados em recursos personalizados do StorageGRID, não foram alterados.
11,1	Adicionado suporte para compartilhamento de recursos entre origens (CORS), HTTP para conexões de clientes S3 para nós de grade e configurações de conformidade em buckets.

Solte	Comentários
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 a configuração de controle de consistência disponível.
10,4	Adicionado suporte para alterações de verificação de ILM para controle de versão, atualizações de página de nomes de domínio de endpoints, 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 de várias partes (Upload de peça - cópia).
10,1	Adicionado suporte para upload em várias partes, solicitações virtuais de estilo hospedado e autenticação v4.1X.
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.

Versões suportadas

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

Item	Versão
Especificação S3	*Referência da API de serviço de armazenamento simples* 2006-03-01
HTTP	1,1 Para obter mais informações sobre HTTP, consulte HTTP/1,1 (RFCs 7230-35). **Nota**: O StorageGRID não suporta a canalização HTTP/1,1.

Informações relacionadas

"IETF RFC 2616: Protocolo de transferência de hipertexto (HTTP/1,1)"

"Documentação do Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service"

Suporte para serviços de plataforma StorageGRID

Os serviços da plataforma StorageGRID permitem que as contas de locatários do StorageGRID aproveitem serviços externos, como um bucket remoto do S3, um endpoint do Serviço de notificação simples (SNS) ou um cluster do Elasticsearch para estender os

serviços fornecidos por uma grade.

A tabela a seguir resume os serviços de plataforma disponíveis e as APIs do S3 usadas para configurá-los.

Serviço de plataforma	Finalidade	S3 API usada para configurar o serviço
Replicação do CloudMirror	Replica objetos de um bucket do StorageGRID de origem para o bucket do S3 remoto configurado.	COLOQUE a replicação do balde
Notificações	Envia notificações sobre eventos em um bucket do StorageGRID de origem para um endpoint configurado do Serviço de notificação simples (SNS).	COLOCAR notificação de balde
Integração de pesquisa	Envia metadados de objetos para objetos armazenados em um bucket do StorageGRID para um índice Elasticsearch configurado.	NOTIFICAÇÃO DE metadados do Bucket **Observação:** esta é uma API S3D personalizada do StorageGRID.

Um administrador de grade deve habilitar o uso de serviços de plataforma para uma conta de locatário antes que eles possam ser usados. Em seguida, um administrador de locatário deve criar um endpoint que represente o serviço remoto na conta de locatário. Esta etapa é necessária antes que um serviço possa ser configurado.

Recomendações para o uso de serviços de plataforma

Antes de usar os serviços de plataforma, você deve estar ciente das seguintes recomendações:

- A NetApp recomenda que você não permita mais de 100 locatários ativos com solicitações do S3 que exigem replicação, notificações e integração de pesquisa do CloudMirror. Ter mais de 100 inquilinos ativos ativos pode resultar em desempenho mais lento do cliente S3.
- Se um bucket do S3 no sistema do StorageGRID tiver o controle de versão e a replicação do CloudMirror habilitado, a NetApp recomenda que o endpoint de destino também tenha o controle de versão do bucket do S3 habilitado. Isso permite que a replicação do CloudMirror gere versões de objetos semelhantes no endpoint.
- A replicação do CloudMirror não é suportada se o bucket de origem tiver o S3 Object Lock ativado.
- A replicação do CloudMirror falhará com um erro AccessDenied se o intervalo de destino tiver conformidade legada habilitada.

Informações relacionadas

Use a conta de locatário

Administrar o StorageGRID

Operações em baldes

COLOCAR solicitação de configuração de notificação de metadados do bucket

Configurar contas de inquilino e conexões

Configurar o StorageGRID para aceitar conexões de aplicativos cliente requer a criação de uma ou mais contas de locatário e a configuração das conexões.

Criar e configurar contas de locatário do S3

Uma conta de locatário S3 é necessária antes que os clientes API S3D possam armazenar e recuperar objetos no StorageGRID. Cada conta de locatário tem seu próprio ID de conta, grupos e usuários, além de contentores e objetos.

As contas de locatário do S3 são criadas por um administrador de grade do StorageGRID usando o Gerenciador de grade ou a API de gerenciamento de grade. Ao criar uma conta de locatário do S3, o administrador da grade especifica as seguintes informações:

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

Depois que uma conta de locatário do S3 for criada, os usuários do locatário poderão acessar o Gerenciador do locatário para executar tarefas como as seguintes:

- Configure a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e crie grupos e usuários locais
- Gerenciar S3 chaves de acesso
- Crie e gerencie buckets do S3, incluindo buckets que têm o bloqueio de objetos do S3 ativado
- Usar serviços de plataforma (se ativado)
- Monitorar o uso do storage

> Os usuários de locatários do S3 podem criar e gerenciar buckets do S3 com o Tenant Manager, mas precisam ter S3 chaves de acesso e usar a API REST do S3 para ingerir e gerenciar objetos.

Informações relacionadas

Administrar o StorageGRID

Use a conta de locatário

Como as conexões do cliente podem ser configuradas

Um administrador de grade faz escolhas de configuração que afetam a forma como os clientes S3 se conetam ao StorageGRID para armazenar e recuperar dados. As informações específicas que você precisa para fazer uma conexão dependem da configuração escolhida.

Os aplicativos clientes podem armazenar ou recuperar objetos conetando-se a qualquer um dos seguintes:

- O serviço Load Balancer em nós de administração ou nós de gateway, ou, opcionalmente, o endereço IP virtual de um grupo de alta disponibilidade (HA) de nós de administração ou nós de gateway
- O serviço CLB em nós de Gateway, ou, opcionalmente, o endereço IP virtual de um grupo de nós de gateway de alta disponibilidade

> ⓘ O serviço CLB está obsoleto. Os clientes configurados antes da versão do StorageGRID 11,3 podem continuar a usar o serviço CLB nos nós de gateway. Todos os outros aplicativos clientes que dependem do StorageGRID para fornecer balanceamento de carga devem se conetar usando o serviço de balanceamento de carga.

- Nós de storage, com ou sem um balanceador de carga externo

Ao configurar o StorageGRID, um administrador de grade pode usar o Gerenciador de grade ou a API de gerenciamento de grade para executar as seguintes etapas, todas opcionais:

1. Configure endpoints para o serviço Load Balancer.

   Você deve configurar endpoints para usar o serviço Load Balancer. O serviço Load Balancer em nós de administração ou nós de gateway distribui conexões de rede recebidas de aplicativos clientes para nós de storage. Ao criar um endpoint de balanceador de carga, o administrador do StorageGRID especifica um número de porta, se o endpoint aceita conexões HTTP ou HTTPS, o tipo de cliente (S3 ou Swift) que usará o endpoint e o certificado a ser usado para conexões HTTPS (se aplicável).

2. Configurar redes de clientes não confiáveis.

   Se um administrador do StorageGRID configurar a rede cliente de um nó para não ser confiável, o nó só aceita conexões de entrada na rede cliente em portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

3. Configurar grupos de alta disponibilidade.

   Se um administrador criar um grupo de HA, as interfaces de rede de vários nós de Admin ou nós de Gateway serão colocadas em uma configuração de backup ativo. As conexões de cliente são feitas usando o endereço IP virtual do grupo HA.

Para obter mais informações sobre cada opção, consulte as instruções para administrar o StorageGRID.

Informações relacionadas

Administrar o StorageGRID

Resumo: Endereços IP e portas para conexões de clientes

Os aplicativos cliente se conetam ao StorageGRID usando o endereço IP de um nó de grade e o número da porta de um serviço nesse nó. Se os grupos de alta disponibilidade (HA) estiverem configurados, os aplicativos clientes poderão se conetar usando o endereço IP virtual do grupo HA.

Informações necessárias para fazer conexões com o cliente

A tabela resume as diferentes maneiras pelas quais os clientes podem se conetar ao StorageGRID e os endereços IP e as portas usadas para cada tipo de conexão. Contate o administrador do StorageGRID para obter mais informações ou consulte as instruções de administração do StorageGRID para obter uma descrição de como localizar essas informações no Gerenciador de Grade.

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	• Porta de extremidade do balanceador de carga
Grupo HA	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP virtual de um grupo HA	Portas S3 padrão: • HTTPS: 8082 • HTTP: 8084
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	• Porta de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	• Porta de extremidade do balanceador de carga
Nó de gateway	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP do nó de gateway **Nota:** por predefinição, as portas HTTP para CLB e LDR não estão ativadas.	Portas S3 padrão: • HTTPS: 8082 • HTTP: 8084
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084

Exemplo

Para conetar um cliente S3 ao ponto de extremidade do Load Balancer de um grupo de HA de nós de Gateway, use um URL estruturado como mostrado abaixo:

- `https://VIP-of-HA-group:_LB-endpoint-port_`

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.5 e o número da porta de um endpoint do balanceador de carga S3 for 10443, um cliente S3 poderá usar o seguinte URL para se conetar ao StorageGRID:

- `https://192.0.2.5:10443`

É possível configurar um nome DNS para o endereço IP que os clientes usam para se conetar ao StorageGRID. Contacte o administrador da rede local.

Informações relacionadas

Administrar o StorageGRID

Decida usar conexões HTTPS ou HTTP

Quando as conexões de cliente são feitas usando um endpoint de Load Balancer, as conexões devem ser feitas usando o protocolo (HTTP ou HTTPS) especificado para esse endpoint. Para usar HTTP para conexões de cliente a nós de armazenamento ou ao serviço CLB em nós de gateway, você deve habilitar seu uso.

Por padrão, quando os aplicativos cliente se conetam a nós de armazenamento ou ao serviço CLB nos nós de Gateway, eles devem usar HTTPS criptografado para todas as conexões. Opcionalmente, você pode habilitar conexões HTTP menos seguras selecionando a opção de grade **Ativar conexão HTTP** no Gerenciador de Grade. Por exemplo, um aplicativo cliente pode usar HTTP ao testar a conexão com um nó de armazenamento em um ambiente que não seja de produção.

> Tenha cuidado ao ativar o HTTP para uma grade de produção, já que as solicitações serão enviadas sem criptografia.

> O serviço CLB está obsoleto.

Se a opção **Enable HTTP Connection** estiver selecionada, os clientes devem usar portas diferentes para HTTP do que para HTTPS. Consulte as instruções para administrar o StorageGRID.

Informações relacionadas

Administrar o StorageGRID

Benefícios de conexões HTTP ativas, ociosas e simultâneas

Nomes de domínio de endpoint para solicitações S3

Antes de poder usar nomes de domínio S3 para solicitações de cliente, um administrador do StorageGRID deve configurar o sistema para aceitar conexões que usam nomes de domínio S3 em solicitações de estilo de caminho S3 e S3 solicitações virtuais de estilo hospedado.

Sobre esta tarefa

Para permitir que você use S3 solicitações de estilo hospedadas virtuais, um administrador de grade deve executar as seguintes tarefas:

- Use o Gerenciador de Grade para adicionar os nomes de domínio de endpoint S3 ao sistema StorageGRID.
- Certifique-se de que o certificado que o cliente usa para conexões HTTPS com o StorageGRID está assinado para todos os nomes de domínio que o cliente requer.

  Por exemplo, se o endpoint for `s3.company.com`, o administrador de grade deve garantir que o certificado usado para conexões HTTPS inclua o `s3.company.com` endpoint e o nome alternativo (SAN) de assunto universal (Wildcard Subject Alternative Name) do endpoint: `*.s3.company.com`.

- Configure o servidor DNS usado pelo cliente para incluir Registros DNS que correspondam aos nomes de domínio de endpoint, incluindo todos os Registros curinga necessários.

Se o cliente se conetar usando o serviço Load Balancer, o certificado que o administrador da grade configura é o certificado para o ponto de extremidade do balanceador de carga que o cliente usa.

> Cada ponto de extremidade do balanceador de carga tem seu próprio certificado e cada ponto de extremidade pode ser configurado para reconhecer nomes de domínio de endpoint diferentes.

Se o cliente se conetar a nós de armazenamento ou ao serviço CLB em nós de Gateway, o certificado que o administrador de grade configura é o único certificado de servidor personalizado usado para a grade.

> O serviço CLB está obsoleto.

Consulte as instruções para administrar o StorageGRID para obter mais informações.

Depois que essas etapas forem concluídas, você poderá usar solicitações virtuais de estilo hospedado (por exemplo, `bucket.s3.company.com`).

Informações relacionadas

Administrar o StorageGRID

Configure a segurança para a API REST

Teste a configuração da API REST do S3

Você pode usar a interface de linha de comando (AWS CLI) do Amazon Web Services para testar sua conexão com o sistema e verificar se é possível ler e gravar objetos no sistema.

O que você vai precisar

- Você baixou e instalou a AWS CLI do "aws.amazon.com/cli".
- Você criou uma conta de locatário S3 no sistema StorageGRID.

Passos

1. Configure as configurações do Amazon Web Services para usar a conta criada no sistema StorageGRID:
   a. Entre no modo de configuração: `aws configure`
   b. Insira o ID da chave de acesso da AWS para a conta criada.
   c. Insira a chave de acesso secreto da AWS para a conta criada.
   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.

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

Se o bucket for criado com êxito, a localização do bucket será retornada, como visto no exemplo a seguir:

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

1. Carregue um objeto.

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

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

2. 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
```

3. Exclua o objeto.

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

4. Elimine o balde.

```
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

Um aplicativo cliente pode usar S3 chamadas de API REST para se conetar ao StorageGRID para criar, excluir e modificar buckets, bem como armazenar e recuperar objetos.

Solicitações de cliente conflitantes

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes".

O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Controles de consistência

Os controles de consistência fornecem um equilíbrio entre a disponibilidade dos objetos

e a consistência desses objetos em diferentes nós de storage e locais, conforme necessário pela aplicação.

Por padrão, o StorageGRID garante consistência de leitura após gravação para objetos recém-criados. Qualquer GET seguindo um PUT concluído com sucesso será capaz de ler os dados recém-escritos. As 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 em um nível de consistência diferente, você pode especificar um controle de consistência para cada bucket ou para cada operação de API.

Controles de consistência

O controle de consistência afeta como os metadados que o StorageGRID usa para rastrear objetos são distribuídos entre nós e, portanto, a disponibilidade de objetos para solicitações de clientes.

Você pode definir o controle de consistência para um bucket ou 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.
- **Read-after-novo-write**: (Padrão) fornece consistência de leitura-após-gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
- **Disponível**: Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets do S3, use somente conforme necessário (por exemplo, para um bucket que contém valores de log raramente lidos, ou para operações HEAD ou GET em chaves que não existem). Não compatível com buckets do FabricPool S3.

Use controles de consistência "read-after-new-write" e "available"

Quando uma operação HEAD ou GET usa o controle de consistência "read-after-new-write", o StorageGRID executa a pesquisa em várias etapas, como segue:

- Ele primeiro procura o objeto usando uma baixa consistência.
- Se essa pesquisa falhar, ela repete a pesquisa no próximo nível de consistência até atingir um nível de consistência equivalente ao comportamento para strong-global.

Se uma operação HEAD ou GET usar o controle de consistência "read-after-novo-write", mas o objeto não existir, a pesquisa de objetos sempre alcançará um nível de consistência equivalente ao comportamento para strong-global. Como esse nível de consistência exige que várias cópias dos metadados de objetos estejam disponíveis em cada local, você pode receber um número alto de 500 erros de servidor interno se um ou mais nós de storage no mesmo local não estiverem disponíveis.

A menos que você precise de garantias de consistência semelhantes ao Amazon S3, você pode evitar esses erros para operações HEAD and GET definindo o controle de consistência como "disponível". Quando uma operação HEAD ou GET usa o controle de consistência "disponível", o StorageGRID fornece consistência eventual apenas. Ele não tenta novamente uma operação com falha em níveis crescentes de consistência,

portanto, não requer que várias cópias dos metadados do objeto estejam disponíveis.

Especifique o controle de consistência para a operação da API

Para definir o controle de consistência para uma operação de API individual, os controles de consistência devem ser suportados para a operação e você deve especificar o controle de consistência no cabeçalho da solicitação. Este exemplo define o controle de consistência como "local-trong" para uma operação GET Object.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

> Você deve usar o mesmo controle de consistência para as operações COLOCAR Objeto e OBTER Objeto.

Especifique o controle de consistência para o balde

Para definir o controle de consistência para o bucket, você pode usar a solicitação de consistência do bucket do StorageGRID PUT e a solicitação DE consistência do bucket do GET. Ou você pode usar o Gerenciador do Locatário ou a API de Gerenciamento do Locatário.

Ao definir os controlos de consistência para um balde, tenha em atenção o seguinte:

- Definir o controle de consistência para um balde determina qual controle de consistência é usado para operações S3D realizadas nos objetos no balde ou na configuração do balde. Não afeta as operações no próprio balde.
- O controle de consistência para uma operação de API individual substitui o controle de consistência para o bucket.
- Em geral, os buckets devem usar o controle de consistência padrão, "read-after-new-write". Se as solicitações não estiverem funcionando corretamente, altere o comportamento do cliente do aplicativo, se possível. Ou configure o cliente para especificar o controle de consistência para cada solicitação de API. Defina o controle de consistência no nível do balde apenas como último recurso.

Como os controles de consistência e as regras de ILM interagem para afetar a proteção de dados

Tanto a sua escolha de controle de consistência quanto a sua regra ILM afetam a forma como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, o controle de consistência usado 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 exige acesso aos metadados de um objeto e aos dados para atender às solicitações do cliente, selecionar níveis de proteção correspondentes para o nível de consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas do sistema mais previsíveis.

Os seguintes comportamentos de ingestão estão disponíveis para regras ILM:

- **Strict**: Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja devolvido

ao cliente.

- **Balanced**: O StorageGRID tenta fazer todas as cópias especificadas na regra ILM no ingest; 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.
- * Commit duplo*: O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

> Antes de selecionar o comportamento de ingestão para uma regra ILM, leia a descrição completa dessas configurações no Gerenciar objetos com ILM.

Exemplo de como o controle de consistência e a regra ILM podem interagir

Suponha que você tenha uma grade de dois locais com a seguinte regra ILM e a seguinte configuração de nível de consistência:

- **Regra ILM**: Crie duas cópias de objeto, uma no local e outra em um local remoto. O comportamento de ingestão estrita é selecionado.
- **Nível de consistência**: "Trong-global" (metadados de objetos são imediatamente distribuídos para todos os sites.)

Quando um cliente armazena um objeto na grade, o StorageGRID faz cópias de objeto e distribui metadados para ambos os sites antes de retornar sucesso ao cliente.

O objeto é totalmente protegido contra perda no momento da mensagem de ingestão bem-sucedida. Por exemplo, se o local for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existem no local remoto. O objeto é totalmente recuperável.

Se, em vez disso, você usou a mesma regra ILM e o nível de consistência "site-trong", o cliente poderá receber uma mensagem de sucesso depois que os dados do objeto forem replicados para o site remoto, mas antes que os metadados do objeto sejam distribuídos lá. Nesse caso, o nível de proteção dos metadados de objetos não corresponde ao nível de proteção dos dados de 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 níveis de consistência e regras de ILM pode ser complexa. Contacte a NetApp se necessitar de assistência.

Informações relacionadas

OBTER pedido de consistência de balde

COLOCAR pedido consistência balde

Como as regras do StorageGRID ILM gerenciam objetos

O administrador da grade cria regras de gerenciamento do ciclo de vida das informações (ILM) para gerenciar dados de objetos ingeridos no sistema StorageGRID a partir de aplicativos clientes da API REST do S3. Essas regras são então adicionadas à política ILM para determinar como e onde os dados do objeto são armazenados ao longo do tempo.

As configurações de ILM determinam os seguintes aspetos de um objeto:

- **Geografia**

O local dos dados de um objeto, seja no sistema StorageGRID (pool de storage) ou em um pool de storage de nuvem.

- **Grau de armazenamento**

  O tipo de storage usado para armazenar dados de objetos: Por exemplo, flash ou disco giratório.

- * Proteção contra perdas*

  Quantas cópias são feitas e os tipos de cópias criadas: Replicação, codificação de apagamento ou ambos.

- **Retenção**

  As mudanças ao longo do tempo para como os dados de um objeto são gerenciados, onde são armazenados e como eles são protegidos contra perda.

- **Proteção durante o consumo**

  O método usado para proteger dados de objetos durante a ingestão: Colocação síncrona (usando as opções balanceadas ou rigorosas para o comportamento de ingestão) ou fazendo cópias provisórias (usando a opção de confirmação dupla).

As regras do ILM podem filtrar e selecionar objetos. Para objetos ingeridos usando S3, as regras do ILM podem filtrar objetos com base nos seguintes metadados:

- Conta de locatário
- Nome do balde
- Tempo de ingestão
- Chave
- Último tempo de acesso

> Por padrão, as atualizações para o último tempo de acesso são desativadas para todos os buckets do S3. Se o seu sistema StorageGRID incluir uma regra ILM que use a opção último tempo de acesso, você deverá habilitar as atualizações para o último tempo de acesso para os buckets do S3 especificados nessa regra. Você pode habilitar as atualizações da última hora de acesso usando a solicitação de última hora de acesso do PUT Bucket, a caixa de seleção **S3 Buckets Configurar último tempo de acesso** no Gerenciador de locatário ou usando a API de Gerenciamento de locatário. Ao ativar as atualizações da última hora de acesso, esteja ciente de que o desempenho do StorageGRID pode ser reduzido, especialmente em sistemas com objetos pequenos.

- Restrição de localização
- Tamanho do objeto
- Metadados do utilizador
- Etiqueta Objeto

Para obter mais informações sobre o ILM, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Informações relacionadas

Use a conta de locatário

Gerenciar objetos com ILM

COLOCAR o último pedido de tempo de acesso do balde

Controle de versão de objetos

Você pode usar o controle de versão para reter várias versões de um objeto, o que protege contra a exclusão acidental de objetos e permite recuperar e restaurar 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 1.000 versões de cada objeto.

O controle de versão de objetos pode ser combinado com o gerenciamento do ciclo de vida das informações do StorageGRID (ILM) ou com a configuração do ciclo de vida do bucket do S3. Você deve habilitar explicitamente o controle de versão para cada bucket para ativar essa funcionalidade para o bucket. Cada objeto no seu bucket recebe um ID de versão, que é gerado pelo sistema StorageGRID.

O uso de MFA (autenticação multifator) Excluir não é compatível.

> O controle de versão pode ser ativado somente em buckets criados com o StorageGRID versão 10,3 ou posterior.

ILM e versionamento

As políticas de ILM são aplicadas a cada versão de um objeto. Um processo de digitalização ILM verifica continuamente todos os objetos e os reavalia em relação à política ILM atual. Quaisquer alterações feitas às políticas ILM são aplicadas a todos os objetos ingeridos anteriormente. Isso inclui versões ingeridas anteriormente se o controle de versão estiver ativado. A digitalização ILM aplica novas alterações ILM a objetos ingeridos anteriormente.

Para objetos S3 em buckets habilitados para versionamento, o suporte ao versionamento permite criar regras ILM que usam o tempo não-atual como o tempo de referência. Quando um objeto é atualizado, suas versões anteriores se tornam não atuais. O uso de um filtro de tempo não atual permite criar políticas que reduzam o impactos de armazenamento de versões anteriores de objetos.

> Quando você carrega uma nova versão de um objeto usando uma operação de upload multipart, o tempo não atual para a versão original do objeto reflete quando o upload multipart foi criado para a nova versão, não quando o upload multipart foi concluído. Em casos limitados, o tempo não atual para a versão original pode ser horas ou dias antes do tempo para a versão atual.

Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações para obter um exemplo de política ILM para objetos com versão S3.

Informações relacionadas

Gerenciar objetos com ILM

Recomendações para a implementação da API REST do S3

Você deve seguir estas recomendações ao implementar a API REST do S3 para uso com o StorageGRID.

Recomendações para heads to non-existent objects

Se seu aplicativo verifica rotineiramente para ver se um objeto existe em um caminho onde você não espera que o objeto realmente exista, você deve usar o controle de consistência ""disponível"". Por exemplo, você deve usar o controle de consistência "disponível" se seu aplicativo dirigir um local antes DE COLOCÁ-lo.

Caso contrário, se a operação PRINCIPAL não encontrar o objeto, você poderá receber um número alto de 500 erros de servidor interno se um ou mais nós de storage não estiverem disponíveis.

Você pode definir o controle de consistência "'disponível'" para cada bucket usando a solicitação de consistência do PUT Bucket, ou você pode especificar o controle de consistência no cabeçalho da solicitação para uma operação de API individual.

Recomendações para chaves de objeto

Para buckets criados no StorageGRID 11,4 ou posterior, não é mais necessário restringir nomes de chaves do objeto para atender às práticas recomendadas de desempenho. Por exemplo, agora você pode usar valores aleatórios para os primeiros quatro carateres de nomes de chave de objeto.

Para buckets que foram criados em versões anteriores ao StorageGRID 11,4, continue seguindo estas recomendações para nomes de chaves de objeto:

- Você não deve usar valores aleatórios como os primeiros quatro carateres de chaves de objeto. Isso contrasta com a antiga recomendação da AWS para prefixos-chave. Em vez disso, você deve usar prefixos não aleatórios e não exclusivos, como `image` .
- Se você seguir a antiga recomendação da AWS para usar carateres aleatórios e exclusivos em prefixos de chave, você deve prefixar 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
  ```

Recomendações para "leituras de intervalo"

Se a opção **Compress Stored Objects** estiver selecionada (**CONFIGURATION System Grid options**), os aplicativos cliente S3 devem evitar executar operações GET Object que especificem um intervalo de bytes que sejam retornados. Essas operações de leitura de intervalo são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GET Object que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é muito ineficiente ler um intervalo de 10 MB de um objeto compactado de 50 GB.

Se os intervalos forem lidos a partir de objetos compatados, as solicitações do cliente podem expirar.

> Se você precisar compactar objetos e seu aplicativo cliente precisar usar leituras de intervalo, aumente o tempo limite de leitura para o aplicativo.

Informações relacionadas

- Controles de consistência

- COLOCAR pedido consistência balde
- Administrar o StorageGRID

S3 operações e limitações suportadas pela API REST

O sistema StorageGRID implementa a API de serviço de armazenamento simples (API versão 2006-03-01) com suporte para a maioria das operações e com algumas limitações. Você precisa entender os detalhes da implementação quando você está integrando aplicativos clientes REST API do S3.

O sistema StorageGRID oferece suporte a solicitações virtuais de estilo hospedado e a solicitações de estilo de caminho.

Tratamento da data

A implementação do StorageGRID da API REST S3 suporta apenas formatos de data HTTP válidos.

O sistema StorageGRID suporta apenas formatos de data HTTP válidos para qualquer cabeçalho que aceite valores de data. A parte da hora da data pode ser especificada no formato Greenwich Mean Time (GMT) ou no formato Universal Coordinated Time (UTC) sem deslocamento de fuso horário (o 0000 deve ser especificado). Se você incluir o `x-amz-date` cabeçalho em sua solicitação, ele substituirá qualquer valor especificado no cabeçalho da solicitação de data. Ao usar o AWS Signature versão 4, o `x-amz-date` cabeçalho deve estar presente na solicitação assinada porque o cabeçalho de data não é suportado.

Cabeçalhos de solicitação comuns

O sistema StorageGRID suporta cabeçalhos de solicitação comuns definidos pelo "Documentação do Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service", com uma exceção.

Cabeçalho da solicitação	Implementação
Autorização	Suporte completo para AWS Signature versão 2 Suporte para AWS Signature versão 4, com as seguintes exceções: • O valor SHA256 não é calculado para o corpo da solicitação. O valor enviado pelo usuário é aceito sem validação, como se o valor `UNSIGNED-PAYLOAD` tivesse sido fornecido para o `x-amz-content-sha256` cabeçalho.
x-amz-security-token	Não implementado. Retorna `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 suporta acesso autenticado e anônimo a objetos usando a API S3.

A API S3 suporta a assinatura versão 2 e a assinatura versão 4 para autenticar solicitações de API S3.

As solicitações autenticadas devem ser assinadas usando seu ID de chave de acesso e chave de acesso secreta.

O sistema StorageGRID suporta dois métodos de autenticação: O cabeçalho HTTP `Authorization` e o uso de parâmetros de consulta.

Use o cabeçalho de autorização HTTP

O cabeçalho HTTP `Authorization` é usado por todas as operações da API S3, exceto solicitações anônimas, onde permitido pela política de bucket. O `Authorization` cabeçalho contém todas as informações de assinatura necessárias para autenticar uma solicitação.

Use parâmetros de consulta

Você pode usar parâmetros de consulta para adicionar informações de autenticação a um URL. Isso é conhecido como pré-assinar o URL, que pode ser usado para conceder acesso temporário a recursos específicos. Os usuários com o URL pré-assinado não precisam saber a chave de acesso secreto 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
Serviço GET	Implementado com todo o comportamento da API REST do Amazon S3.
OBTER uso de armazenamento	A solicitação OBTER uso do armazenamento 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.

Operação	Implementação
OPÇÕES /	Os aplicativos clientes podem emitir `OPTIONS /` solicitações para a porta S3 em um nó de storage, sem fornecer credenciais de autenticação S3.1X, para determinar se o nó de storage está disponível. Você pode usar essa solicitação para monitoramento ou permitir que balanceadores de carga externos identifiquem quando um nó de storage está inativo.

Informações relacionadas

OBTER solicitação de uso de armazenamento

Operações em baldes

O sistema StorageGRID dá suporte a um máximo de 1.000 buckets para cada conta de locatário de S3 TB.

As restrições de nome de bucket seguem as restrições de região padrão dos EUA da AWS, mas você deve restringi-las ainda mais a convenções de nomenclatura de DNS para oferecer suporte a solicitações de estilo hospedado virtual do S3.

"Documentação do Amazon Web Services (AWS): Restrições e limitações do bucket"

Configure os nomes de domínio de endpoint da API S3

As operações GET Bucket (List Objects) e GET Bucket Versions suportam controles de consistência do StorageGRID.

Você pode verificar se as atualizações para a última hora de acesso estão ativadas ou desativadas para buckets individuais.

A tabela a seguir descreve como o StorageGRID implementa as operações de bucket da API REST do S3. Para realizar qualquer uma dessas operações, as credenciais de acesso necessárias devem ser fornecidas para a conta.

Operação	Implementação
ELIMINAR balde	Implementado com todo o comportamento da API REST do Amazon S3.
ELIMINAR Cors balde	Esta operação exclui a configuração CORS para o bucket.
ELIMINAR encriptação Bucket	Esta operação exclui a criptografia padrão do intervalo. Os objetos criptografados existentes permanecem criptografados, mas todos os novos objetos adicionados ao bucket não são criptografados.
ELIMINAR ciclo de vida do balde	Esta operação exclui a configuração do ciclo de vida do bucket.

Operação	Implementação
ELIMINAR política de balde	Esta operação exclui a política anexada ao bucket.
ELIMINAR replicação de balde	Esta operação exclui a configuração de replicação anexada ao bucket.
ELIMINAR marcação de intervalo	Esta operação usa o `tagging` subrecurso para remover todas as tags de um bucket.
GET Bucket (List Objects), versão 1 e versão 2	Esta operação retorna alguns ou todos (até 1.000) dos objetos em um balde. A Classe de armazenamento para objetos pode ter um de dois valores, mesmo que o objeto tenha sido ingerido com a `REDUCED_REDUNDANCY` opção de classe de armazenamento: • `STANDARD`, Que indica que o objeto está armazenado em um pool de storage que consiste em nós de storage. • `GLACIER`, Que indica que o objeto foi movido para o bucket externo especificado pelo pool de armazenamento em nuvem. Se o intervalo contiver um grande número de chaves excluídas que tenham o mesmo prefixo, a resposta pode incluir algumas `CommonPrefixes` que não contêm chaves.
OBTER acl balde	Esta operação retorna uma resposta positiva e a ID, DisplayName e permissão do proprietário do bucket, indicando que o proprietário tem acesso total ao bucket.
OBTER Bucket Cors	Esta operação retorna a `cors` configuração do balde.
OBTER criptografia Bucket	Esta operação retorna a configuração de criptografia padrão para o bucket.
OBTENHA o ciclo de vida do Bucket	Esta operação retorna a configuração do ciclo de vida do bucket.
OBTER localização do balde	Esta operação retorna a região que foi definida usando o `LocationConstraint` elemento na solicitação PUT Bucket. Se a região do bucket for `us-east-1`, uma string vazia será retornada para a região.
OBTER notificação Bucket	Esta operação retorna a configuração de notificação anexada ao bucket.
OBTER versões Objeto balde	Com ACESSO DE LEITURA em um bucket, essa operação com o `versions` subrecurso lista metadados de todas as versões de objetos no bucket.
OBTER política Bucket	Esta operação retorna a política anexada ao bucket.

Operação	Implementação
OBTER replicação do bucket	Esta operação retorna a configuração de replicação anexada ao bucket.
OBTER marcação Bucket	Esta operação usa o `tagging` subrecurso para retornar todas as tags para um bucket.
OBTENHA o controle de versão do Bucket	Essa implementação usa `versioning` o subrecurso para retornar o estado de controle de versão de um bucket. • *Blank*: O controle de versão nunca foi habilitado (o bucket é "não versionado") • Habilitado: O controle de versão está habilitado • Suspenso: O controle de versão foi ativado anteriormente e está suspenso
OBTER Configuração bloqueio Objeto	Esta operação retorna o modo de retenção padrão do bucket e o período de retenção padrão, se configurado. OBTER Configuração bloqueio ObjetoConsulte para obter informações detalhadas.
Balde DA cabeça	Esta operação determina se existe um intervalo e 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.

Operação	Implementação
COLOQUE o balde	Esta operação cria um novo balde. Ao criar o balde, você se torna o proprietário do balde. • Os nomes dos buckets devem estar em conformidade com as seguintes regras: ◦ Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário). ◦ Deve ser compatível com DNS. ◦ Deve conter pelo menos 3 e não mais de 63 carateres. ◦ Pode ser uma série de uma ou mais etiquetas, com etiquetas adjacentes separadas por um período. Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hífens. ◦ Não deve se parecer com um endereço IP formatado em texto. ◦ Não deve usar períodos em solicitações de estilo hospedadas virtuais. Os períodos causarão problemas com a verificação do certificado curinga do servidor. • Por padrão, os intervalos são criados na `us-east-1` região; no entanto, você pode usar o `LocationConstraint` elemento de solicitação 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 Gerenciador de Grade ou a API de Gerenciamento de Grade. Contacte o administrador do sistema se não souber o nome da região que deve utilizar. **Nota**: Ocorrerá um erro se a solicitação PUT Bucket usar uma região que não foi definida no StorageGRID. • Você pode incluir o `x-amz-bucket-object-lock-enabled` cabeçalho de solicitação para criar um bucket com o bloqueio de objeto S3 ativado. Use o bloqueio de objetos S3D.Consulte . Você deve ativar o bloqueio de objeto S3 quando você criar o bucket. Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação de um intervalo. O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.
COLOQUE cors de balde	Esta operação define a configuração do CORS para um bucket de modo que o bucket possa atender às solicitações de origem cruzada. O compartilhamento de recursos de origem cruzada (CORS) é um mecanismo de segurança que permite que aplicativos da Web do cliente em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket S3 chamado `images` para armazenar gráficos. Ao definir a configuração CORS para o `images` intervalo, pode permitir que as imagens nesse intervalo sejam apresentadas no website `http://www.example.com`.

Operação	Implementação
COLOQUE a criptografia Bucket	Esta operação define o estado de criptografia padrão de um bucket existente. Quando a criptografia no nível do bucket está ativada, todos os novos objetos adicionados ao bucket são criptografados. O StorageGRID suporta criptografia no lado do servidor com chaves gerenciadas pelo StorageGRID. Ao especificar a regra de configuração de criptografia do lado do servidor, defina o `SSEAlgorithm` parâmetro como `AES256`, e não use o `KMSMasterKeyID` parâmetro. A configuração de criptografia padrão do bucket é ignorada se a solicitação de upload de objeto já especificar criptografia (ou seja, se a solicitação incluir o `x-amz-server-side-encryption-*` cabeçalho da solicitação).
COLOQUE o ciclo de vida do balde	Essa operação cria uma nova configuração de ciclo de vida para o bucket ou substitui uma configuração de ciclo de vida existente. O StorageGRID dá suporte a até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML: • Validade (dias, Data) • Não-currentVersionExpiration (não-currentDays) • Filtro (prefixo, Tag) • Estado • ID O StorageGRID não oferece suporte a essas ações: • AbortIncompleteMultipartUpload • ExpiredObjectDeleteMarker • Transição Para entender como a ação Expiration em um ciclo de vida de um bucket interage com as instruções de colocação do ILM, consulte "como o ILM opera ao longo da vida de um objeto" nas instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações. **Nota**: A configuração do ciclo de vida do bucket pode ser usada com buckets que têm o S3 Object Lock ativado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis com o legado.

Operação	Implementação

COLOCAR notificação de balde	Esta operação 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 a tópicos do Serviço de notificação simples (SNS) como destinos. Os endpoints do Simple Queue Service (SQS) ou do Amazon Lambda não são suportados.
	• O destino das notificações deve ser especificado como a URNA de um endpoint do StorageGRID. Os endpoints podem ser criados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário.
	O endpoint deve existir para que a configuração de notificação seja bem-sucedida. Se o endpoint 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 são **não** suportados.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• As notificações de eventos enviadas do StorageGRID usam o formato JSON padrão, exceto que elas não incluem algumas chaves e usam valores específicos para outras, como mostrado na seguinte listagem:
	• **EventSource**
	`sgws:s3`
	• **AwsRegion**
	não incluído
	• **x-amz-id-2**
	não incluído
	• **arn**
	`urn:sgws:s3:::bucket_name`

Política COLOCAR balde	Esta operação define a política anexada ao balde.

Operação	Implementação
COLOQUE a replicação do balde	Esta operação configura a replicação do StorageGRID CloudMirror para o bucket usando o XML de configuração de replicação fornecido no corpo da solicitação. Para a replicação do CloudMirror, você deve estar ciente dos seguintes detalhes de implementação: • O StorageGRID suporta apenas V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue convenções V1 para exclusão de versões de objetos. Para obter detalhes, consulte "Documentação do Amazon S3 sobre configuração de replicação" . • A replicação do bucket pode ser configurada em buckets versionados ou não versionados. • Você pode especificar um intervalo 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 a URN dos endpoints do StorageGRID, conforme especificado no Gerenciador do Locatário ou na API de Gerenciamento do Locatário. O endpoint deve existir para que a configuração de replicação seja bem-sucedida. Se o endpoint não existir, a solicitação falhará como um `400 Bad Request`. a mensagem de erro indica: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Não é necessário 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 a `STANDARD` classe de armazenamento por padrão. • Se você excluir um objeto do bucket de origem ou excluir o bucket de origem, o comportamento de replicação entre regiões é o seguinte: ◦ Se você excluir o objeto ou o bucket antes que ele tenha sido replicado, o objeto/bucket não será replicado e você não será notificado. ◦ Se você excluir o objeto ou o bucket depois que ele foi replicado, o StorageGRID segue o comportamento padrão de exclusão do Amazon S3 para V1 TB de replicação entre regiões.
COLOQUE a marcação de balde	Esta operação usa o `tagging` subrecurso para adicionar ou atualizar um conjunto de tags para um bucket. Ao adicionar etiquetas de bucket, esteja ciente das seguintes limitações: • O StorageGRID e 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 carateres Unicode de comprimento. • Os valores de tag podem ter até 256 carateres Unicode de comprimento. • Chave e valores são sensíveis a maiúsculas e minúsculas.

Operação	Implementação
COLOQUE o controle de versão do Bucket	Essa implementação usa `versioning` o subrecurso 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: Permite o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo. • Suspenso: Desativa o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão `null` .
COLOCAR Configuração bloqueio Objeto	Esta operação 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 até as versões de objetos existentes permanecerá a mesma e não será recalculada usando o novo período de retenção padrão. COLOCAR Configuração bloqueio ObjetoConsulte para obter informações detalhadas.

Informações relacionadas

Controles de consistência

OBTER último pedido de tempo de acesso do Bucket

Políticas de acesso ao bucket e ao grupo

S3 operações rastreadas em logs de auditoria

Gerenciar objetos com ILM

Use a conta de locatário

Crie a 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 do ciclo de vida do S3 pode controlar quando certos objetos são excluídos (expirados) de buckets específicos do S3. O exemplo nesta seção é apenas para fins ilustrativos. Para obter detalhes completos sobre como criar configurações de ciclo de vida do S3, "Amazon Simple Storage Service Developer Guide: Gerenciamento do ciclo de vida do objeto" consulte . Observe que o StorageGRID suporta apenas ações de expiração; ele não oferece suporte a ações de transição.

Qual é a configuração do ciclo de vida

Uma configuração de ciclo de vida é um conjunto de regras que são 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 algum número de dias).

O StorageGRID dá suporte a 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 é atingida ou quando um número especificado de dias é atingido, a partir de quando o objeto foi ingerido.
- NoncurrentVersionExpiration: Exclua um objeto quando um número especificado de dias é atingido, a partir de quando o objeto se tornou inatual.
- Filtro (prefixo, Tag)
- Estado
- ID

Se você aplicar uma configuração de ciclo de vida a um bucket, as configurações de ciclo de vida do bucket sempre substituem as configurações de ILM do StorageGRID. O StorageGRID usa as configurações de expiração para o bucket, não o ILM, para determinar se deseja excluir ou reter objetos específicos.

Como resultado, um objeto pode ser removido da grade, mesmo que as instruções de colocação em uma regra ILM ainda se apliquem ao objeto. Ou, um objeto pode ser retido na grade mesmo depois que quaisquer instruções de colocação de ILM para o objeto tiverem expirado. Para obter detalhes, Como o ILM opera ao longo da vida de um objetoconsulte .

> A configuração do ciclo de vida do bucket pode ser usada com buckets que têm o S3 Object Lock ativado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis com legado.

O StorageGRID dá suporte ao uso das seguintes operações de bucket para gerenciar configurações do ciclo de vida:

- ELIMINAR ciclo de vida do balde
- OBTENHA o ciclo de vida do Bucket
- COLOQUE o ciclo de vida do balde

Criar configuração do 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 aplica-se apenas a objetos que correspondam ao prefixo `category1/` e que tenham um `key2` valor `tag2` de . O `Expiration` parâmetro especifica que os objetos correspondentes ao filtro expirarão à meia-noite de 22 de agosto de 2020.
2. A regra 2 aplica-se apenas a objetos que correspondam ao prefixo `category2/`. O `Expiration` parâmetro especifica que os objetos correspondentes ao filtro expirarão 100 dias após serem ingeridos.

   > As 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 podem ser removidos do intervalo assim que a configuração do ciclo de vida for aplicada.

3. A regra 3 aplica-se apenas a objetos que correspondam ao prefixo `category3/`. O `Expiration` parâmetro especifica que quaisquer versões não atuais de objetos correspondentes expirarão 50 dias após se tornarem não atuais.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Aplique a configuração do ciclo de vida ao bucket

Depois de criar o arquivo de configuração do ciclo de vida, aplique-o a um bucket emitindo uma solicitação DE ciclo de vida do PUT Bucket.

Essa solicitação aplica a configuração do ciclo de vida no arquivo de exemplo a objetos em um bucket `testbucket` chamado .

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que uma configuração de ciclo de vida foi aplicada com sucesso ao bucket, emita uma solicitação DE ciclo de vida do GET Bucket. 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.

Valide que a expiração do ciclo de vida do bucket se aplica ao objeto

É possível determinar se uma regra de expiração na configuração do ciclo de vida se aplica a um objeto específico ao emitir uma SOLICITAÇÃO PUT Object, HEAD Object ou GET Object. Se uma regra se aplicar, a resposta inclui um `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, a `expiry-date` mostrada é a data real em que o objeto será excluído. Para obter detalhes, Como a retenção de objetos é determinadaconsulte .

Por exemplo, essa SOLICITAÇÃO PUT Object foi emitida em 22 de junho de 2020 e coloca um objeto no `testbucket` intervalo.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

A resposta de sucesso indica que o objeto expirará em 100 dias (01 de outubro de 2020) e que correspondia 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, essa solicitação de objeto PRINCIPAL foi usada para obter metadados para o mesmo objeto no bucket do testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

A resposta de sucesso inclui os metadados do objeto e indica que o objeto expirará em 100 dias e que correspondia 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": {}
}
```

Use retenção padrão do bucket do bloqueio de objetos S3

Se um bucket tiver o bloqueio de objetos S3 ativado, você poderá especificar um modo de retenção padrão e um período de retenção padrão que é aplicado a cada objeto adicionado ao bucket.

- S3 o bloqueio de objetos pode ser ativado ou desativado para um balde durante a criação do balde.
- Se o bloqueio de objetos S3 estiver ativado para um bucket, você poderá configurar a retenção padrão para o bucket.
- A configuração de retenção padrão especifica:
  - Modo de retenção padrão: O StorageGRID suporta apenas o modo de "CONFORMIDADE".
  - Período de retenção padrão em dias ou anos.

OBTER Configuração bloqueio Objeto

A solicitação DE configuração GET Object Lock permite determinar se o Object Lock está habilitado para um bucket e, se ele está ativado, ver se há um modo de retenção padrão e período de retenção configurados para o bucket.

Quando novas versões de objetos são ingeridas para o bucket, o modo de retenção padrão é aplicado se `x-amz-object-lock-mode` não for especificado. O período de retenção padrão é usado para calcular a data de retenção até se `x-amz-object-lock-retain-until-date` não for especificado.

Você deve ter a permissão S3:GetBucketObjectLockConfiguration, ou ser raiz 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>
```

COLOCAR Configuração bloqueio Objeto

A solicitação de configuração de bloqueio de objeto PUT permite modificar o modo de retenção padrão e o período de retenção padrão para um bucket que tem bloqueio de objeto ativado. Você também pode remover as configurações de retenção padrão configuradas anteriormente.

Quando novas versões de objetos são ingeridas para o bucket, o modo de retenção padrão é aplicado se `x-amz-object-lock-mode` não for especificado. O período de retenção padrão é usado para calcular a data de retenção até se `x-amz-object-lock-retain-until-date` não for especificado.

Se o período de retenção padrão for modificado após a ingestão de uma versão de objeto, a data de retenção até a versão do objeto permanecerá a mesma e não será recalculada usando o novo período de retenção padrão.

Você deve ter a permissão S3:PutBucketObjectLockConfiguration, ou ser raiz da conta, para concluir esta operação.

O `Content-MD5` cabeçalho da solicitação deve ser especificado na solicitação DE COLOCAÇÃO.

Exemplo de solicitação

```
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>
```

Operações personalizadas em buckets

O sistema StorageGRID dá suporte a operações de bucket personalizadas que são adicionadas à API REST do S3 e são específicas do sistema.

A tabela a seguir lista as operações de bucket personalizadas suportadas pelo StorageGRID.

Operação	Descrição	Para mais informações
OBTER consistência de balde	Retorna o nível de consistência que está sendo aplicado a um balde específico.	OBTER pedido de consistência de balde

Operação	Descrição	Para mais informações
COLOQUE a consistência do balde	Define o nível de consistência aplicado a um balde específico.	COLOCAR pedido consistência balde
OBTER último tempo de acesso do Bucket	Retorna se as atualizações da última hora de acesso estão ativadas ou desativadas para um intervalo específico.	OBTER último pedido de tempo de acesso do Bucket
COLOQUE o último tempo de acesso do balde	Permite-lhe ativar ou desativar as atualizações da última hora de acesso para um intervalo específico.	COLOCAR o último pedido de tempo de acesso do balde
ELIMINAR configuração de notificação de metadados do bucket	Exclui o XML de configuração de notificação de metadados associado a um bucket específico.	EXCLUIR solicitação de configuração de notificação de metadados do bucket
OBTER configuração de notificação de metadados do bucket	Retorna o XML de configuração de notificação de metadados associado a um intervalo específico.	OBTER solicitação de configuração de notificação de metadados do bucket
COLOQUE a configuração de notificação de metadados do bucket	Configura o serviço de notificação de metadados para um bucket.	COLOCAR solicitação de configuração de notificação de metadados do bucket
COLOQUE o balde com as definições de conformidade	Obsoleto e não suportado: Você não pode mais criar novos buckets com a conformidade ativada.	Obsoleto: COLOQUE o Bucket com as configurações de conformidade
OBTENHA conformidade com o balde	Obsoleto, mas suportado: Retorna as configurações de conformidade atualmente em vigor para um bucket compatível com legado existente.	Obsoleto: OBTER solicitação de conformidade do bucket
COLOQUE a conformidade do balde	Obsoleto, mas suportado: Permite modificar as configurações de conformidade para um bucket compatível com legado existente.	Obsoleto: COLOQUE a solicitação de conformidade do bucket

Informações relacionadas

S3 operações rastreadas nos logs de auditoria

Operações em objetos

Esta seção descreve como o sistema StorageGRID implementa S3 operações de API REST para objetos.

As seguintes condições se aplicam a todas as operações de objetos:

- Os StorageGRID controles de consistênciasão suportados por todas as operações em objetos, com exceção dos seguintes:
  - OBTER ACL Objeto
  - `OPTIONS /`
  - COLOCAR guarda legal Objeto
  - COLOCAR retenção Objeto
  - SELECIONE conteúdo do objeto
- As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação, e não em quando os clientes S3 começam uma operação.
- Todos os objetos em um bucket do StorageGRID são de propriedade do proprietário do bucket, incluindo objetos criados por um usuário anônimo ou por outra conta.
- Os objetos de dados ingeridos para o sistema StorageGRID através do Swift não podem ser acedidos através do S3.

A tabela a seguir descreve como o StorageGRID implementa operações de objetos API REST do S3.

Operação	Implementação
Objeto DELETE	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. Ao processar uma solicitação DE EXCLUSÃO de objetos, o StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais armazenados. Se for bem-sucedido, o StorageGRID retornará uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas dentro de 30 segundos (por exemplo, porque um local está temporariamente indisponível), o StorageGRID coloca as cópias em fila para remoção e, em seguida, indica sucesso para o cliente. **Controle de versão** Para remover uma versão específica, o solicitante deve ser o proprietário do bucket e usar o `versionId` subrecurso. O uso deste subrecurso exclui permanentemente a versão. Se o `versionId` corresponder a um marcador de exclusão, o cabeçalho de resposta `x-amz-delete-marker` será retornado como `true`. • Se um objeto for excluído sem o `versionId` subrecurso em um bucket habilitado para versão, isso resultará 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` cabeçalho de resposta é retornado como `true`. • Se um objeto for excluído sem o `versionId` sub-recurso em um bucket suspenso de versão, ele resultará em uma exclusão permanente de uma versão 'null' já existente ou um marcador 'null' delete, e a geração de um novo marcador 'null' delete. O `x-amz-delete-marker` cabeçalho de resposta é retornado definido como `true`. **Nota**: Em certos casos, vários marcadores de exclusão podem existir para um objeto.
Excluir vários objetos	Autenticação multifator (MFA) e o cabeçalho de resposta `x-amz-mfa` não são suportados. Vários objetos podem ser excluídos na mesma mensagem de solicitação.

Operação	Implementação
ELIMINAR marcação Objeto	Usa o `tagging` subrecurso para remover todas as tags de um objeto. Implementado com todo o comportamento da API REST do Amazon S3. **Controle de versão** Se o `versionId` parâmetro de consulta não for especificado na solicitação, a operação excluirá todas as tags da versão mais recente do objeto em um bucket com versão. 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`.
Objeto GET	Objeto GET
OBTER ACL Objeto	Se as credenciais de acesso necessárias forem fornecidas para a conta, a operação retornará uma resposta positiva e a ID, DisplayName e permissão do proprietário do objeto, indicando que o proprietário tem acesso total ao objeto.
OBTER retenção legal Objeto	Use o bloqueio de objetos S3D.
OBTER retenção de objetos	Use o bloqueio de objetos S3D.
OBTER marcação de objetos	Usa o `tagging` subrecurso para retornar todas as tags para um objeto. Implementado com todo o comportamento da API REST do Amazon S3 **Controle de versão** Se o `versionId` 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`.
Objeto HEAD	Objeto HEAD
Restauração PÓS-objeto	Restauração PÓS-objeto
Objeto PUT	Objeto PUT
COLOCAR Objeto - Copiar	COLOCAR Objeto - Copiar
COLOCAR guarda legal Objeto	Use o bloqueio de objetos S3D.
COLOCAR retenção Objeto	Use o bloqueio de objetos S3D.

Operação	Implementação
COLOQUE a marcação Objeto	Usa o `tagging` subrecurso para adicionar um conjunto de tags a um objeto existente. Implementado com todo o comportamento da API REST do Amazon S3 • Limites de tag de objeto* Você pode adicionar tags a novos objetos ao enviá-los ou adicioná-los a objetos existentes. O StorageGRID e o Amazon S3 suportam até 10 tags para cada objeto. Tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 carateres Unicode de comprimento e os valores de tag podem ter até 256 carateres Unicode de comprimento. Chave e valores são sensíveis a maiúsculas e minúsculas. **Atualizações de tags e comportamento de ingestão** Quando você usa a marcação "COLOCAR objeto" para atualizar as tags de um objeto, o StorageGRID não reingere o objeto. Isso significa que a opção de comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento de objetos que são acionadas pela atualização são feitas quando o ILM é reavaliado por processos normais de ILM em segundo plano. Isso significa que, se a regra ILM usar a opção estrita para o comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objeto necessários não puderem ser feitos (por exemplo, porque um local recém-exigido não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível. **Resolução de conflitos** As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação, e não em quando os clientes S3 começam uma operação. **Controle de versão** Se o `versionId` parâmetro de consulta não for especificado na solicitação, a operação adicionará tags à versão mais recente do objeto em um bucket com versão. 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`.

Informações relacionadas

S3 operações rastreadas em logs de auditoria

Use o bloqueio de objetos S3D.

Se a configuração global de bloqueio de objetos S3 estiver ativada para o seu sistema StorageGRID, você poderá criar buckets com o bloqueio de objetos S3 ativado e especificar períodos de retenção padrão para cada bucket ou configurações específicas de retenção até a data e retenção legal para cada versão de objeto adicionada a esse bucket.

O bloqueio de objetos S3 permite especificar configurações no nível do objeto para impedir que objetos sejam excluídos ou substituídos por um período fixo de tempo ou indefinidamente.

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

Ative o bloqueio de objetos S3D para o balde

Se a configuração global de bloqueio de objetos S3 estiver ativada para o seu sistema StorageGRID, você poderá ativar opcionalmente o bloqueio de objetos S3 quando criar cada bucket. Você pode usar qualquer um destes métodos:

- Crie o bucket usando o Gerenciador do locatário.

  Use a conta de locatário

- Crie o bucket usando uma solicitação DE COLOCAR balde com o `x-amz-bucket-object-lock-enabled` cabeçalho de solicitação.

  Operações em baldes

Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação do bucket. O bloqueio de objetos S3 requer o controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.

Um bucket com S3 Object Lock ativado pode conter uma combinação de objetos com e sem configurações de bloqueio de objeto S3. O StorageGRID oferece suporte a períodos de retenção padrão para os objetos nos buckets do bloqueio de objetos do S3 e suporta a operação do bucket Configuração do bloqueio de objetos do PUT. A `s3:object-lock-remaining-retention-days` chave de condição de política define os períodos de retenção mínimo e máximo permitidos para seus objetos.

Determinar se o bloqueio de objetos S3 está ativado para o balde

Para determinar se o bloqueio de objeto S3 está ativado, use a OBTER Configuração bloqueio Objeto solicitação.

Crie objeto com as configurações de bloqueio de objeto S3

Para especificar as configurações de bloqueio de objeto S3 ao adicionar uma versão de objeto a um intervalo que tenha o bloqueio de objeto S3 ativado, emita um Objeto PUT, COLOCAR Objeto - Copiar ou inicie uma solicitação de upload de várias partes. Use os cabeçalhos de solicitação a seguir.

Você deve habilitar o bloqueio de objeto S3 quando criar um bucket. Não é possível adicionar ou desativar o bloqueio de objetos S3 após a criação de um intervalo.

- `x-amz-object-lock-mode`, Que deve ser CONFORMIDADE (sensível a maiúsculas e 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 ATIVADA (sensível a maiúsculas e minúsculas), o objeto é colocado sob uma retenção legal. Se a retenção legal estiver DESLIGADA, nenhuma retenção legal será colocada. Qualquer outro valor resulta em um erro de 400 Bad Request (InvalidArgument).

Se você usar qualquer um desses cabeçalhos de solicitação, esteja ciente dessas restrições:

- O `Content-MD5` cabeçalho de solicitação é necessário se qualquer `x-amz-object-lock-*` cabeçalho de solicitação estiver presente na solicitação DE Objeto PUT. `Content-MD5` Não é necessário para COLOCAR Objeto - Copiar ou iniciar carregamento Multipart.
- Se o bucket não tiver o bloqueio de objeto S3 ativado e um `x-amz-object-lock-*` cabeçalho de solicitação estiver presente, um erro de solicitação incorreta 400 (InvalidRequest) será retornado.
- A solicitação put Object suporta o uso do `x-amz-storage-class: REDUCED_REDUNDANCY` para corresponder ao comportamento da AWS. No entanto, quando um objeto é ingerido em um bucket com o bloqueio de objeto S3 ativado, o StorageGRID sempre realizará uma ingestão de confirmação dupla.
- Uma resposta DE versão DE GET ou HEAD Object posterior 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 as permissões corretas `s3:Get*`.
- Uma solicitação DE versão DE EXCLUSÃO de objeto subsequente ou versões de EXCLUSÃO de objetos falhará se for antes da data de retenção ou se uma retenção legal estiver ativada.

Atualizar as definições do bloqueio de objetos do S3

Se você precisar atualizar as configurações de retenção legal ou retenção para uma versão de objeto existente, poderá executar as seguintes operações de subrecursos de objeto:

- `PUT Object legal-hold`

  Se o novo valor de retenção legal estiver ATIVADO, o objeto será colocado sob uma retenção legal. Se o valor de retenção legal estiver DESLIGADO, a retenção legal é levantada.

- `PUT Object retention`
  - O valor do modo deve ser CONFORMIDADE (sensível a maiúsculas e 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 de objeto tiver uma data retida-até-data existente, você só poderá aumentá-la. O novo valor deve estar no futuro.

Informações relacionadas

Gerenciar objetos com ILM

Use a conta de locatário

Objeto PUT

COLOCAR Objeto - Copiar

Inicie o carregamento de várias peças

Controle de versão de objetos

"Guia do usuário do Amazon Simple Storage Service: Usando o bloqueio de objeto S3"

Utilize S3 Select (Selecionar)

O StorageGRID oferece suporte às seguintes cláusulas, tipos de dados e operadores do AWS S3 Select para o SelectObjectContent - comando.

Os itens não listados não são suportados.

Para obter a sintaxe, Selecione ObjectContentconsulte . Para obter mais informações sobre S3 Select, consulte "Documentação da AWS para o S3 Select".

Apenas as contas de inquilino que tenham S3 Select ativado podem emitir consultas SelectObjectContent. Consulte Considerações e requisitos para usar o S3 Select.

Cláusulas

- Selecione a lista
- Da cláusula
- Cláusula where
- CLÁUSULA LIMIT (LIMITE)

Tipos de dados

- bool
- número inteiro
- cadeia de carateres
- flutuação
- decimal, numérico
- timestamp

Operadores

Operadores lógicos

- E
- NÃO
- OU

Operadores de comparação

* * * lt * gt * . * . * * ! * ENTRE * EM

Operadores de correspondência de padrões

- GOSTO
- _
- %

Operadores unitários

- É NULO
- NÃO É NULL

Operadores de matemática

- E
- -
- *
- /
- %

O StorageGRID segue a precedência do operador AWS S3 Select.

Agregar funções

- MÉDIA ()
- CONTAGEM (*)
- MÁX. ()
- MIN. ()
- SOMA()

Funções condicionais

- CASO
- COALESCE
- NULLIF

Funções de conversão

- CAST (para tipos de dados suportados)

Funções de data

- DATE_ADD
- DATE_DIFF
- EXTRAIR
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

Funções de cadeia de carateres

- CHAR_LENGTH, CHARACTER_LENGTH
- BAIXAR
- SUBSTRING
- APARAR
- SUPERIOR

Use a criptografia do lado do servidor

A criptografia do lado do servidor permite proteger os dados do 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, você pode escolher uma das duas opções mutuamente exclusivas, com base em como as chaves de criptografia são gerenciadas:

- **SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID)**: Quando você 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. Quando você recupera 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 seus dados de objeto serão retornados.

  Enquanto o StorageGRID gerencia todas as operações de criptografia e descriptografia de objetos, você deve gerenciar as chaves de criptografia fornecidas.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente.

> Se um objeto for criptografado com SSE ou SSE-C, quaisquer configurações de criptografia no nível de bucket ou no nível de grade serão ignoradas.

Use 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:

- Objeto PUT
- COLOCAR Objeto - Copiar
- Inicie o carregamento de várias peças

Use 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 da plataforma 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 256 bits, codificado em base64.
`x-amz-server-side-encryption-customer-key-MD5`	Especifique o resumo MD5 da chave de criptografia de acordo com a RFC 1321, que é usada para garantir que a chave de criptografia foi transmitida sem erros. O valor para o resumo MD5 deve ser base64-codificado 128-bit.

Os cabeçalhos de solicitação SSE-C são suportados pelas seguintes operações de objeto:

- Objeto GET
- Objeto HEAD
- Objeto PUT
- COLOCAR Objeto - Copiar
- Inicie o carregamento de várias peças
- Carregar artigo
- Carregar artigo - Copiar

Considerações sobre o uso de criptografia no lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Antes de usar SSE-C, esteja ciente das seguintes considerações:

- Você deve usar https.

> O StorageGRID rejeita quaisquer solicitações feitas por http ao usar SSE-C. para considerações de segurança, você deve considerar qualquer chave que você enviar acidentalmente usando http para ser comprometida. Elimine a chave e rode-a conforme adequado.

- O ETag na resposta não é o MD5 dos dados do objeto.
- É necessário 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 seu bucket estiver habilitado para versionamento, cada versão do objeto deve 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, você também deve gerenciar quaisquer proteções adicionais, como rotação de chaves, no lado do cliente.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente.

- Se a replicação do CloudMirror estiver configurada para o bucket, você não poderá ingerir objetos SSE-C. A operação de ingestão falhará.

Informações relacionadas

Objeto GET

Objeto HEAD

Objeto PUT

COLOCAR Objeto - Copiar

Inicie o carregamento de várias peças

Carregar artigo

Carregar artigo - Copiar

"Guia do desenvolvedor do Amazon S3: Protegendo dados usando criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)"

Objeto GET

Você pode usar a solicitação S3 GET Object para recuperar um objeto de um bucket do S3.

OBTER objetos e multipartes

Você pode usar o `partNumber` parâmetro Request para recuperar uma parte específica de um objeto multipart ou segmentado. O `x-amz-mp-parts-count` elemento de resposta indica quantas partes o objeto tem.

Você pode definir `partNumber` como 1 para objetos segmentados/multipartes e objetos não segmentados/não multipartes; no entanto, o `x-amz-mp-parts-count` elemento de resposta é retornado apenas para objetos segmentados ou multipartes.

Cabeçalhos de solicitação para criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use todos os três cabeçalhos se o objeto for criptografado com uma chave exclusiva que você forneceu.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do objeto.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

UTF-8 carateres em metadados do usuário

O StorageGRID não analisa nem interpreta carateres UTF-8 escapados em metadados definidos pelo usuário. Obter solicitações para um objeto com carateres UTF-8 escapados em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome ou valor da chave incluir carateres não imprimíveis.

Cabeçalho de pedido 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 busca a versão mais recente do objeto em um bucket com versão. 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`.

Comportamento DO GET Object para objetos Pool de storage de nuvem

Se um objeto tiver sido armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), o comportamento de uma SOLICITAÇÃO GET Object depende do estado do objeto. Consulte "Objeto PRINCIPAL" para obter mais detalhes.

> Se um objeto for armazenado em um pool de armazenamento em nuvem e uma ou mais cópias do objeto também existirem na grade, as SOLICITAÇÕES DE OBTENÇÃO de objetos tentarão recuperar dados da grade, antes de recuperá-los do pool de armazenamento em nuvem.

Estado do objeto	Comportamento de GET Object
Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento	`200 OK` Uma cópia do objeto é recuperada.

Estado do objeto	Comportamento de GET Object
Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável	`200 OK` Uma cópia do objeto é recuperada.
Objeto transicionado para um estado não recuperável	`403 Forbidden`, `InvalidObjectState` Use uma solicitação de restauração PÓS-objeto para restaurar o objeto para um estado recuperável.
Objeto em processo de restauração a partir de um estado não recuperável	`403 Forbidden`, `InvalidObjectState` Aguarde até que a solicitação de restauração PÓS-objeto seja concluída.
Objeto totalmente restaurado para o Cloud Storage Pool	`200 OK` Uma cópia do objeto é recuperada.

Objetos segmentados ou multiparte em um pool de armazenamento em nuvem

Se você carregou um objeto multipart ou se o StorageGRID dividir um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no pool de armazenamento em nuvem amostrando um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação GET Object pode retornar incorretamente `200 OK` quando algumas partes do objeto já tiverem sido transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não tiverem sido restauradas.

Nestes casos:

- A solicitação GET Object pode retornar alguns dados, mas parar no meio da transferência.
- Uma solicitação OBTER Objeto subsequente pode retornar `403 Forbidden`.

Informações relacionadas

Use a criptografia do lado do servidor

Gerenciar objetos com ILM

Restauração PÓS-objeto

S3 operações rastreadas em logs de auditoria

Objeto HEAD

Você pode usar a solicitação de Objeto S3 HEAD para recuperar metadados de um objeto sem retornar o próprio objeto. Se o objeto for armazenado em um pool de armazenamento em nuvem, você poderá usar Objeto HEAD para determinar o estado de transição do objeto.

Objeto PRINCIPAL e objetos multipart

Você pode usar o `partNumber` parâmetro Request para recuperar metadados de uma parte específica de um objeto multipart ou segmentado. O `x-amz-mp-parts-count` elemento de resposta indica quantas partes o objeto tem.

Você pode definir `partNumber` como 1 para objetos segmentados/multipartes e objetos não segmentados/não multipartes; no entanto, o `x-amz-mp-parts-count` elemento de resposta é retornado apenas para objetos segmentados ou multipartes.

Cabeçalhos de solicitação para criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use os três cabeçalhos se o objeto for criptografado com uma chave exclusiva que você forneceu.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do objeto.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

UTF-8 carateres em metadados do usuário

O StorageGRID não analisa nem interpreta carateres UTF-8 escapados em metadados definidos pelo usuário. As SOLICITAÇÕES HEAD para um objeto com carateres UTF-8 escapados em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome ou valor da chave incluir carateres não imprimíveis.

Cabeçalho de pedido não suportado

O seguinte cabeçalho de solicitação não é suportado e retorna `XNotImplemented`:

- `x-amz-website-redirect-location`

Cabeçalhos de resposta para objetos Pool de armazenamento em nuvem

Se o objeto for armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), os seguintes cabeçalhos de resposta serão retornados:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Os cabeçalhos de resposta fornecem informações sobre o estado de um objeto à medida que ele é movido para um pool de armazenamento em nuvem, opcionalmente transferido para um estado não recuperável e restaurado.

Estado do objeto	Resposta ao objeto PRINCIPAL
Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de storage tradicional ou usando codificação de apagamento	`200 OK` (Nenhum cabeçalho de resposta especial é retornado.)

Objeto no Cloud Storage Pool, mas ainda não transicionado 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` é definido para algum tempo distante no futuro. A hora exata da transição não é controlada pelo sistema StorageGRID.

O objeto fez a transição para o 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` é definido para algum tempo distante no futuro.
	
	Nota: Se a cópia na grade não estiver disponível (por exemplo, um nó de armazenamento está inativo), você deve emitir uma solicitação de restauração PÓS-Objeto para restaurar a cópia do pool de armazenamento em nuvem antes de recuperar o objeto com êxito.

Objeto transicionado para um estado não recuperável e nenhuma cópia existe na grade	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objeto em processo de restauração a partir de um estado não recuperável	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Estado do objeto	Resposta ao objeto PRINCIPAL

Objeto totalmente restaurado para o 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 pool de armazenamento em nuvem será retornado a um estado não recuperável.

Objetos segmentados ou multiparte no Cloud Storage Pool

Se você carregou um objeto multipart ou se o StorageGRID dividir um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no pool de armazenamento em nuvem amostrando um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação de objeto PRINCIPAL pode retornar incorretamente `x-amz-restore: ongoing-request="false"` quando algumas partes do objeto já tiverem sido transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não tiverem sido restauradas.

Controle de versão

Se um `versionId` sub-recurso não for especificado, a operação busca a versão mais recente do objeto em um bucket com versão. 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`.

Informações relacionadas

Use a criptografia do lado do servidor

Gerenciar objetos com ILM

Restauração PÓS-objeto

S3 operações rastreadas em logs de auditoria

Restauração PÓS-objeto

Você pode usar a solicitação de restauração PÓS-objeto S3 para restaurar um objeto armazenado em um pool de storage de nuvem.

Tipo de solicitação suportada

O StorageGRID suporta apenas solicitações de restauração PÓS-objeto para restaurar um objeto. Não suporta o `SELECT` tipo de restauração. Selecione Requests Return (retornar solicitações `XNotImplemented`).

Controle de versão

Opcionalmente, especifique `versionId` para restaurar uma versão específica de um objeto em um bucket com versão. Se você não especificar `versionId`, a versão mais recente do objeto será restaurada

Comportamento da restauração PÓS-objeto em objetos do Cloud Storage Pool

Se um objeto tiver sido armazenado em um pool de armazenamento em nuvem (consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações), uma solicitação de restauração PÓS-objeto terá o seguinte comportamento, com base no estado do objeto. Consulte "Objeto PRINCIPAL" para obter mais detalhes.

> Se um objeto for armazenado em um pool de armazenamento em nuvem e uma ou mais cópias do objeto também existirem na grade, não será necessário restaurar o objeto emitindo uma solicitação de restauração PÓS-objeto. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma SOLICITAÇÃO GET Object.

Estado do objeto	Comportamento da restauração PÓS-objeto
Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou objeto não está em um pool de storage de nuvem	`403 Forbidden`, `InvalidObjectState`
Objeto no Cloud Storage Pool, mas ainda não transicionado para um estado não recuperável	`200 OK` Nenhuma alteração é feita. **Nota**: Antes de um objeto ser transferido para um estado não recuperável, não é possível alterar o seu `expiry-date`.
Objeto transicionado para um estado não recuperável	`202 Accepted` Restaura uma cópia recuperável do objeto para o pool de armazenamento em nuvem pelo número de dias especificado no corpo da solicitação. No final desse período, o objeto é retornado a um estado não recuperável. Opcionalmente, use o `Tier` elemento de solicitação para determinar quanto tempo o trabalho de restauração levará para concluir (`Expedited`, `Standard` ou `Bulk`). Se você não especificar `Tier`, o `Standard` nível será usado. **Atenção**: Se um objeto tiver sido transferido para o S3 Glacier Deep Archive ou se o Cloud Storage Pool usar o armazenamento Blob do Azure, não será possível restaurá-lo usando o `Expedited` nível. O seguinte erro é retornado `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class`.
Objeto em processo de restauração a partir de um estado não recuperável	`409 Conflict`, `RestoreAlreadyInProgress`

Estado do objeto	Comportamento da restauração PÓS-objeto
Objeto totalmente restaurado para o Cloud Storage Pool	`200 OK` **Observação:** se um objeto foi restaurado para um estado recuperável, você pode alterar o mesmo `expiry-date` reemitindo a solicitação de restauração PÓS-objeto com um novo valor para `Days`. A data de restauração é atualizada em relação à hora da solicitação.

Informações relacionadas

Gerenciar objetos com ILM

Objeto HEAD

S3 operações rastreadas em logs de auditoria

Objeto PUT

Você pode usar a solicitação de objetos S3D PUT para adicionar um objeto a um bucket.

Resolver conflitos

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Tamanho do objeto

O tamanho máximo *recommended* para uma única operação PUT Object é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multipart.

> No StorageGRID 11,6, o tamanho máximo *suportado* para uma operação de objeto PUT único é de 5 TIB (5.497.558.138.880 bytes). No entanto, o alerta **S3 PUT Object Size too large** será acionado se você tentar fazer o upload de um objeto que exceda 5 GiB.

Tamanho dos metadados do usuário

O Amazon S3 limita o tamanho dos metadados definidos pelo usuário dentro de cada cabeçalho de SOLICITAÇÃO PUT para 2 KB. O StorageGRID limita os metadados do usuário a 24 KiB. O tamanho dos metadados definidos pelo usuário é medido tomando a soma do número de bytes na codificação UTF-8 de cada chave e valor.

UTF-8 carateres em metadados do usuário

Se uma solicitação incluir valores UTF-8 (não escapados) no nome da chave ou valor dos metadados definidos pelo usuário, o comportamento do StorageGRID é indefinido.

O StorageGRID não analisa nem interpreta carateres UTF-8 escapados incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Os carateres UTF-8 escapados são tratados como carateres

ASCII:

- As solicitações PUT, PUT Object-Copy, GET e HEAD são bem-sucedidas se os metadados definidos pelo usuário incluírem carateres UTF-8 escapados.
- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome ou valor da chave incluir carateres não imprimíveis.

Limites da etiqueta do objeto

Você pode adicionar tags a novos objetos ao enviá-los ou adicioná-los a objetos existentes. O StorageGRID e o Amazon S3 suportam até 10 tags para cada objeto. Tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 carateres Unicode de comprimento e os valores de tag podem ter até 256 carateres Unicode de comprimento. Chave e valores são sensíveis a maiúsculas e minúsculas.

Propriedade do objeto

No StorageGRID, todos os objetos são de propriedade da conta de 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 de bloco.
  - O StorageGRID não verifica o valor que você fornece `x-amz-decoded-content-length` em relação ao objeto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  A codificação de transferência Chunked é suportada se `aws-chunked` a assinatura de payload também for usada.

- `x-amz-meta-`, seguido por um par de 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 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 em segundos desde 1 de janeiro de 1970.

> Uma regra ILM não pode usar um **tempo de criação definido pelo usuário** para o tempo de referência e as opções balanceadas ou rigorosas para o comportamento de ingestão. Um erro é retornado quando a regra ILM é criada.

- `x-amz-tagging`
- S3 cabeçalhos de solicitação de bloqueio de objetos
  - `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 intervalo serão usadas para calcular a versão do objeto retida até a data.

  Use o bloqueio de objetos S3D.

- Cabeçalhos de pedido SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Consulte Cabeçalhos de solicitação para criptografia do lado do servidor

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- O `x-amz-acl` cabeçalho da solicitação não é suportado.
- O `x-amz-website-redirect-location` cabeçalho da solicitação não é suportado e retorna `XNotImplemented`.

Opções de classe de armazenamento

O `x-amz-storage-class` cabeçalho da solicitação é suportado. O valor enviado para `x-amz-storage-class` afeta a forma como o StorageGRID protege os dados de objetos durante a ingestão e não quantas cópias persistentes do objeto são armazenadas no sistema StorageGRID (que é determinado pelo ILM).

Se a regra ILM que corresponde a um objeto ingerido usar a opção estrita para comportamento de ingestão, o `x-amz-storage-class` cabeçalho não terá efeito.

Os seguintes valores podem ser usados para `x-amz-storage-class`:

- `STANDARD` (Predefinição)
  - * Commit duplo*: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, assim que um objeto é ingerido, uma segunda cópia desse objeto é criada e distribuída para um nó de armazenamento diferente (commit duplo). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais satisfazem as instruções de colocação na regra. Caso contrário, novas cópias de objetos podem precisar ser feitas em locais diferentes e as cópias provisórias iniciais podem precisar ser excluídas.
  - **Balanced**: Se a regra ILM especificar a opção Balanced e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em nós de storage diferentes.

    Se o StorageGRID puder criar imediatamente todas as cópias de objeto especificadas na regra ILM (colocação síncrona), `x-amz-storage-class` o cabeçalho não terá efeito.

- `REDUCED_REDUNDANCY`
  - **Commit duplo**: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, o StorageGRID cria uma única cópia provisória à medida que o objeto é ingerido (commit único).
  - **Balanced**: Se a regra ILM especificar a opção Balanced, 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. A `REDUCED_REDUNDANCY` opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso, o uso `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia de objeto extra para cada operação de ingestão.

  A utilização da `REDUCED_REDUNDANCY` opção não é recomendada noutras circunstâncias. `REDUCED_REDUNDANCY` aumenta o risco de perda de dados do objeto durante a ingestão. Por exemplo, você pode perder dados se a única cópia for inicialmente armazenada em um nó de armazenamento que falha antes que a avaliação ILM possa ocorrer.

Atenção: Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver 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.

Especificar `REDUCED_REDUNDANCY` apenas afeta quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Ele não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pela política ILM ativa e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

Nota: Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a

`REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a `REDUCED_REDUNDANCY` opção retornará um erro. A StorageGRID sempre realizará 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 cabeçalhos de solicitação a seguir para criptografar um objeto com criptografia do lado do servidor. As opções SSE e SSE-C são mutuamente exclusivas.

- **SSE**: Use o seguinte cabeçalho se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID.
  - `x-amz-server-side-encryption`
- **SSE-C**: Use todos os três cabeçalhos se você quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `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.

Atenção: as chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

Observação: se um objeto for criptografado com SSE ou SSE-C, qualquer configuração de criptografia no nível de bucket ou no nível de grade será ignorada.

Controle de versão

Se o controle de versão estiver habilitado para um bucket, um exclusivo `versionId` será gerado automaticamente para a versão do objeto que está sendo armazenado. Isso `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho de resposta.

Se o controle de versão estiver suspenso, a versão do objeto será armazenada com um nulo `versionId` e se já existir uma versão nula, ela será substituída.

Informações relacionadas

Gerenciar objetos com ILM

Operações em baldes

S3 operações rastreadas em logs de auditoria

Use a criptografia do lado do servidor

Como as conexões do cliente podem ser configuradas

COLOCAR Objeto - Copiar

Você pode usar a solicitação S3 PUT Object - Copy para criar uma cópia de um objeto que já está armazenado no S3. Uma operação PUT Object - Copy é a mesma que

executar um GET e depois um PUT.

Resolver conflitos

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Tamanho do objeto

O tamanho máximo *recommended* para uma única operação PUT Object é de 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multipart.

> No StorageGRID 11,6, o tamanho máximo *suportado* para uma operação de objeto PUT único é de 5 TIB (5.497.558.138.880 bytes). No entanto, o alerta **S3 PUT Object Size too large** será acionado se você tentar fazer o upload de um objeto que exceda 5 GiB.

UTF-8 carateres em metadados do usuário

Se uma solicitação incluir valores UTF-8 (não escapados) no nome da chave ou valor dos metadados definidos pelo usuário, o comportamento do StorageGRID é indefinido.

O StorageGRID não analisa nem interpreta carateres UTF-8 escapados incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Os carateres UTF-8 escapados são tratados como carateres ASCII:

- As solicitações são bem-sucedidas se os metadados definidos pelo usuário incluírem carateres UTF-8 escapados.
- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome ou valor da chave incluir carateres 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 de 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.

- S3 cabeçalhos de solicitação de bloqueio de objetos:

  - `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 intervalo serão usadas para calcular a versão do objeto retida até a data.

  Use o bloqueio de objetos S3D.

- Cabeçalhos de pedido SSE:

  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Consulte Cabeçalhos de solicitação para criptografia do lado do servidor

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-website-redirect-location`

Opções de classe de armazenamento

O `x-amz-storage-class` cabeçalho de solicitação é suportado e afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM correspondente especificar um comportamento de ingestão de confirmação dupla ou equilibrada.

- `STANDARD`

  (Padrão) especifica uma operação de ingestão de commit duplo quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

- `REDUCED_REDUNDANCY`

  Especifica uma operação de ingestão de commit único quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

  > Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a `REDUCED_REDUNDANCY` opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Usando x-amz-copy-source em PUT Object - Copy

Se o intervalo de origem e a chave, especificados no `x-amz-copy-source` cabeçalho, forem diferentes do intervalo de destino e da chave, uma cópia dos dados do objeto de origem será gravada no destino.

Se a origem e o destino corresponderem e o `x-amz-metadata-directive` cabeçalho for especificado como `REPLACE`, os metadados do objeto serão atualizados com os valores de metadados fornecidos na solicitação. Nesse caso, o StorageGRID não reingere o objeto. Isto tem duas consequências importantes:

- Não é possível usar COLOCAR Objeto - Copiar para criptografar um objeto existente no lugar ou para alterar a criptografia de um objeto existente no lugar. Se você fornecer o `x-amz-server-side-encryption` cabeçalho ou o `x-amz-server-side-encryption-customer-algorithm` cabeçalho, o StorageGRID rejeita a solicitação e retorna `XNotImplemented`.
- A opção de comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento de objetos que são acionadas pela atualização são feitas quando o ILM é reavaliado por processos normais de ILM em segundo plano.

  Isso significa que, se a regra ILM usar a opção estrita para o comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objeto necessários não puderem ser feitos (por exemplo, porque um local recém-exigido 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 no lado do servidor, os cabeçalhos de solicitação fornecidos 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 deve incluir os três cabeçalhos a seguir na solicitação PUT Object - Copy, para que o objeto possa ser descriptografado e copiado:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` `AES256` Especifique .
  - `x-amz-copy-source-server-side-encryption-customer-key` Especifique a chave de criptografia fornecida quando você 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`: Especificar `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.

Atenção: as chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva gerenciada pelo StorageGRID (SSE), inclua esse cabeçalho no pedido COLOCAR Objeto - Copiar:
  - `x-amz-server-side-encryption`

Nota: o `server-side-encryption` valor do objeto não pode ser atualizado. Em vez disso, faça uma cópia com um novo `server-side-encryption` valor usando `x-amz-metadata-directive`: `REPLACE`.

Controle de 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` subrecurso. Se o intervalo de destino for versionado, a versão gerada será retornada `x-amz-version-id` no cabeçalho de resposta. Se o controle de versão estiver suspenso para o bucket de destino, `x-amz-version-id` então retornará um valor "'null'".

Informações relacionadas

Gerenciar objetos com ILM

Use a criptografia do lado do servidor

S3 operações rastreadas em logs de auditoria

Objeto PUT

Selecione ObjectContent

Você pode usar a solicitação SelectObjectContent S3 para filtrar o conteúdo de um objeto S3 com base em uma instrução SQL simples.

Para obter mais informações, consulte "Documentação da AWS para SelectObjectContent" .

O que você vai precisar

- A conta de locatário tem a permissão S3 Select (Selecionar).
- Você tem `s3:GetObject` permissão para o objeto que deseja consultar.
- O objeto que você deseja consultar está em formato CSV ou é um arquivo compactado GZIP ou bzip2 contendo um arquivo formatado CSV.

- Sua expressão SQL tem um comprimento máximo de 256 KB.
- Qualquer Registro na entrada ou resultados tem um comprimento máximo de 1 MIB.

Exemplo de sintaxe de solicitação

```
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 consulta SQL

Esta consulta obtém o nome do estado, 2010 populações, 2015 populações estimadas e a porcentagem de mudança dos dados do censo americano. Os 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 serem consultadas, `SUB-EST2020_ALL.csv`, são 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 da AWS-CLI

```
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`, são assim:

```
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 de várias partes

Esta seção descreve como o StorageGRID suporta operações para uploads de várias partes.

As seguintes condições e notas aplicam-se a todas as operações de carregamento em várias partes:

- Você não deve exceder 1.000 uploads simultâneos de várias partes para um único bucket, porque os resultados das consultas de uploads de várias partes para esse bucket podem retornar resultados incompletos.
- O StorageGRID impõe limites de tamanho da AWS para peças multipeças. S3 os clientes devem seguir estas diretrizes:
  - Cada parte em um upload de várias partes deve estar 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 tão grandes quanto possível. Por exemplo, use tamanhos de peças de 5 GiB para um objeto de 100 GiB. Como cada peça é considerada um objeto exclusivo, o uso de tamanhos de peças grandes reduz a sobrecarga de metadados do StorageGRID.
  - Para objetos menores que 5 GiB, considere usar upload não multipart.
- O ILM é avaliado para cada parte de um objeto multipart à medida que é ingerido e para o objeto como um todo quando o upload multipart é concluído, se a regra ILM usa o comportamento de ingestão rigoroso ou equilibrado. Você deve estar ciente de como isso afeta o posicionamento do objeto e da peça:
  - Se o ILM mudar enquanto um upload multipart S3 estiver em andamento, quando o upload multipart concluir algumas partes do objeto talvez não atendam aos requisitos atuais do ILM. Qualquer peça que não seja colocada corretamente está na fila para reavaliação ILM e é movida para o local correto mais tarde.
  - 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 de ILM para o objeto como um todo. Por exemplo, se uma regra especifica que todos os objetos de 10 GB ou maior são armazenados em DC1 enquanto todos os objetos menores são armazenados em DC2, na ingestão cada parte de 1 GB de um upload multipart de 10 partes é armazenado em DC2. Quando ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.
- Todas as operações de upload em várias partes suportam controles de consistência do StorageGRID.
- Conforme necessário, você pode usar a criptografia do lado do servidor com uploads de várias partes. Para usar o SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID), você inclui o `x-amz-server-side-encryption` cabeçalho da solicitação somente na solicitação de upload de

múltiplas partes. Para usar SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente), você especifica os mesmos três cabeçalhos de solicitação de chave de criptografia na solicitação de carregamento de múltiplas partes Iniciar e em cada solicitação de peça de carregamento subsequente.

Operação	Implementação
Listar carregamentos Multipart	Consulte Listar carregamentos Multipart
Inicie o carregamento de várias peças	Consulte Inicie o carregamento de várias peças
Carregar artigo	Consulte Carregar artigo
Carregar artigo - Copiar	Consulte Carregar artigo - Copiar
Concluir carregamento Multipart	Consulte Concluir carregamento Multipart
Abortar carregamento Multipart	Implementado com todo o comportamento da API REST do Amazon S3
Listar peças	Implementado com todo o comportamento da API REST do Amazon S3

Informações relacionadas

- Controles de consistência
- Use a criptografia do lado do servidor

Listar carregamentos Multipart

A operação List Multipart uploads lista uploads em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

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

O `delimiter` parâmetro Request não é suportado.

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Quando a operação completa de Upload Multipart é executada, esse é o ponto em que os objetos são criados (e versionados, se aplicável).

Inicie o carregamento de várias peças

A operação Iniciar carregamento Multipart inicia um upload multipart para um objeto e retorna um ID de upload.

O `x-amz-storage-class` cabeçalho da solicitação é suportado. O valor enviado para `x-amz-storage-class` afeta a forma como o StorageGRID protege os dados de objetos durante a ingestão e não quantas cópias persistentes do objeto são armazenadas no sistema StorageGRID (que é determinado pelo ILM).

Se a regra ILM que corresponde a um objeto ingerido usar a opção estrita para comportamento de ingestão, o `x-amz-storage-class` cabeçalho não terá efeito.

Os seguintes valores podem ser usados para `x-amz-storage-class`:

- `STANDARD` (Predefinição)
  - * Commit duplo*: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, assim que um objeto é ingerido, uma segunda cópia desse objeto é criada e distribuída para um nó de armazenamento diferente (commit duplo). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais satisfazem as instruções de colocação na regra. Caso contrário, novas cópias de objetos podem precisar ser feitas em locais diferentes e as cópias provisórias iniciais podem precisar ser excluídas.
  - **Balanced**: Se a regra ILM especificar a opção Balanced e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em nós de storage diferentes.

    Se o StorageGRID puder criar imediatamente todas as cópias de objeto especificadas na regra ILM (colocação síncrona), `x-amz-storage-class` o cabeçalho não terá efeito.
- `REDUCED_REDUNDANCY`
  - **Commit duplo**: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, o StorageGRID cria uma única cópia provisória à medida que o objeto é ingerido (commit único).
  - **Balanced**: Se a regra ILM especificar a opção Balanced, 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. A `REDUCED_REDUNDANCY` opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso, o uso `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia de objeto extra para cada operação de ingestão.

  A utilização da `REDUCED_REDUNDANCY` opção não é recomendada noutras circunstâncias. `REDUCED_REDUNDANCY` aumenta o risco de perda de dados do objeto durante a ingestão. Por exemplo, você pode perder dados se a única cópia for inicialmente armazenada em um nó de armazenamento que falha antes que a avaliação ILM possa ocorrer.

Atenção: Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver 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.

Especificar `REDUCED_REDUNDANCY` apenas afeta quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Ele não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pela política ILM ativa e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema

StorageGRID.

Nota: Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a `REDUCED_REDUNDANCY` opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Type`
- `x-amz-meta-`, seguido por um par de 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 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 em segundos desde 1 de janeiro de 1970.

  > ⓘ A adição `creation-time` de metadados definidos pelo usuário não é permitida se você estiver adicionando um objeto a um bucket que tenha a conformidade legada habilitada. Um erro será retornado.

- S3 cabeçalhos de solicitação de bloqueio de objetos:
  - `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 intervalo serão usadas para calcular a versão do objeto retida até a data.

  Usando S3 Object Lock

- Cabeçalhos de pedido 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 carateres UTF-8, consulte a documentação do PUT Object.

Cabeçalhos de solicitação para criptografia do lado do servidor

Você pode usar os cabeçalhos de solicitação a seguir 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 de carregamento de múltiplas partes se você quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações de Upload Part.
  - `x-amz-server-side-encryption`
- **SSE-C**: Use todos esses três cabeçalhos na solicitação de Upload Multipart iniciada (e em cada solicitação de Upload Part subsequente) se você quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `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.

Atenção: as chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

Cabeçalhos de solicitação não suportados

O cabeçalho de solicitação a seguir não é suportado e retorna `XNotImplemented`

- `x-amz-website-redirect-location`

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação completa de Upload Multipart é executada.

Informações relacionadas

Gerenciar objetos com ILM

Use a criptografia do lado do servidor

Objeto PUT

Carregar artigo

A operação Upload Part carrega uma peça em um upload multipart para um objeto.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Length`
- `Content-MD5`

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação de carregamento de múltiplas peças iniciada, você também deve incluir os seguintes cabeçalhos de solicitação em cada solicitação de Upload de peça:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia fornecida na solicitação Iniciar carregamento Multipart.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação de Envio de Multipart Iniciar.

> As chaves de criptografia que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação completa de Upload Multipart é executada.

Informações relacionadas

Use a criptografia do lado do servidor

Carregar artigo - Copiar

A operação Upload Part - Copy carrega uma parte de um objeto copiando dados de um objeto existente como fonte de dados.

A operação Upload Part - Copy é implementada com todo o comportamento da API REST do Amazon S3.

Essa solicitação lê e grava os dados de objeto especificados no `x-amz-copy-source-range` 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 de carregamento de múltiplas partes, você também deve incluir os seguintes cabeçalhos de solicitação em cada peça de carregamento - solicitação de cópia:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia fornecida na solicitação Iniciar carregamento Multipart.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação de Envio de Multipart Iniciar.

Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deve incluir os três cabeçalhos a seguir na solicitação de Upload Part - Copy, para que o objeto possa ser descriptografado e copiado:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia fornecida quando você 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 que você fornece nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger os dados do objeto, revise as considerações em "usar criptografia do lado do servidor".

Controle de versão

O upload de várias partes consiste em operações separadas para iniciar o upload, listar uploads, carregar peças, montar as peças carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação completa de Upload Multipart é executada.

Concluir carregamento Multipart

A operação completa de Upload Multipart completa um upload multipart de um objeto, montando as peças carregadas anteriormente.

Resolver conflitos

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes S3 começam uma operação.

Cabeçalhos de solicitação

O `x-amz-storage-class` cabeçalho de solicitação é suportado e afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM correspondente especificar um comportamento de ingestão de confirmação dupla ou equilibrada.

- `STANDARD`

  (Padrão) especifica uma operação de ingestão de commit duplo quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

- `REDUCED_REDUNDANCY`

  Especifica uma operação de ingestão de commit único quando a regra ILM usa a opção de commit duplo ou quando a opção Balanced retorna à criação de cópias provisórias.

> Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock ativado, a `REDUCED_REDUNDANCY` opção será ignorada. Se você estiver ingerindo um objeto em um bucket compatível com legado, a `REDUCED_REDUNDANCY` opção retornará um erro. A StorageGRID sempre realizará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

> Se um upload multipart não for concluído dentro de 15 dias, a operação será marcada como inativa e todos os dados associados serão excluídos do sistema.

> O `ETag` valor retornado não é uma soma MD5 dos dados, mas segue a implementação da API do Amazon S3 do `ETag` valor para objetos multipart.

Controle de versão

Esta operação completa um upload de várias partes. Se o controle de versão estiver habilitado para um bucket, a versão do objeto será criada após a conclusão do upload de várias partes.

Se o controle de versão estiver habilitado para um bucket, um exclusivo `versionId` será gerado automaticamente para a versão do objeto que está sendo armazenado. Isso `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho de resposta.

Se o controle de versão estiver suspenso, a versão do objeto será armazenada com um nulo `versionId` e se já existir uma versão nula, ela será substituída.

> Quando o controle de versão está habilitado para um bucket, concluir um upload multipart sempre cria uma nova versão, mesmo que haja carregamentos simultâneos de várias partes concluídos na mesma chave de objeto. Quando o controle de versão não está habilitado para um bucket, é possível iniciar um upload multipart e, em seguida, ter outro upload multipart iniciado e concluído primeiro na mesma chave de objeto. Em buckets não versionados, o upload multipart que completa o último tem precedência.

Falha na replicação, notificação ou notificação de metadados

Se o intervalo onde ocorre o upload de várias partes estiver configurado para um serviço de plataforma, o upload de várias partes será bem-sucedido mesmo se a ação de replicação ou notificação associada falhar.

Se isso ocorrer, um alarme é gerado no Gerenciador de Grade em Eventos totais (SMTT). A mensagem último evento exibe "'Falha ao publicar notificações para chave de bucket-naameobject'" para o último objeto cuja notificação falhou. (Para ver esta mensagem, selecione **NÓS *Storage Node* Eventos**. Veja o último evento no topo da tabela.) As mensagens de evento também são listadas em `/var/local/log/bycast-err.log`.

Um locatário pode acionar a replicação ou notificação com falha atualizando os metadados ou as tags do objeto. Um locatário pode reenviar os valores existentes para evitar fazer alterações indesejadas.

Informações relacionadas

Gerenciar objetos com ILM

Respostas de erro

O sistema StorageGRID suporta todas as respostas de erro padrão da API REST S3 que se aplicam. Além disso, a implementação do StorageGRID adiciona várias respostas personalizadas.

Códigos de erro S3 API suportados

Nome	Status HTTP
AccessDenied	403 proibido
BadDigest	400 pedido incorreto
BucketAlreadyExists	409 conflito
BucketNotEmpty	409 conflito
IncompleteBody	400 pedido incorreto
InternalError (erro internacional)	500 erro interno do servidor
InvalidAccessKeyId	403 proibido
InvalidArgument	400 pedido incorreto
InvalidBucketName	400 pedido incorreto
InvalidBucketState	409 conflito
InvalidDigest	400 pedido incorreto
InvalidEncryptionAlgorithmError	400 pedido incorreto
InvalidPart	400 pedido incorreto
InvalidPartOrder	400 pedido incorreto
Intervalo Invalidável	416 intervalo solicitado não satisfatório
InvalidRequest	400 pedido incorreto

Nome	Status HTTP
InvalidStorageClass	400 pedido incorreto
InvalidTag	400 pedido incorreto
InvalidURI	400 pedido incorreto
KeyTooLong	400 pedido incorreto
MalformedXML	400 pedido incorreto
MetadataTooLarge	400 pedido incorreto
MetodNotAlloved	Método 405 não permitido
MissingContentLength	411 comprimento necessário
MissingRequestBodyError	400 pedido incorreto
MissingSecurityHeader	400 pedido incorreto
NoSuchBucket	404 não encontrado
NoSuchKey	404 não encontrado
NoSuchUpload	404 não encontrado
Sem Implementado	501 não implementado
NoSuchBucketPolicy	404 não encontrado
ObjectLockConfigurationNotFounError	404 não encontrado
Pré-condiçãoFailed	412 Pré-condição falhou
RequestTimeTooSwed	403 proibido
Serviço indisponível	503 Serviço indisponível
SignatureDoesNotMatch	403 proibido
TooManyBuckets	400 pedido incorreto
UserKeyMustBeSpecified	400 pedido incorreto

Códigos de erro personalizados do StorageGRID

Nome	Descrição	Status HTTP
XBucketLifecycleNotAllowed	A configuração do ciclo de vida do bucket não é permitida em um bucket compatível com legado	400 pedido incorreto
XBucketPolicyParseException	Falha ao analisar JSON da política de bucket recebida.	400 pedido incorreto
XComplianceConflict	Operação negada devido às configurações de conformidade legadas.	403 proibido
XComplianceReducedRedundancy Forbidden	Redundância reduzida não é permitida no bucket em conformidade com o legado	400 pedido incorreto
XMaxBucketPolicyLengthExceeded	Sua política excede o comprimento máximo permitido da política de intervalo.	400 pedido incorreto
XMissingInternalRequestHeader	Falta um cabeçalho de uma solicitação interna.	400 pedido incorreto
XNoSuchBucketCompliance	O bucket especificado não tem conformidade legada habilitada.	404 não encontrado
XNotAcceptable	A solicitação contém um ou mais cabeçalhos de aceitação que não puderam ser satisfeitos.	406 não aceitável
XNotImplementado	A solicitação que você forneceu implica funcionalidade que não é implementada.	501 não implementado

Operações da API REST do StorageGRID S3

Há operações adicionadas à API REST do S3 que são específicas do sistema StorageGRID.

- OBTER pedido de consistência de balde

  A solicitação GET Bucket Consistency permite determinar o nível de consistência que está sendo aplicado a um determinado bucket.

- COLOCAR pedido consistência balde

  A solicitação de consistência do PUT Bucket permite especificar o nível de consistência a ser aplicado às

operações realizadas em um bucket.

- OBTER último pedido de tempo de acesso do Bucket

  A solicitação de última hora de acesso do GET Bucket permite determinar se as atualizações da última hora de acesso estão ativadas ou desativadas para buckets individuais.

- COLOCAR o último pedido de tempo de acesso do balde

  A solicitação de última hora de acesso do PUT Bucket permite ativar ou desativar as atualizações da última hora de acesso para intervalos individuais. A desativação das atualizações da última hora de acesso melhora o desempenho e é a configuração padrão para todos os buckets criados com a versão 10,3.0 ou posterior.

- EXCLUIR solicitação de configuração de notificação de metadados do bucket

  A solicitação de configuração de notificação de metadados DELETE Bucket permite desativar o serviço de integração de pesquisa para buckets individuais excluindo o XML de configuração.

- OBTER solicitação de configuração de notificação de metadados do bucket

  A solicitação de configuração de notificação de metadados do GET Bucket permite recuperar o XML de configuração usado para configurar a integração de pesquisa para buckets individuais.

- COLOCAR solicitação de configuração de notificação de metadados do bucket

  A solicitação de configuração de notificação de metadados do PUT Bucket permite ativar o serviço de integração de pesquisa para buckets individuais. O XML de configuração de notificação de metadados que você fornece no corpo da solicitação especifica os objetos cujos metadados são enviados para o índice de pesquisa de destino.

- OBTER solicitação de uso de armazenamento

  A solicitação OBTER uso do armazenamento informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta.

- Pedidos de Bucket obsoletos para conformidade legada

  Talvez seja necessário usar a API REST do StorageGRID S3 para gerenciar buckets criados com o recurso de conformidade legado.

OBTER pedido de consistência de balde

A solicitação GET Bucket Consistency permite determinar o nível de consistência que está sendo aplicado a um determinado bucket.

Os controles de consistência padrão são definidos para garantir leitura após gravação para objetos recém-criados.

Você tem a permissão S3:GetBucketConsistency, ou seja raiz de conta, para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Resposta

No XML de resposta `<Consistency>`, retornará um dos seguintes valores:

Controle de consistência	Descrição
tudo	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.
forte local	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 eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Mais de perto corresponde às garantias de consistência do Amazon S3. **Observação:** se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, defina o controle de consistência como "disponível", a menos que você exija garantias de consistência semelhantes ao Amazon S3.
Disponível (eventual consistência para OPERAÇÕES DE CABEÇA)	Comporta-se da mesma forma que o nível de consistência "read-after-novo-write", mas apenas fornece consistência eventual para operações HEAD. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis. Difere das garantias de consistência do Amazon S3 apenas para operações PRINCIPAIS.

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

Controles de consistência

COLOCAR pedido consistência balde

A solicitação de consistência do PUT Bucket permite especificar o nível de consistência a ser aplicado às operações realizadas em um bucket.

Os controles de consistência padrão são definidos para garantir leitura após gravação para objetos recém-criados.

Você tem a permissão S3:PutBucketConsistency, ou seja raiz de conta, para concluir esta operação.

Pedido

O `x-ntap-sg-consistency` parâmetro deve conter um dos seguintes valores:

Controle de consistência	Descrição
tudo	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.
forte local	Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.

Controle de consistência	Descrição
leitura-após-nova-gravação	(Padrão) fornece consistência de leitura após gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Mais de perto corresponde às garantias de consistência do Amazon S3. **Observação:** se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, defina o controle de consistência como "disponível", a menos que você exija garantias de consistência semelhantes ao Amazon S3.
Disponível (eventual consistência para OPERAÇÕES DE CABEÇA)	Comporta-se da mesma forma que o nível de consistência "read-after-novo-write", mas apenas fornece consistência eventual para operações HEAD. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis. Difere das garantias de consistência do Amazon S3 apenas para operações PRINCIPAIS.

Nota: em geral, você deve usar o valor de controle de consistência "read-after-new-write". Se as solicitações não estiverem funcionando corretamente, altere o comportamento do cliente do aplicativo, se possível. Ou configure o cliente para especificar o controle de consistência para cada solicitação de API. Defina o controle de consistência no nível do balde apenas como último recurso.

Exemplo de solicitação

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Informações relacionadas

Controles de consistência

OBTER último pedido de tempo de acesso do Bucket

A solicitação de última hora de acesso do GET Bucket permite determinar se as atualizações da última hora de acesso estão ativadas ou desativadas para buckets individuais.

Você tem a permissão S3:GetBucketLastAccessTime, ou seja raiz da conta, para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Exemplo de resposta

Este exemplo mostra que as atualizações da última hora de acesso estão ativadas para o intervalo.

```
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>
```

COLOCAR o último pedido de tempo de acesso do balde

A solicitação de última hora de acesso do PUT Bucket permite ativar ou desativar as atualizações da última hora de acesso para intervalos individuais. A desativação das atualizações da última hora de acesso melhora o desempenho e é a configuração padrão para todos os buckets criados com a versão 10,3.0 ou posterior.

Você tem a permissão S3:PutBucketLastAccessTime para um bucket, ou ser raiz de conta, para concluir esta operação.

> ⓘ A partir da versão 10,3 do StorageGRID, as atualizações da última hora de acesso são desativadas por padrão para todos os novos buckets. Se você tiver buckets criados usando uma versão anterior do StorageGRID e quiser corresponder ao novo comportamento padrão, desative explicitamente as atualizações da última hora de acesso para cada um desses buckets anteriores. Você pode ativar ou desativar as atualizações para o último tempo de acesso usando a solicitação DE última hora de acesso do PUT Bucket, a caixa de seleção **S3 Buckets Change Last Access Setting** no Gerenciador de locatários ou na API de Gerenciamento do locatário.

Se as atualizações da última hora de acesso estiverem desativadas para um bucket, o seguinte comportamento é aplicado às operações no bucket:

- OBTER Objeto, OBTER ACL Objeto, OBTER marcação Objeto e solicitações Objeto HEAD não atualizam a última hora de acesso. O objeto não é adicionado às filas para avaliação do gerenciamento do ciclo de vida das informações (ILM).

- COLOCAR Objeto - Copiar e COLOCAR solicitações de marcação de objetos que atualizam apenas os metadados também atualizam a última hora de acesso. O objeto é adicionado às filas para avaliação ILM.
- Se as atualizações para o último tempo de acesso estiverem desativadas para o intervalo de origem, as solicitações COLOCAR Objeto - cópia não atualizam o último tempo de acesso para o intervalo de origem. O objeto que foi copiado não é adicionado às filas para avaliação ILM para o bucket de origem. No entanto, para o destino, COLOCAR Objeto - solicitações de cópia sempre atualizam o último tempo de acesso. A cópia do objeto é adicionada às filas para avaliação ILM.
- Concluir a atualização de pedidos de carregamento de várias peças da última vez de acesso. O objeto concluído é adicionado às filas para avaliação ILM.

Exemplos de pedidos

Este exemplo permite o último tempo de acesso para um bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Este exemplo desativa a última hora de acesso para um bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Informações relacionadas

Use a conta de locatário

EXCLUIR solicitação de configuração de notificação de metadados do bucket

A solicitação de configuração de notificação de metadados DELETE Bucket permite desativar o serviço de integração de pesquisa para buckets individuais excluindo o XML de configuração.

Você tem a permissão S3:DeleteBucketMetadataNotification para um bucket, ou ser raiz de 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

OBTER solicitação de configuração de notificação de metadados do bucket

A solicitação de configuração de notificação de metadados do GET Bucket permite recuperar o XML de configuração usado para configurar a integração de pesquisa para buckets individuais.

Você tem a permissão S3:GetBucketMetadataNotification, ou seja o root da conta, para concluir esta operação.

Exemplo de solicitação

Essa solicitação recupera a configuração de notificação de metadados para o bucket chamado `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Resposta

O corpo da resposta inclui a configuração de notificação de metadados para o bucket. A configuração de notificação de metadados permite determinar como o intervalo é configurado para integração de pesquisa. Ou seja, ele permite determinar quais objetos são indexados e 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 onde o StorageGRID deve enviar metadados de objeto. Os destinos devem ser especificados usando a URNA de um endpoint StorageGRID.

Nome	Descrição	Obrigatório
MetadataNotificationConfiguration	Tag de contentor para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos de regra.	Sim
Regra	Tag container para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
ID	Identificador exclusivo para a regra. Incluído no elemento regra.	Não
Estado	O estado pode ser "ativado" ou "Desativado". Nenhuma ação é tomada para regras que são desativadas. Incluído no elemento regra.	Sim
Prefixo	Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento regra.	Sim
Destino	Etiqueta de contentor para o destino de uma regra. Incluído no elemento regra.	Sim

Nome	Descrição	Obrigatório
Urna	URNA do destino onde os metadados do objeto são enviados. Deve ser a URNA de um endpoint StorageGRID com as seguintes propriedades: • `es` deve ser o terceiro elemento. • A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário `domain-name/myindex/mytype`. Os endpoints são configurados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário. Eles assumem a seguinte forma: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O endpoint deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. Urna está incluído no elemento destino.	Sim

Exemplo de resposta

O XML incluído entre as `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags mostra como a integração com um endpoint de integração de pesquisa é configurada para o bucket. Neste exemplo, metadados de objeto estão sendo enviados para um índice Elasticsearch nomeado `current` e tipo nomeado `2017` que está hospedado em um domínio da AWS `records` chamado .

```
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 a conta de locatário

COLOCAR solicitação de configuração de notificação de metadados do bucket

A solicitação de configuração de notificação de metadados do PUT Bucket permite ativar o serviço de integração de pesquisa para buckets individuais. O XML de configuração de notificação de metadados que você fornece no corpo da solicitação especifica os objetos cujos metadados são enviados para o índice de pesquisa de destino.

Você tem a permissão S3:PutBucketMetadataNotification para um bucket, ou ser raiz de conta, para concluir esta operação.

Pedido

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 ao qual o StorageGRID deve enviar metadados de objetos.

Os objetos podem ser filtrados no prefixo do nome do objeto. Por exemplo, você pode enviar metadados para objetos com o prefixo `/images` para um destino e objetos com o prefixo `/videos` para outro.

As configurações que têm prefixos sobrepostos não são válidas e são rejeitadas quando são enviadas. Por exemplo, uma configuração que incluía uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não seria permitida.

Os destinos devem ser especificados usando a URNA de um endpoint StorageGRID. O endpoint deve existir quando a configuração de notificação de metadados é enviada ou a solicitação falha como um `400 Bad`

`Request`. a mensagem de erro afirma: `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
MetadataNotificationConfiguration	Tag de contentor para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos de regra.	Sim
Regra	Tag container para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
ID	Identificador exclusivo para a regra. Incluído no elemento regra.	Não

Nome	Descrição	Obrigatório
Estado	O estado pode ser "ativado" ou "Desativado". Nenhuma ação é tomada para regras que são desativadas. Incluído no elemento regra.	Sim
Prefixo	Os objetos que correspondem ao prefixo são afetados pela regra e seus metadados são enviados para o destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento regra.	Sim
Destino	Etiqueta de contentor para o destino de uma regra. Incluído no elemento regra.	Sim

Nome	Descrição	Obrigatório
Urna	URNA do destino onde os metadados do objeto são enviados. Deve ser a URNA de um endpoint StorageGRID com as seguintes propriedades: • `es` deve ser o terceiro elemento. • A URNA deve terminar com o índice e digitar onde os metadados são armazenados, no formulário `domain-name/myindex/mytype`. Os endpoints são configurados usando o Gerenciador do Locatário ou a API de Gerenciamento do Locatário. Eles assumem a seguinte forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` O endpoint deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. Urna está incluído no elemento destino.	Sim

Exemplos de pedidos

Este exemplo mostra a ativação da integração de pesquisa para um bucket. Neste exemplo, metadados de objetos para todos os objetos são enviados para o mesmo destino.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

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

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

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

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

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

Metadados de objetos incluídos nas notificações de metadados

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

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

Tipo	Nome do item	Descrição
Informações sobre o balde e o objeto	balde	Nome do balde
Informações sobre o balde e o objeto	chave	Nome da chave do objeto
Informações sobre o balde e o objeto	ID de versão	Versão do objeto, para objetos em buckets versionados
Informações sobre o balde e o objeto	região	Região do balde, por exemplo `us-east-1`
Metadados do sistema	tamanho	Tamanho do objeto (em bytes) como visível para um cliente HTTP
Metadados do sistema	md5	Hash de objeto
Metadados do usuário	metadados *`key:value`*	Todos os metadados de usuário para o objeto, como pares de chave-valor

Tipo	Nome do item	Descrição
Tags	tags *key:value*	Todas as tags de objeto definidas para o objeto, como pares chave-valor

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

Informações relacionadas

Use a conta de locatário

OBTER solicitação de uso de armazenamento

A solicitação OBTER uso do armazenamento 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 uma solicitação GET Service modificada com o `x-ntap-sg-usage` parâmetro de consulta. O uso do armazenamento de buckets é rastreado separadamente das SOLICITAÇÕES DE 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, especialmente 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 tem a permissão S3:ListAllMyBuckets, ou seja raiz de conta, para concluir esta operação.

Exemplo de solicitação

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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 de objeto armazenada contribuirá para os `ObjectCount` valores e `DataBytes` na resposta. Excluir marcadores não são adicionados ao `ObjectCount` total.

Informações relacionadas

Controles de consistência

Solicitações de bucket obsoletas para conformidade legada

Talvez seja necessário usar a API REST do StorageGRID S3 para gerenciar buckets criados com o recurso de conformidade legado.

Funcionalidade de conformidade obsoleta

O recurso de conformidade do StorageGRID que estava disponível nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3.

Se você ativou anteriormente a configuração de conformidade global, a configuração de bloqueio de objeto global S3 será ativada no StorageGRID 11,6. Você não pode mais criar novos buckets com a conformidade

ativada. No entanto, conforme necessário, você pode usar a API REST do StorageGRID S3 para gerenciar buckets em conformidade existentes.

- Use o bloqueio de objetos S3D.
- Gerenciar objetos com ILM
- "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

Solicitações de conformidade obsoletas:

- Obsoleto - COLOCAR modificações de solicitação de balde para conformidade

  O elemento SGCompliance XML está obsoleto. Anteriormente, você poderia incluir esse elemento personalizado do StorageGRID no corpo opcional da solicitação XML de SOLICITAÇÕES PUT Bucket para criar um bucket compatível.

- Obsoleto - OBTER solicitação de conformidade de bucket

  A solicitação de conformidade GET Bucket está obsoleta. No entanto, você pode continuar usando essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket em conformidade legado existente.

- Obsoleto - COLOCAR solicitação de conformidade de balde

  A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar usando essa solicitação para modificar as configurações de conformidade de um bucket em conformidade com o legado existente. Por exemplo, você pode colocar um bucket existente em retenção legal ou aumentar seu período de retenção.

Obsoleto: Modificações de solicitação de Bucket para conformidade

O elemento SGCompliance XML está obsoleto. Anteriormente, você poderia incluir esse elemento personalizado do StorageGRID no corpo opcional da solicitação XML de SOLICITAÇÕES PUT Bucket para criar um bucket compatível.

> O recurso de conformidade do StorageGRID que estava disponível nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3.

Use o bloqueio de objetos S3D.

Gerenciar objetos com ILM

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

Você não pode mais criar novos buckets com a conformidade ativada. A seguinte mensagem de erro é retornada se você tentar usar as modificações de solicitação DE armazenamento 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.
```

Informações relacionadas

Gerenciar objetos com ILM

Use a conta de locatário

Obsoleto: OBTER solicitação de conformidade do bucket

A solicitação de conformidade GET Bucket está obsoleta. No entanto, você pode continuar usando essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket em conformidade legado existente.

> O recurso de conformidade do StorageGRID que estava disponível nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3.

Use o bloqueio de objetos S3D.

Gerenciar objetos com ILM

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

Você tem a permissão S3:GetBucketCompliance, ou seja raiz da conta, para concluir esta operação.

Exemplo de solicitação

Esta solicitação de exemplo permite que você determine as configurações de conformidade para o bucket chamado `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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 de um intervalo no qual cada objeto será retido por um ano (525.600 minutos), a partir de quando o objeto é ingerido na grade. Atualmente, não existe qualquer retenção legal neste intervalo. Cada objeto será automaticamente excluído após um ano.

```
HTTP/1.1 200 OK
Date: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrição
Repetição de PeriodMinutes	A duração do período de retenção para objetos adicionados a este intervalo, em minutos. O período de retenção começa quando o objeto é ingerido na grade.
LegalHod	• Verdadeiro: Este balde está atualmente sob uma guarda legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja levantada, mesmo que seu período de retenção tenha expirado. • Falso: Este balde não está atualmente sob um guarda legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Autodelete	• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob uma retenção legal. • Falso: Os objetos neste intervalo 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 intervalo 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`.

Informações relacionadas

Gerenciar objetos com ILM

Use a conta de locatário

Obsoleto: COLOQUE a solicitação de conformidade do bucket

A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar usando essa solicitação para modificar as configurações de conformidade de um bucket em conformidade com o 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 nas versões anteriores do StorageGRID está obsoleto e foi substituído pelo bloqueio de objetos do S3.

Use o bloqueio de objetos S3D.

Gerenciar objetos com ILM

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

Você tem a permissão S3:PutBucketCompliance, ou seja raiz de conta, para concluir esta operação.

Você deve especificar um valor para cada campo das configurações de conformidade ao emitir uma solicitação de conformidade PUT Bucket.

Exemplo de solicitação

Esta solicitação de exemplo modifica as configurações de conformidade para o bucket `mybucket` chamado . Neste exemplo, os objetos em `mybucket` agora serão retidos por dois anos (1.051.200 minutos) em vez de um ano, a partir de quando o objeto é ingerido na grade. Não há retenção legal neste balde. Cada objeto será automaticamente excluído após dois anos.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrição
Repetição de PeriodMinutes	A duração do período de retenção para objetos adicionados a este intervalo, em minutos. O período de retenção começa quando o objeto é ingerido na grade. **Atenção:** ao especificar um novo valor para RetentionPeriodMinutes, você deve especificar um valor igual ou maior que o período de retenção atual do bucket. Após o período de retenção do balde ser definido, não é possível diminuir esse valor; só é possível aumentá-lo.
LegalHod	• Verdadeiro: Este balde está atualmente sob uma guarda legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja levantada, mesmo que seu período de retenção tenha expirado. • Falso: Este balde não está atualmente sob um guarda legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Autodelete	• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob uma retenção legal. • Falso: Os objetos neste intervalo não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Nível de consistência para configurações de conformidade

Quando você atualiza as configurações de conformidade de um bucket do S3 com uma solicitação de conformidade de ARMAZENAMENTO, o StorageGRID tenta atualizar os metadados do bucket na grade. Por padrão, o StorageGRID usa o nível de consistência **strong-global** para garantir que todos os sites de data center e todos os nós de storage que contêm metadados de bucket tenham consistência de leitura após gravação para as configurações de conformidade alteradas.

Se o StorageGRID não conseguir atingir o nível de 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 grade para garantir que os serviços de armazenamento necessários sejam disponibilizados o mais rápido possível. Se o administrador da grade não conseguir disponibilizar o suficiente dos nós de armazenamento em cada local, o suporte técnico pode direcioná-lo a tentar novamente a solicitação com falha forçando o nível de consistência **strong-site**.

Nunca force o nível de consistência **strong-site** para a conformidade com o bucket, a menos que você tenha sido direcionado a fazê-lo por suporte técnico e a menos que você entenda as possíveis consequências de usar esse nível.

Quando o nível de consistência é reduzido para **strong-site**, o StorageGRID garante que as configurações de conformidade atualizadas terão consistência de leitura após gravação apenas para solicitações de clientes dentro de um site. Isso significa que o sistema StorageGRID pode ter temporariamente várias configurações inconsistentes para esse intervalo até que todos os sites e nós de storage estejam disponíveis. As definições inconsistentes podem resultar num comportamento inesperado e indesejado. Por exemplo, se você estiver colocando um bucket sob uma retenção legal e forçar um nível de consistência inferior, as configurações de conformidade anteriores do bucket (ou seja, retenção legal) podem continuar em vigor em alguns sites de data center. Como resultado, os objetos que você acha que estão em retenção legal podem ser excluídos quando seu período de retenção expirar, seja pelo usuário ou pela exclusão automática, se ativado.

Para forçar o uso do nível de consistência **strong-site**, reemita a solicitação de conformidade PUT Bucket e inclua o `Consistency-Control` cabeçalho de solicitação HTTP, da seguinte forma:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Respostas de erro

- Se o intervalo não foi criado para ser compatível, o código de status HTTP para a resposta é `404 Not Found`.
- Se `RetentionPeriodMinutes` na solicitação for inferior ao período de retenção atual do bucket, o código de status HTTP será `400 Bad Request`.

Informações relacionadas

Obsoleto: Modificações de solicitação de Bucket para conformidade

Use a conta de locatário

Gerenciar objetos com ILM

Políticas de acesso ao bucket e ao grupo

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 nesses buckets. O sistema StorageGRID implementa um subconjunto da linguagem de política da API REST S3. As políticas de acesso para a API S3 são escritas em JSON.

Visão geral da política de acesso

Existem dois tipos de políticas de acesso suportadas pelo StorageGRID.

- **Políticas de bucket**, que são configuradas usando a política OBTER bucket, COLOCAR bucket e EXCLUIR Bucket policy S3 operações de API. As políticas de bucket são anexadas a buckets, portanto, são configuradas para controlar o acesso dos usuários na conta de proprietário do bucket ou 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 Gerenciador do locatário ou a API de gerenciamento do locatário. As políticas de grupo são anexadas a um grupo na conta, portanto 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 vários buckets.

As políticas de grupo e bucket do StorageGRID seguem uma gramática específica definida pela Amazon. Dentro de cada política há uma matriz de declarações de política, e cada declaração contém os seguintes elementos:

- ID de declaração (Sid) (opcional)
- Efeito
- Principal/NotPrincipal
- Recurso/não recurso
- Ação/não Ação
- Condição (opcional)

As instruções de política são construídas usando esta estrutura para especificar permissões: Conceder efeito para permitir/negar que o principal execute Ação em recurso quando a condição se aplica.

Cada elemento de política é usado para uma função específica:

Elemento	Descrição
SID	O elemento Sid é opcional. O Sid é apenas uma descrição para o usuário. Ele é armazenado, mas não interpretado pelo sistema StorageGRID.
Efeito	Use o elemento efeito para determinar se as operações especificadas são permitidas ou negadas. É necessário identificar operações que você permite (ou nega) em buckets ou objetos usando as palavras-chave do elemento Ação suportado.
Principal/NotPrincipal	Você pode permitir que usuários, grupos e contas acessem recursos específicos e executem ações específicas. Se nenhuma assinatura S3 estiver incluída na solicitação, o acesso anônimo será permitido especificando o caractere curinga (*) como principal. Por padrão, somente a raiz 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/não recurso	O elemento recurso identifica buckets e objetos. Você pode permitir ou negar permissões a buckets e objetos usando o Nome do recurso da Amazon (ARN) para identificar o recurso.

Elemento	Descrição
Ação/não Ação	Os elementos Ação e efeito são os dois componentes das permissões. Quando um grupo solicita um recurso, é concedido ou negado o acesso ao recurso. O acesso é negado a menos que você atribua permissões especificamente, mas você pode usar Negar explícito para substituir uma permissão concedida por outra política.
Condição	O elemento de condição 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 carateres curinga (**) e (?). Enquanto o asterisco (**) corresponde a 0 ou mais carateres, o ponto de interrogação (?) corresponde a qualquer caractere único.

No elemento principal, carateres curinga não são suportados, exceto para definir acesso anônimo, o que concede permissão a todos. Por exemplo, você define o caractere curinga (*) como o valor principal.

```
"Principal":"*"
```

No exemplo a seguir, a instrução está usando os elementos efeito, Principal, Ação e recurso. Este exemplo mostra uma declaração de política de bucket completa que usa o efeito "permitir" para dar aos Principals, ao grupo admin `federated-group/admin` e ao grupo financeiro `federated-group/finance` , permissões para executar a Ação `s3:ListBucket` no bucket nomeado e a Ação `s3:GetObject` em todos os objetos dentro desse bucket `mybucket`.

```
{
  "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:iam:s3:::mybucket",
        "arn:aws:iam: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.

Informações relacionadas

Use a conta de locatário

Configurações de controle de consistência para políticas

Por padrão, quaisquer atualizações feitas para políticas de grupo são eventualmente consistentes. Uma vez que uma política de grupo se torna consistente, as alterações podem levar mais 15 minutos para entrar em vigor, devido ao armazenamento em cache de políticas. Por padrão, todas as atualizações feitas às políticas de bucket também são, eventualmente, 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 se torne efetiva o mais rápido possível por razões de segurança.

Nesse caso, você pode definir o `Consistency-Control` cabeçalho na solicitação de política COLOCAR balde ou usar a solicitação DE consistência COLOCAR balde. Ao alterar o controle de consistência para essa solicitação, você deve usar o valor **All**, que fornece a maior garantia de consistência de leitura após gravação. Se você especificar qualquer outro valor de controle de consistência em um cabeçalho para a solicitação DE consistência de armazenamento PUT, a solicitação será rejeitada. Se você especificar qualquer outro valor para uma solicitação DE política PUT Bucket, o valor será ignorado. Depois que uma política de bucket se tornar consistente, as alterações podem levar mais 8 segundos para entrar em vigor, devido ao armazenamento em cache de políticas.

Se você definir o nível de consistência como **All** para forçar uma nova política de bucket a entrar em vigor mais cedo, certifique-se de definir o controle de nível de bucket de volta ao valor original quando terminar. Caso contrário, todas as futuras solicitações de bucket usarão a configuração **All**.

Use ARN em declarações de política

Em declarações de política, o ARN é usado em elementos Principal e recursos.

- Use esta sintaxe para especificar o ARN de recursos 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 carateres dentro da chave de objeto.
- Carateres internacionais, que podem ser especificados na chave do objeto, devem ser codificados usando JSON UTF-8 ou usando sequências de escape JSON. A codificação percentual não é suportada.

  "RFC 2141 sintaxe de URNA"

  O corpo de solicitação HTTP para a operação de política PUT Bucket deve ser codificado com charset UTF-8.

Especifique recursos em uma política

Em declarações de política, você pode usar o elemento recurso para especificar o intervalo 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 recursos S3. Por exemplo:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Você também pode usar variáveis de política dentro da chave de objeto. Por exemplo:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- O valor do recurso pode especificar um intervalo que ainda não existe quando uma política de grupo é criada.

Informações relacionadas

Especifique variáveis em uma política

Especifique princípios em uma política

Use o elemento principal para identificar a conta de usuário, grupo ou locatário que é permitido/negado acesso ao recurso pela declaração de política.

- Cada declaração de política em uma política de bucket deve incluir um elemento principal. As 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 princípios são denotados pelo elemento "principal" ou, alternativamente, "NotPrincipal" para exclusão.
- As identidades baseadas em contas devem ser especificadas usando um ID ou um ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- Este exemplo usa o ID de 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 usuário UUID em vez do nome de usuário:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Por exemplo, suponha que Alex deixe a organização e o nome de usuário `Alex` seja excluído. Se um novo Alex se juntar à organização e receber o mesmo `Alex` nome de usuário, o novo usuário poderá involuntariamente herdar as permissões concedidas ao usuário original.

- O valor principal pode especificar um nome de grupo/usuário que ainda não existe quando uma política de bucket é criada.

Especifique permissões em uma política

Em uma política, o elemento Ação é usado para permitir/negar permissões a um recurso. Há um conjunto de permissões que você pode especificar em uma política, que são denotadas pelo elemento "Ação" ou, alternativamente, "NotAction" para exclusão. Cada um desses elementos mapeia para operações específicas da API REST do S3.

As tabelas lista 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 de replicação PUT e DELETE Bucket. O StorageGRID usa permissões separadas para cada ação, que corresponde à especificação original do Amazon S3.

> Uma EXCLUSÃO é executada quando uma PUT é usada para substituir um valor existente.

Permissões que se aplicam a buckets

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:CreateBucket	COLOQUE o balde	
S3:DeleteBucket	ELIMINAR balde	
S3:DeleteBucketMetadataNotification	ELIMINAR configuração de notificação de metadados do bucket	Sim
S3:DeleteBucketPolicy	ELIMINAR política de balde	
S3:DeleteReplicationConfiguration	ELIMINAR replicação de balde	Sim, permissões separadas para COLOCAR e EXCLUIR*

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:GetBucketAcl	OBTER ACL balde	
S3:GetBucketCompliance	OBTER conformidade com balde (obsoleto)	Sim
S3:GetBucketConsistência	OBTER consistência de balde	Sim
S3:GetBucketCORS	OBTER Bucket Cors	
S3:GetEncryptionConfiguration	OBTER criptografia Bucket	
S3:GetBucketLastAccessTime	OBTER último tempo de acesso do Bucket	Sim
S3:GetBucketLocation	OBTER localização do balde	
S3:GetBucketMetadataNotification	OBTER configuração de notificação de metadados do bucket	Sim
S3:GetBucketNotification	OBTER notificação Bucket	
S3:GetBucketObjectLockConfiguration	OBTER Configuração bloqueio Objeto	
S3:GetBucketPolicy	OBTER política Bucket	
S3:GetBucketTagging	OBTER marcação Bucket	
S3:GetBucketControle de versão	OBTENHA o controle de versão do Bucket	
S3:GetLifecycleConfiguration	OBTENHA o ciclo de vida do Bucket	
S3:GetReplicationConfiguration	OBTER replicação do bucket	
S3:ListAllMyBuckets	• Serviço GET • OBTER uso de armazenamento	Sim, para OBTER uso de armazenamento
S3: ListBucket	• OBTER balde (Listar objetos) • Balde DA cabeça • Restauração PÓS-objeto	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:ListBucketMultipartUploads	• Listar carregamentos Multipart • Restauração PÓS-objeto	
S3:ListBucketVersions	OBTER versões Bucket	
S3:PutBucketCompliance	COLOCAR conformidade com balde (obsoleto)	Sim
S3:PutBucketConsistência	COLOQUE a consistência do balde	Sim
S3:PutBucketCORS	• ELIMINAR Cors Bucket† • COLOQUE cors de balde	
S3:PutEncryptionConfiguration	• ELIMINAR encriptação Bucket • COLOQUE a criptografia Bucket	
S3:PutBucketLastAccessTime	COLOQUE o último tempo de acesso do balde	Sim
S3:PutBucketMetadataNotification	COLOQUE a configuração de notificação de metadados do bucket	Sim
S3:PutBucketNotification	COLOCAR notificação de balde	
S3:PutBucketObjectLockConfiguration	• COLOCAR balde com o `x-amz-bucket-object-lock-enabled: true` cabeçalho de pedido (também requer a permissão S3:CreateBucket) • COLOCAR Configuração bloqueio Objeto	
S3:PutBucketPolicy	Política COLOCAR balde	
S3:PutBucketTagging	• ELIMINAR marcação de intervalo† • COLOQUE a marcação de balde	
S3:PutBucketControle de versão	COLOQUE o controle de versão do Bucket	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:PutLifecycleConfiguration	• ELIMINAR ciclo de vida do balde† • COLOQUE o ciclo de vida do balde	
S3:PutReplicationConfiguration	COLOQUE a replicação do balde	Sim, permissões separadas para COLOCAR e EXCLUIR*

Permissões que se aplicam a objetos

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:AbortMultipartUpload	• Abortar carregamento Multipart • Restauração PÓS-objeto	
S3:DeleteObject	• Objeto DELETE • Excluir vários objetos • Restauração PÓS-objeto	
S3:DeleteObjectTagging	ELIMINAR marcação Objeto	
S3:DeleteObjectVersionTagging	EXCLUIR marcação de objetos (uma versão específica do objeto)	
S3:DeleteObjectVersion	DELETE Object (uma versão específica do objeto)	
S3:GetObject	• Objeto GET • Objeto HEAD • Restauração PÓS-objeto • SELECIONE conteúdo do objeto	
S3:GetObjectAcl	OBTER ACL Objeto	
S3:GetObjectLegalHod	OBTER retenção legal Objeto	
S3:GetObjectRetention	OBTER retenção de objetos	
S3:GetObjectTagging	OBTER marcação Objeto	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:GetObjectVersionTagging	OBTER marcação de objetos (uma versão específica do objeto)	
S3:GetObjectVersion	OBTER Objeto (uma versão específica do objeto)	
S3:ListMultipartUploadParts	Listar Artigos, PÓS-restauração de objetos	
S3:PutObject	• Objeto PUT • COLOCAR Objeto - Copiar • Restauração PÓS-objeto • Inicie o carregamento de várias peças • Concluir carregamento Multipart • Carregar artigo • Carregar artigo - Copiar	
S3:PutObjectLegalHod	COLOCAR guarda legal Objeto	
S3:retenção de objetos Put	COLOCAR retenção Objeto	
S3:PutObjectTagging	Colocar marcação Objeto	
S3:PutObjectVersionTagging	COLOCAR marcação de objetos (uma versão específica do objeto)	
S3:PutOverwriteObject	• Objeto PUT • COLOCAR Objeto - Copiar • COLOQUE a marcação Objeto • ELIMINAR marcação Objeto • Concluir carregamento Multipart	Sim
S3:RestoreObject	Restauração PÓS-objeto	

Use a permissão PutOverwriteObject

A permissão S3:PutOverwriteObject é uma permissão StorageGRID personalizada 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 objeto S3.

As configurações possíveis para essa permissão incluem:

- **Allow**: O cliente pode substituir um objeto. Esta é a configuração padrão.
- **Deny**: O cliente não pode substituir um objeto. Quando definida como Negar, a permissão PutOverwriteObject funciona da seguinte forma:
  - Se um objeto existente for encontrado no mesmo caminho:
    - Os dados do objeto, metadados definidos pelo usuário ou marcação de objeto S3 não podem ser sobrescritos.
    - Todas as operações de ingestão em andamento são canceladas e um erro é retornado.
    - Se o controle de versão do S3 estiver ativado, a configuração Negar impede que as operações de marcação DE objetos PUT ou DELETE modifiquem o TagSet para um objeto e suas versões não atuais.
  - Se um objeto existente não for encontrado, essa permissão não terá efeito.
- Quando esta permissão não está presente, o efeito é o mesmo que se permitir foi definido.

> Se a política S3 atual permitir a substituição e a permissão PutOverwriteObject estiver definida como Negar, o cliente não poderá substituir os dados de um objeto, metadados definidos pelo usuário ou marcação de objeto. Além disso, se a caixa de seleção **Prevent Client Modification** estiver selecionada (**CONFIGURATION System Grid options**), essa configuração substituirá a configuração da permissão PutOverwriteObject.

Informações relacionadas

S3 exemplos de políticas de grupo

Especifique condições em uma política

As condições definem quando uma política estará em vigor. As condições consistem em operadores e pares de valor-chave.

Condições Use pares chave-valor para avaliação. Um elemento de condição pode conter várias condições, e cada condição pode conter vários pares de 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:

- Cadeia de carateres
- Numérico
- Booleano
- Endereço IP
- Verificação nula

Operadores de condição	Descrição
StringEquals	Compara uma chave com um valor de string baseado na correspondência exata (sensível a maiúsculas e minúsculas).
StringNotEquals	Compara uma chave com um valor de string baseado em correspondência negada (sensível a maiúsculas e minúsculas).
StringEquaisIgnoreCase	Compara uma chave com um valor de string baseado na correspondência exata (ignora caso).
StringNotEquaisIgnoreCase	Compara uma chave com um valor de string baseado em correspondência negada (ignora caso).
StringLike	Compara uma chave com um valor de string baseado na correspondência exata (sensível a maiúsculas e minúsculas). Pode incluir * e ? carateres curinga.
StringNotLike	Compara uma chave com um valor de string baseado em correspondência negada (sensível a maiúsculas e minúsculas). Pode incluir * e ? carateres curinga.
NumericEquals	Compara uma chave com um valor numérico baseado na correspondência exata.
NumericNotEquals	Compara uma chave com um valor numérico baseado em correspondência negada.
NumericGreaterThan	Compara uma chave com um valor numérico baseado na correspondência "'maior que".
NumericGreaterThanEquals	Compara uma chave com um valor numérico com base na correspondência "'maior que ou igual'".
NumericLessThan	Compara uma chave com um valor numérico baseado na correspondência "'menos que'".

Operadores de condição	Descrição
NumericLessThanEquals	Compara uma chave com um valor numérico baseado na correspondência "'menor que ou igual".
Bool	Compara uma chave com um valor booleano baseado na correspondência "'true or false".
Endereço IP	Compara uma chave com um endereço IP ou intervalo de endereços IP.
NotIpAddress	Compara uma chave com um endereço IP ou um intervalo de endereços IP com base na correspondência negada.
Nulo	Verifica se uma chave de condição está presente no contexto de solicitação atual.

Teclas de condição suportadas

Categoria	Chaves de condição aplicáveis	Descrição
Operadores IP	AWS:SourceIp	Irá comparar com o endereço IP a partir do qual a solicitação foi enviada. Pode ser usado para operações de balde ou objetos. **Observação:** se a solicitação S3 tiver sido enviada pelo serviço Load Balancer nos nós Admin e Gateways, isso será comparado ao endereço IP upstream do serviço Load Balancer. **Nota**: Se um balanceador de carga não transparente de terceiros for usado, isso será comparado ao endereço IP desse balanceador de carga. Qualquer `X-Forwarded-For` cabeçalho será ignorado, uma vez que sua validade não pode ser determinada.
Recurso/identidade	aws:nome de usuário	Irá comparar com o nome de usuário do remetente a partir do qual a solicitação foi enviada. Pode ser usado para operações de balde ou objetos.

Categoria	Chaves de condição aplicáveis	Descrição
S3: ListBucket e. S3:ListBucketVersions Permissions	s3:delimitador	Irá comparar com o parâmetro delimitador especificado em uma solicitação OBTER bucket ou OBTER versões de Objeto bucket.
S3: ListBucket e. S3:ListBucketVersions Permissions	s3: teclas de max	Irá comparar-se com o parâmetro Max-keys especificado em uma solicitação GET Bucket ou GET Bucket Object Versions.
S3: ListBucket e. S3:ListBucketVersions Permissions	s3:prefixo	Irá comparar com o parâmetro de prefixo especificado em uma solicitação GET Bucket ou GET Bucket Object Versions.
S3:PutObject	s3: object-lock-resting-retension-days	Compara com a data de retenção até especificada no `x-amz-object-lock-retain-until-date` cabeçalho da solicitação ou calculada a partir do período de retenção padrão do intervalo para garantir que esses valores estejam dentro do intervalo permitido para as seguintes solicitações: • Objeto PUT • COLOCAR Objeto - Copiar • Inicie o carregamento de várias peças
S3:retenção de objetos Put	s3: object-lock-resting-retension-days	Compara com a data de retenção até especificada na solicitação DE retenção de objetos PUT para garantir que ela esteja dentro do intervalo permitido.

Especifique variáveis em uma política

Você pode usar variáveis em políticas para preencher informações de política quando elas estiverem disponíveis. Você pode usar variáveis de política no `Resource` elemento e em comparações de string 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 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.
`${s3:prefix}`	Usa a chave de prefixo específica do serviço como a variável fornecida.
`${s3:max-keys}`	Usa a chave de teclas de Max específicas do serviço como a variável fornecida.
`${*}`	Caráter especial. Usa o caractere como um caractere * literal.
`${?}`	Caráter especial. Usa o caractere como um caractere literal ?.
`${$}`	Caráter especial. Usa o caractere como um caractere literal.

Crie políticas que exijam tratamento especial

Às vezes, uma diretiva pode conceder permissões que são perigosas para a segurança ou perigosas para operações contínuas, como bloquear o usuário raiz 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 de StorageGRID
Negar a si mesmo quaisquer permissões para a conta raiz	Balde	Válida e aplicada, mas a conta de usuário root mantém permissão para todas as operações de política de bucket do S3	O mesmo

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento de StorageGRID
Negar auto quaisquer permissões ao usuário/grupo	Grupo	Válido e aplicado	O mesmo
Permita a um grupo de conta estrangeiro qualquer permissão	Balde	Principal inválido	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido quando permitido por uma política
Permitir uma conta estrangeira root ou usuário qualquer permissão	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido quando permitido por uma política	O mesmo
Permitir permissões a todos para todas as ações	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido para a raiz da conta estrangeira e usuários	O mesmo
Negar permissões a todos para todas as ações	Balde	Válida e aplicada, mas a conta de usuário root mantém permissão para todas as operações de política de bucket do S3	O mesmo
Principal é um usuário ou grupo inexistente	Balde	Principal inválido	Válido
Recurso é um bucket S3 inexistente	Grupo	Válido	O mesmo
Principal é um grupo local	Balde	Principal inválido	Válido

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento de StorageGRID
A política concede a uma conta que não seja proprietária (incluindo contas anônimas) permissões para COLOCAR objetos	Balde	Válido. Os objetos são propriedade da conta de criador e a política de bucket não se aplica. A conta de criador deve conceder permissões de acesso ao objeto usando ACLs de objeto.	Válido. Os objetos são propriedade da conta de proprietário do bucket. Aplica-se a política de bucket.

Proteção WORM (write-once-read-many)

Você pode criar buckets do WORM (write-once-read-many) para proteger dados, metadados de objetos definidos pelo usuário e marcação de objetos do S3. Você configura os buckets WORM para permitir a criação de novos objetos e impedir substituições ou exclusões de conteúdo existente. Use uma das abordagens descritas aqui.

Para garantir que as substituições sejam sempre negadas, você pode:

- No Gerenciador de Grade, vá para **CONFIGURATION System Grid options** e marque a caixa de seleção **Prevent Client Modification**.
- Aplique as seguintes regras e políticas do S3:
  - Adicione uma operação PutOverwriteObject NEGAR à política S3.
  - Adicione uma operação DeleteObject NEGAR à política S3.
  - Adicione uma OPERAÇÃO PUT Object ALLOW à política S3.

> A configuração DeleteObject para NEGAR em uma política S3 não impede que o ILM exclua objetos quando uma regra como "'zero cópias após 30 dias'" existir.

> Mesmo quando todas essas regras e políticas são aplicadas, elas não protegem contra gravações simultâneas (ver situação A). Eles protegem contra substituições concluídas sequenciais (ver situação B).

Situação A: Gravações simultâneas (não protegidas contra)

```
/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

Gerenciar objetos com ILM

Crie políticas que exijam tratamento especial

Como as regras do StorageGRID ILM gerenciam objetos

S3 exemplos de políticas de grupo

S3 exemplos de políticas

Use os exemplos nesta seção para criar políticas de acesso ao StorageGRID para buckets e grupos.

S3 exemplos de política de bucket

As políticas de bucket especificam as permissões de acesso para o bucket ao qual a diretiva está anexada. As políticas de bucket são configuradas usando a API S3 PutBucketPolicy.

Uma política de bucket pode ser configurada usando a AWS CLI de acordo com o seguinte comando:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Exemplo: Permita que todos acessem somente leitura a um bucket

Neste exemplo, todos, incluindo anônimos, podem listar objetos no bucket e executar operações Get Object em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que essa política pode não ser particularmente útil, já que ninguém, exceto a raiz da conta, tem permissões para gravar no bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Exemplo: Permita que todos em uma conta tenham acesso total, e todos em outra conta tenham acesso somente leitura a um intervalo

Neste exemplo, todos em uma conta especificada têm acesso total a um bucket, enquanto todos em outra conta especificada só podem listar o bucket e executar operações GetObject em objetos no bucket começando com o `shared/` prefixo da chave do objeto.

No StorageGRID, os objetos criados por uma conta não proprietária (incluindo contas anônimas) são de propriedade da conta de proprietário do bucket. A política de bucket aplica-se 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: Permita que todos acessem somente leitura a um bucket e o acesso total por grupo especificado

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar operações GET Object em todos os objetos no bucket, enquanto somente usuários pertencentes ao grupo `Marketing` na

conta especificada têm acesso total permitido.

```
{
  "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: Permita que todos leiam e gravem o acesso a um bucket se o cliente estiver no intervalo 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 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` bucket e seus objetos. Todos os outros usuários, incluindo "root", são explicitamente negados todas as operações. Note no entanto que "root" nunca é negada permissão para colocar/obter/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` efeito para PutOverwriteObject e DeleteObject garante que ninguém pode substituir ou excluir os dados do objeto, metadados definidos pelo usuário e marcação de objetos 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/*"
    }
  ]
}
```

Informações relacionadas

Operações em baldes

S3 exemplos de políticas de grupo

As políticas de grupo especificam as permissões de acesso para o grupo ao qual a diretiva está anexada. Não `Principal` há nenhum elemento na política, uma vez que está implícita. As políticas de grupo são configuradas usando o Gerenciador de inquilinos ou a API.

Exemplo: Defina a política de grupo usando o Gerenciador do locatário

Ao usar o Gerenciador do Locatário para adicionar ou editar um grupo, você pode selecionar como deseja criar a política de grupo que define quais permissões de acesso S3 membros deste grupo terão, da seguinte forma:

- **No S3 Access**: Opção padrão. Os usuários deste grupo não têm acesso a recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar essa opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
- **Acesso somente leitura**: Os usuários deste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo somente leitura aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
- **Acesso total**: Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo de acesso total aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
- **Custom**: Os usuários do grupo recebem as permissões que você especificar na caixa de texto.

  Neste exemplo, os membros do grupo só podem listar e acessar sua pasta específica (prefixo de chave) no intervalo especificado.

Exemplo: Permitir o acesso total do grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm acesso total a todos os buckets pertencentes à conta de locatário, a menos que explicitamente negado pela política de bucket.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemplo: Permitir acesso somente leitura de grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm acesso somente leitura a recursos do S3, a menos que explicitamente negado pela política de bucket. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemplo: Permita que os membros do grupo tenham acesso total apenas à sua pasta em um intervalo

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

```
{
  "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}/*"
    }
  ]
}
```

Informações relacionadas

Use a conta de locatário

Configurar a segurança para API REST

Você deve analisar as medidas de segurança implementadas para a API REST e entender como proteger seu sistema.

Como o StorageGRID fornece segurança para API REST

Você deve entender como o sistema StorageGRID implementa segurança, autenticação e autorização para a API REST.

O StorageGRID usa as seguintes medidas de segurança.

- As comunicações do cliente com o serviço Load Balancer usam HTTPS se o HTTPS estiver configurado para o ponto de extremidade do balanceador de carga.

  Quando você configura um ponto de extremidade do balanceador de carga, o HTTP pode ser habilitado opcionalmente. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

- Por padrão, o StorageGRID usa HTTPS para comunicações de clientes com nós de armazenamento e o serviço CLB em nós de gateway.

  O HTTP pode, opcionalmente, ser habilitado para essas conexões. Por exemplo, você pode querer usar

HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

> O serviço CLB está obsoleto.

- As comunicações entre o StorageGRID e o cliente são criptografadas usando TLS.
- As comunicações entre o serviço Load Balancer e os nós de armazenamento dentro da grade são criptografadas se o ponto de extremidade do balanceador de carga está configurado para aceitar conexões HTTP ou HTTPS.
- Os clientes devem fornecer cabeçalhos de autenticação HTTP ao StorageGRID para executar operações de API REST.

Certificados de segurança e aplicativos de cliente

Os clientes podem se conetar ao serviço Load Balancer em nós de gateway ou nós de administrador, diretamente aos nós de storage ou ao serviço CLB em nós de gateway.

Em todos os casos, os aplicativos clientes podem fazer conexões TLS usando um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado gerado pelo sistema StorageGRID:

- Quando os aplicativos cliente se conetam ao serviço do Load Balancer, eles fazem isso usando o certificado que foi configurado para o ponto de extremidade do balanceador de carga específico usado para fazer a conexão. Cada endpoint tem seu próprio certificado, que é um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado que o administrador da grade gerou no StorageGRID ao configurar o endpoint.
- Quando os aplicativos cliente se conetam diretamente a um nó de armazenamento ou ao serviço CLB nos nós de gateway, eles usam os certificados de servidor gerados pelo sistema que foram gerados para nós de armazenamento quando o sistema StorageGRID foi instalado (que são assinados pela autoridade de certificação do sistema) ou um único certificado de servidor personalizado fornecido para a grade por um administrador de grade.

Os clientes devem ser configurados para confiar na autoridade de certificação que assinou qualquer certificado que usam para estabelecer conexões TLS.

Consulte as instruções de administração do StorageGRID para obter informações sobre a configuração de pontos de extremidade do balanceador de carga e para obter instruções sobre como adicionar um único certificado de servidor personalizado para conexões TLS diretamente aos nós de armazenamento ou ao serviço CLB nos nós de gateway.

Resumo

A tabela a seguir mostra como os problemas de segurança são implementados nas APIs REST S3 e Swift:

Problema de segurança	Implementação da API REST
Segurança da ligação	TLS
Autenticação do servidor	Certificado de servidor X,509 assinado pela CA do sistema ou certificado de servidor personalizado fornecido pelo administrador

Problema de segurança	Implementação da API REST
Autenticação de cliente	• S3: Conta S3 (ID da chave de acesso e chave de acesso secreta) • Swift: Conta Swift (nome de usuário e senha)
Autorização do cliente	• S3: Propriedade do bucket e todas as políticas de controle de acesso aplicáveis • Swift: Acesso à função de administrador

Informações relacionadas

Administrar o StorageGRID

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID suporta um conjunto limitado de conjuntos de codificação que os aplicativos clientes podem usar ao estabelecer uma sessão de Segurança da camada de Transporte (TLS).

Versões suportadas do TLS

O StorageGRID é compatível com TLS 1,2 e TLS 1,3.

SSLv3 e TLS 1,1 (ou versões anteriores) não são mais compatíveis.

Suítes de cifra suportadas

Versão TLS	IANA nome do conjunto de cifra
1,2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1,2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
1,2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1,3	TLS_AES_256_GCM_SHA384
1,3	TLS_CHACHA20_POLY1305_SHA256
1,3	TLS_AES_128_GCM_SHA256

Conjuntos de codificação obsoletos

Os seguintes conjuntos de codificação são obsoletos. O suporte para essas cifras será removido em uma versão futura.

Nome IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Informações relacionadas

Como as conexões do cliente podem ser configuradas

Monitorar e auditar operações

Você pode monitorar workloads e eficiências das operações do cliente visualizando tendências de transações para toda a grade ou para nós específicos. Você pode usar mensagens de auditoria para monitorar operações e transações do cliente.

Monitorar taxas de ingestão e recuperação de objetos

Você pode monitorar taxas de ingestão e recuperação de objetos, bem como métricas para contagens de objetos, consultas e verificação. Você pode exibir o número de tentativas bem-sucedidas e com falha por aplicativos clientes para ler, gravar e modificar objetos no sistema StorageGRID.

Passos

1. Faça login no Gerenciador de Grade usando um navegador da web suportado.
2. No painel de instrumentos, localize a secção Protocol Operations (operações de protocolo).

   Esta seção resume o número de operações do cliente realizadas pelo seu sistema StorageGRID. As taxas de protocolo são médias nos últimos dois minutos.

3. Selecione **NODES**.
4. Na página inicial dos nós (nível de implantação), clique na guia **Load Balancer**.

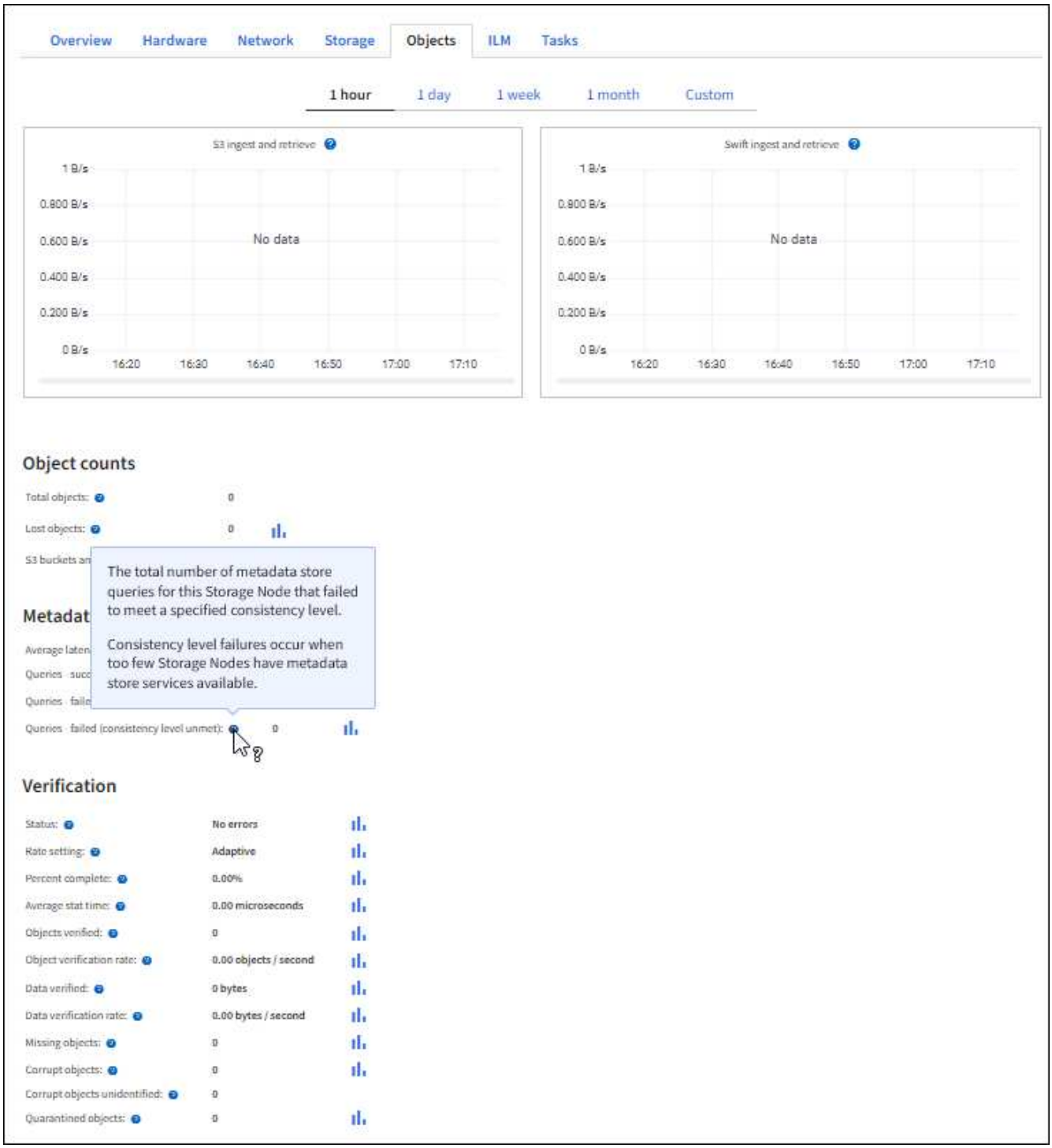
   Os gráficos mostram tendências para todo o tráfego do cliente direcionado para pontos de extremidade do balanceador de carga dentro da grade. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

5. Na home page dos nós (nível de implantação), clique na guia **objetos**.

   O gráfico mostra as taxas de ingestão e recuperação de todo o seu sistema StorageGRID em bytes por segundo e total de bytes. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

6. Para ver as informações de um nó de armazenamento específico, selecione o nó na lista à esquerda e clique na guia **Objects**.

   O gráfico mostra as taxas de ingestão e recuperação de objetos para este nó de armazenamento. A guia também inclui métricas para contagens de objetos, consultas e verificação. Você pode clicar nos rótulos para ver as definições dessas métricas.



7. Se você quiser ainda mais detalhes:
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   b. Selecione ***site* Visão geral Principal**.

      A seção operações da API exibe informações resumidas para toda a grade.

   c. Selecione ***Storage Node* LDR *client Application* Overview Main**

      A seção operações exibe informações resumidas para o nó de armazenamento selecionado.

Acesse e revise logs de auditoria

As mensagens de auditoria são geradas pelos serviços do StorageGRID e armazenadas em arquivos de log de texto. As mensagens de auditoria específicas da API nos logs de auditoria fornecem dados críticos de monitoramento de segurança, operação e desempenho que podem ajudá-lo a avaliar a integridade do sistema.

O que você vai precisar

- Você tem permissões de acesso específicas.
- Você tem o `Passwords.txt` arquivo.
- Você conhece o endereço IP de um nó Admin.

Sobre esta tarefa

O arquivo de log de auditoria ativo é `audit.log` chamado , e é armazenado em nós de administração.

Uma vez por dia, o arquivo audit.log ativo é salvo e um novo `audit.log` arquivo é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato *`yyyy-mm-dd.txt`*.

Após um dia, o arquivo salvo é compactado e renomeado, no formato *`yyyy-mm-dd.txt.gz`*, que preserva a data original.

Este exemplo mostra o `audit.log` ficheiro ativo, o ficheiro do dia anterior (`2018-04-15.txt`) e o ficheiro comprimido para o dia anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Vá para o diretório que contém os arquivos de log de auditoria:

   ```
   cd /var/local/audit/export
   ```

3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.

S3 operações rastreadas nos logs de auditoria

Várias operações de bucket e operações de objetos são rastreadas nos logs de auditoria do StorageGRID.

Operações de bucket rastreadas nos logs de auditoria

- ELIMINAR balde
- ELIMINAR marcação de intervalo
- Excluir vários objetos
- OBTER balde (Listar objetos)
- OBTER versões Objeto balde
- OBTER marcação Bucket
- Balde DA cabeça
- COLOQUE o balde
- COLOQUE a conformidade do balde
- COLOQUE a marcação de balde
- COLOQUE o controle de versão do Bucket

Operações de objeto rastreadas nos logs de auditoria

- Concluir carregamento Multipart
- Carregar artigo (quando a regra ILM usa os comportamentos de ingestão rigorosos ou equilibrados)
- Carregar artigo - Copiar (quando a regra ILM usa os comportamentos de ingestão estritos ou equilibrados)
- Objeto DELETE
- Objeto GET
- Objeto HEAD
- Restauração PÓS-objeto
- Objeto PUT
- COLOCAR Objeto - Copiar

Informações relacionadas

Operações em baldes

Operações em objetos

Benefícios de conexões HTTP ativas, ociosas e simultâneas

Como configurar conexões HTTP pode afetar o desempenho do sistema StorageGRID. As configurações diferem dependendo se a conexão HTTP está ativa ou inativa ou se você tem várias conexões simultâneas.

Você pode identificar os benefícios de desempenho para os seguintes tipos de conexões HTTP:

- Conexões HTTP ociosas
- Conexões HTTP ativas
- Conexões HTTP simultâneas

Benefícios de manter conexões HTTP ociosas abertas

Você deve manter as conexões HTTP abertas mesmo quando os aplicativos cliente estiverem ociosos para permitir que os aplicativos cliente executem transações subsequentes pela conexão aberta. Com base nas medições do sistema e na experiência de integração, você deve manter uma conexão HTTP inativa aberta por um máximo de 10 minutos. O StorageGRID pode fechar automaticamente uma conexão HTTP que é mantida aberta e inativa por mais de 10 minutos.

Conexões HTTP abertas e ociosas fornecem os seguintes benefícios:

- Latência reduzida desde o tempo em que o sistema StorageGRID determina que ele tem que executar uma transação HTTP para o tempo em que o sistema StorageGRID pode executar a transação

  A latência reduzida é a principal vantagem, especialmente pelo tempo necessário para estabelecer conexões TCP/IP e TLS.

- Aumento da taxa de transferência de dados por priming do algoritmo de início lento TCP/IP com transferências realizadas anteriormente
- Notificação instantânea de várias classes de condições de falha que interrompem a conetividade entre o aplicativo cliente e o sistema StorageGRID

Determinar por quanto tempo manter uma conexão inativa aberta é uma troca entre os benefícios do início lento que está associado à conexão existente e à alocação ideal da conexão com os recursos internos do sistema.

Benefícios de conexões HTTP ativas

Para conexões diretamente aos nós de armazenamento ou ao serviço CLB (obsoleto) em nós de Gateway, você deve limitar a duração de uma conexão HTTP ativa a um máximo de 10 minutos, mesmo que a conexão HTTP realize transações continuamente.

Determinar a duração máxima em que uma conexão deve ser mantida aberta é um trade-off entre os benefícios da persistência da conexão e a alocação ideal da conexão aos recursos internos do sistema.

Para conexões de cliente a nós de armazenamento ou ao serviço CLB, limitar conexões HTTP ativas fornece os seguintes benefícios:

- Permite o balanceamento de carga ideal em todo o sistema StorageGRID.

  Ao usar o serviço CLB, você deve evitar conexões TCP/IP de longa duração para otimizar o balanceamento de carga em todo o sistema StorageGRID. Você deve configurar aplicativos cliente para controlar a duração de cada conexão HTTP e fechar a conexão HTTP após um tempo definido para que a conexão HTTP possa ser restabelecida e reequilibrada.

  O serviço CLB equilibra a carga em todo o sistema StorageGRID no momento em que um aplicativo cliente estabelece uma conexão HTTP. Ao longo do tempo, uma conexão HTTP pode não ser mais ótima, pois os requisitos de balanceamento de carga mudam. O sistema executa seu melhor balanceamento de carga quando os aplicativos clientes estabelecem uma conexão HTTP separada para cada transação, mas isso nega os ganhos muito mais valiosos associados às conexões persistentes.

  > O serviço CLB está obsoleto.

- Permite que aplicativos cliente direcionem transações HTTP para serviços LDR que têm espaço disponível.
- Permite iniciar os procedimentos de manutenção.

  Alguns procedimentos de manutenção começam somente depois que todas as conexões HTTP em andamento estiverem concluídas.

Para conexões de clientes ao serviço Load Balancer, limitar a duração das conexões abertas pode ser útil para permitir que alguns procedimentos de manutenção sejam iniciados prontamente. Se a duração das conexões do cliente não for limitada, pode levar vários minutos para que as conexões ativas sejam automaticamente encerradas.

Benefícios de conexões HTTP simultâneas

Você deve manter várias conexões TCP/IP ao sistema StorageGRID abertas para permitir paralelismo, o que aumenta o desempenho. O número ideal de conexões paralelas depende de uma variedade de fatores.

As conexões HTTP simultâneas oferecem os seguintes benefícios:

- Latência reduzida

  As transações podem começar imediatamente em vez de esperar que outras transações sejam concluídas.

- Maior taxa de transferência

  O sistema StorageGRID pode executar transações paralelas e aumentar a taxa de transferência de transações agregadas.

Os aplicativos clientes devem estabelecer várias conexões HTTP. Quando um aplicativo cliente tem que executar uma transação, ele pode selecionar e usar imediatamente qualquer conexão estabelecida que não esteja processando uma transação no momento.

A topologia de cada sistema StorageGRID tem um throughput de pico diferente para transações e conexões simultâneas antes que o desempenho comece a degradar. A taxa de transferência de pico depende de fatores como recursos de computação, recursos de rede, recursos de armazenamento e links WAN. O número de servidores e serviços e o número de aplicativos suportados pelo sistema StorageGRID também são fatores.

Os sistemas StorageGRID geralmente suportam vários aplicativos clientes. Você deve ter isso em mente quando determinar o número máximo de conexões simultâneas usadas por um aplicativo cliente. Se o aplicativo cliente consistir em várias entidades de software que estabelecem conexões com o sistema StorageGRID, você deve adicionar todas as conexões entre as entidades. Talvez seja necessário ajustar o número máximo de conexões simultâneas nas seguintes situações:

- A topologia do sistema StorageGRID afeta o número máximo de transações simultâneas e conexões que o sistema pode suportar.
- Os aplicativos clientes que interagem com o sistema StorageGRID em uma rede com largura de banda limitada podem ter que reduzir o grau de simultaneidade para garantir que as transações individuais sejam concluídas em um tempo razoável.
- Quando muitos aplicativos clientes compartilham o sistema StorageGRID, você pode ter que reduzir o grau de simultaneidade para evitar exceder os limites do sistema.

Separação de pools de conexão HTTP para operações de leitura e gravação

Você pode usar pools separados de conexões HTTP para operações de leitura e gravação e controlar quanto de um pool usar para cada um. Pools separados de conexões HTTP permitem que você controle melhor as transações e equilibre as cargas.

Os aplicativos clientes podem criar cargas que são retrieve-dominant (read) ou store-dominant (write). Com pools separados de conexões HTTP para transações de leitura e gravação, você pode ajustar quanto de cada pool a dedicar para transações de leitura ou gravação.

Use Swift

Use Swift: Visão geral

Os aplicativos clientes podem usar a API OpenStack Swift para fazer interface com o sistema StorageGRID.

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

Item	Versão
Especificação Swift	API de storage de objetos OpenStack Swift v1 em novembro de 2015
HTTP	1,1 para obter mais informações sobre HTTP, consulte HTTP/1,1 (RFCs 7230-35). **Nota**: O StorageGRID não suporta a canalização HTTP/1,1.

Informações relacionadas

"OpenStack: API de storage de objetos"

Histórico do suporte à API Swift no StorageGRID

Você deve estar ciente das alterações no suporte do sistema StorageGRID para a API REST Swift.

Solte	Comentários
11,6	Pequenas alterações editoriais.
11,5	Removido o controle de consistência fraca. O nível de consistência disponível será usado em vez disso.
11,4	Adicionado suporte para TLS 1,3 e lista atualizada de pacotes de criptografia TLS suportados. O CLB está obsoleto. Adicionada descrição da inter-relação entre ILM e a configuração de consistência.

Solte	Comentários
11,3	Operações PUT Object atualizadas para descrever o impactos das regras de ILM que usam o posicionamento síncrono na ingestão (as opções equilibradas e rigorosas para o comportamento de ingestão). Adicionada descrição das conexões de cliente que usam pontos de extremidade do balanceador de carga ou grupos de alta disponibilidade. Lista atualizada dos conjuntos de encriptação TLS suportados. As cifras TLS 1,1 não são mais suportadas.
11,2	Pequenas alterações editoriais ao documento.
11,1	Adicionado suporte para o uso de HTTP para conexões de cliente Swift para nós de grade. Atualizadas as definições dos controles de consistência.
11,0	Adicionado suporte para 1.000 contentores para cada conta de locatário.
10,3	Atualizações administrativas e correções do documento. Seções removidas para configurar certificados de servidor personalizados.
10,2	Suporte inicial da API Swift pelo sistema StorageGRID. A versão atualmente suportada é a API de armazenamento de objetos OpenStack Swift v1.

Como o StorageGRID implementa a API Swift REST

Um aplicativo cliente pode usar chamadas de API REST do Swift para se conetar a nós de storage e nós de Gateway para criar contentores e armazenar e recuperar objetos. Isso permite que aplicativos orientados a serviços desenvolvidos para o OpenStack Swift se conetem com storage de objetos no local fornecido pelo sistema StorageGRID.

Gerenciamento de objetos Swift

Depois que os objetos Swift foram ingeridos no sistema StorageGRID, eles são gerenciados pelas regras de gerenciamento do ciclo de vida da informação (ILM) na política ativa de ILM do sistema. As regras e a política do ILM determinam como o StorageGRID cria e distribui cópias de dados de objetos e como gerencia essas cópias ao longo do tempo. Por exemplo, uma regra ILM pode se aplicar a objetos em contentores Swift específicos e pode especificar que várias cópias de objetos sejam salvas em vários data centers por um certo número de anos.

Entre em Contato com o administrador do StorageGRID se você precisar entender como as regras e políticas do ILM da grade afetarão os objetos em sua conta de locatário do Swift.

Solicitações de cliente conflitantes

As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação, e não em quando clientes Swift iniciam uma operação.

Garantias de consistência e controles

Por padrão, o StorageGRID fornece consistência de leitura após gravação para objetos recém-criados e consistência para atualizações de objetos e operações HEAD. Qualquer GET seguindo um PUT concluído com sucesso será capaz de ler os dados recém-escritos. As 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.

O StorageGRID também permite que você controle a consistência por contentor. Você pode alterar o controle de consistência para fornecer um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de storage e locais, conforme necessário pela aplicação.

Informações relacionadas

Gerenciar objetos com ILM

OBTER solicitação de consistência de contêiner

COLOQUE o pedido de consistência do recipiente

Recomendações para a implementação da API Swift REST

Você deve seguir estas recomendações ao implementar a API REST do Swift para uso com o StorageGRID.

Recomendações para heads to non-existent objects

Se seu aplicativo verifica rotineiramente para ver se um objeto existe em um caminho onde você não espera que o objeto realmente exista, você deve usar o controle de consistência ""disponível"". Por exemplo, você deve usar o controle de consistência "disponível" se seu aplicativo executar uma operação DE CABEÇA para um local antes de executar uma OPERAÇÃO DE COLOCAÇÃO nesse local.

Caso contrário, se a operação PRINCIPAL não encontrar o objeto, você poderá receber um número alto de 500 erros de servidor interno se um ou mais nós de storage não estiverem disponíveis.

Você pode definir o controle de consistência "disponível" para cada recipiente usando o pedido de consistência de contentor PUT.

Recomendações para nomes de objetos

Para contêineres criados no StorageGRID 11,4 ou posterior, a restrição de nomes de objetos para atender às práticas recomendadas de performance não é mais necessária. Por exemplo, agora você pode usar valores aleatórios para os primeiros quatro carateres de nomes de objetos.

Para contêineres que foram criados em versões anteriores ao StorageGRID 11,4, siga estas recomendações para nomes de objetos:

- Você não deve usar valores aleatórios como os primeiros quatro carateres de nomes de objetos. Isso está em contraste com a antiga recomendação da AWS para prefixos de nomes. Em vez disso, você deve usar

prefixos não aleatórios e não exclusivos, como `image` .

- Se você seguir a antiga recomendação da AWS para usar carateres aleatórios e exclusivos em prefixos de nome, você deve prefixar os nomes de objeto com um nome de diretório. Ou seja, use este formato:

```
mycontainer/mydir/f8e3-image3132.jpg
```

Em vez deste formato:

```
mycontainer/f8e3-image3132.jpg
```

Recomendações para "leituras de intervalo"

Se a opção **Compress Stored Objects** estiver selecionada (**CONFIGURATION System Grid options**), os aplicativos cliente Swift devem evitar executar operações de objeto GET que especificam um intervalo de bytes que serão retornados. Essas operações de leitura de intervalo são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GET Object que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é muito ineficiente ler um intervalo de 10 MB de um objeto compactado de 50 GB.

Se os intervalos forem lidos a partir de objetos compatados, as solicitações do cliente podem expirar.

> Se você precisar compactar objetos e seu aplicativo cliente precisar usar leituras de intervalo, aumente o tempo limite de leitura para o aplicativo.

Informações relacionadas

OBTER solicitação de consistência de contêiner

COLOQUE o pedido de consistência do recipiente

Administrar o StorageGRID

Configurar contas de inquilino e conexões

Configurar o StorageGRID para aceitar conexões de aplicativos cliente requer a criação de uma ou mais contas de locatário e a configuração das conexões.

Criar e configurar contas de locatário Swift

Uma conta de locatário Swift é necessária antes que os clientes da API Swift possam armazenar e recuperar objetos no StorageGRID. Cada conta de locatário tem seu próprio ID de conta, grupos e usuários, além de contentores e objetos.

As contas de locatário Swift são criadas por um administrador de grade do StorageGRID usando o Gerenciador de grade ou a API de gerenciamento de grade.

Ao criar uma conta de locatário Swift, o administrador da grade especifica as seguintes informações:

- Nome de exibição para o locatário (o ID da conta do locatário é atribuído automaticamente e não pode ser alterado)

- Opcionalmente, uma cota de armazenamento para a conta de locatário - o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos do locatário. A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco).
- Se o logon único (SSO) não estiver em uso para o sistema StorageGRID, se a conta do locatário usará sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.
- Se o SSO estiver ativado, qual grupo federado tem permissão de acesso root para configurar a conta de locatário.

Depois que uma conta de locatário Swift for criada, os usuários com a permissão de acesso root podem acessar o Gerenciador do locatário para executar tarefas como as seguintes:

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

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

Informações relacionadas

Administrar o StorageGRID

Use a conta de locatário

Endpoints de API Swift compatíveis

Como as conexões do cliente podem ser configuradas

Um administrador de grade faz escolhas de configuração que afetam a forma como os clientes Swift se conetam ao StorageGRID para armazenar e recuperar dados. As informações específicas que você precisa para fazer uma conexão dependem da configuração escolhida.

Os aplicativos clientes podem armazenar ou recuperar objetos conetando-se a qualquer um dos seguintes:

- O serviço Load Balancer em nós de administração ou nós de gateway, ou, opcionalmente, o endereço IP virtual de um grupo de alta disponibilidade (HA) de nós de administração ou nós de gateway
- O serviço CLB em nós de Gateway, ou, opcionalmente, o endereço IP virtual de um grupo de nós de gateway de alta disponibilidade

> O serviço CLB está obsoleto. Os clientes configurados antes da versão do StorageGRID 11,3 podem continuar a usar o serviço CLB nos nós de gateway. Todos os outros aplicativos clientes que dependem do StorageGRID para fornecer balanceamento de carga devem se conetar usando o serviço de balanceamento de carga.

- Nós de storage, com ou sem um balanceador de carga externo

Ao configurar o StorageGRID, um administrador de grade pode usar o Gerenciador de grade ou a API de gerenciamento de grade para executar as seguintes etapas, todas opcionais:

1. Configure endpoints para o serviço Load Balancer.

Você deve configurar endpoints para usar o serviço Load Balancer. O serviço Load Balancer em nós de administração ou nós de gateway distribui conexões de rede recebidas de aplicativos clientes para nós de storage. Ao criar um endpoint de balanceador de carga, o administrador do StorageGRID especifica um número de porta, se o endpoint aceita conexões HTTP ou HTTPS, o tipo de cliente (S3 ou Swift) que usará o endpoint e o certificado a ser usado para conexões HTTPS (se aplicável).

2. Configurar redes de clientes não confiáveis.

   Se um administrador do StorageGRID configurar a rede cliente de um nó para não ser confiável, o nó só aceita conexões de entrada na rede cliente em portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

3. Configurar grupos de alta disponibilidade.

   Se um administrador criar um grupo de HA, as interfaces de rede de vários nós de Admin ou nós de Gateway serão colocadas em uma configuração de backup ativo. As conexões de cliente são feitas usando o endereço IP virtual do grupo HA.

Para obter mais informações sobre cada opção, consulte as instruções para administrar o StorageGRID.

Resumo: Endereços IP e portas para conexões de clientes

Os aplicativos cliente se conetam ao StorageGRID usando o endereço IP de um nó de grade e o número da porta de um serviço nesse nó. Se os grupos de alta disponibilidade (HA) estiverem configurados, os aplicativos clientes poderão se conetar usando o endereço IP virtual do grupo HA.

Informações necessárias para fazer conexões com o cliente

A tabela resume as diferentes maneiras pelas quais os clientes podem se conetar ao StorageGRID e os endereços IP e as portas usadas para cada tipo de conexão. Contate o administrador do StorageGRID para obter mais informações ou consulte as instruções de administração do StorageGRID para obter uma descrição de como localizar essas informações no Gerenciador de Grade.

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	• Porta de extremidade do balanceador de carga
Grupo HA	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP virtual de um grupo HA	Portas Swift padrão: • HTTPS: 8083 • HTTP: 8085
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	• Porta de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	• Porta de extremidade do balanceador de carga

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Nó de gateway	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP do nó de gateway **Nota:** por padrão, as portas HTTP para CLB e LDR não estão ativadas.	Portas Swift padrão: • HTTPS: 8083 • HTTP: 8085
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas Swift padrão: • HTTPS: 18083 • HTTP: 18085

Exemplo

Para conetar um cliente Swift ao endpoint do Load Balancer de um grupo de HA de nós de Gateway, use um URL estruturado como mostrado abaixo:

- `https://VIP-of-HA-group:LB-endpoint-port`

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.6 e o número da porta de um endpoint do Swift Load Balancer for 10444, um cliente Swift poderá usar o seguinte URL para se conetar ao StorageGRID:

- `https://192.0.2.6:10444`

É possível configurar um nome DNS para o endereço IP que os clientes usam para se conetar ao StorageGRID. Contacte o administrador da rede local.

Decida usar conexões HTTPS ou HTTP

Quando as conexões de cliente são feitas usando um endpoint de Load Balancer, as conexões devem ser feitas usando o protocolo (HTTP ou HTTPS) especificado para esse endpoint. Para usar HTTP para conexões de cliente a nós de armazenamento ou ao serviço CLB em nós de gateway, você deve habilitar seu uso.

Por padrão, quando os aplicativos cliente se conetam a nós de armazenamento ou ao serviço CLB nos nós de Gateway, eles devem usar HTTPS criptografado para todas as conexões. Opcionalmente, você pode habilitar conexões HTTP menos seguras selecionando a opção de grade **Ativar conexão HTTP** no Gerenciador de Grade. Por exemplo, um aplicativo cliente pode usar HTTP ao testar a conexão com um nó de armazenamento em um ambiente que não seja de produção.

Tenha cuidado ao ativar o HTTP para uma grade de produção, já que as solicitações serão enviadas sem criptografia.

O serviço CLB está obsoleto.

Se a opção **Enable HTTP Connection** estiver selecionada, os clientes devem usar portas diferentes para HTTP do que para HTTPS. Consulte as instruções para administrar o StorageGRID.

Informações relacionadas

Administrar o StorageGRID

Teste sua conexão na configuração da API Swift

Você pode usar o Swift CLI para testar sua conexão com o sistema StorageGRID e verificar se você pode ler e gravar objetos no sistema.

O que você vai precisar

- Você deve ter baixado e instalado Python-swiftclient, o cliente de linha de comando Swift.

  "SwiftStack: python-swiftclient"

- Você deve ter uma conta de locatário Swift no sistema StorageGRID.

Sobre esta tarefa

Se você não tiver configurado a segurança, você deve adicionar o `--insecure` sinalizador a cada um desses comandos.

Passos

1. Consulte o URL de informações para sua implantação do StorageGRID Swift:

   ```
   swift
   -U <Tenant_Account_ID:Account_User_Name>
   -K <User_Password>
   -A https://<FQDN | IP>:<Port>/info
   capabilities
   ```

   Isso é suficiente para testar se sua implantação do Swift está funcional. Para testar ainda mais a configuração da conta armazenando um objeto, continue com as etapas adicionais.

2. Coloque um objeto no recipiente:

   ```
   touch test_object
   swift
   -U <Tenant_Account_ID:Account_User_Name>
   -K <User_Password>
   -A https://<FQDN | IP>:<Port>/auth/v1.0
   upload test_container test_object
   --object-name test_object
   ```

3. Obtenha o contentor para verificar o objeto:

   ```
   swift
   -U <Tenant_Account_ID:Account_User_Name>
   -K <User_Password>
   -A https://<FQDN | IP>:<Port>/auth/v1.0
   list test_container
   ```

4. Eliminar o objeto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Eliminar o recipiente:

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

Informações relacionadas

Criar e configurar contas de locatário Swift

Configurar a segurança para API REST

Operações suportadas pela API REST Swift

O sistema StorageGRID dá suporte à maioria das operações na API OpenStack Swift. Antes de integrar clientes API REST do Swift com o StorageGRID, revise os detalhes de implementação para operações de conta, contentor e objeto.

Operações suportadas no StorageGRID

As seguintes operações da API Swift são suportadas:

- Operações de conta
- Operações de contêiner
- Operações de objetos

Cabeçalhos de resposta comuns para todas as operações

O sistema StorageGRID implementa todos os cabeçalhos comuns para operações com suporte, conforme definido pela API de armazenamento de objetos OpenStack Swift v1.

Informações relacionadas

"OpenStack: API de storage de objetos"

Endpoints de API Swift compatíveis

O StorageGRID oferece suporte aos seguintes endpoints da API Swift: O URL de

informações, o URL de autenticação e o URL de armazenamento.

URL de informações

Você pode determinar os recursos e limitações da implementação do StorageGRID Swift emitindo uma solicitação GET para o URL base do Swift com o caminho /info.

```
https://FQDN | Node IP:Swift Port/info/
```

No pedido:

- *FQDN* é o nome de domínio totalmente qualificado.
- *Node IP* É o endereço IP do nó de armazenamento ou do nó de gateway na rede StorageGRID.
- *Swift Port* É o número de porta usado para conexões Swift API no nó de armazenamento ou nó de gateway.

Por exemplo, o seguinte URL de informações solicitaria informações de um nó de armazenamento com o endereço IP de 10.99.106.103 e usando a porta 18083.

```
https://10.99.106.103:18083/info/
```

A resposta inclui os recursos da implementação Swift como um dicionário JSON. Uma ferramenta cliente pode analisar a resposta JSON para determinar os recursos da implementação e usá-los como restrições para operações de armazenamento subsequentes.

A implementação do StorageGRID do Swift permite o acesso não autenticado ao URL de informações.

URL de autenticação

Um cliente pode usar o URL de autenticação Swift para autenticar como usuário de conta de locatário.

```
https://FQDN | Node IP:Swift Port/auth/v1.0/
```

Você deve fornecer o ID da conta do locatário, o nome de usuário e a senha como parâmetros nos `X-Auth-User` cabeçalhos e `X-Auth-Key` da solicitação, da seguinte forma:

```
X-Auth-User: Tenant_Account_ID:Username

X-Auth-Key: Password
```

Nos cabeçalhos de solicitação:

- *Tenant_Account_ID* É o ID de conta atribuído pelo StorageGRID quando o locatário Swift foi criado. Esse é o mesmo ID de conta de locatário usado na página de login do Gerenciador do Locatário.
- *Username* É o nome de um usuário do locatário que foi criado no Gerenciador do Locatário. Esse usuário deve pertencer a um grupo que tenha a permissão Swift Administrator. O usuário raiz do locatário não pode ser configurado para usar a API REST do Swift.

  Se a Federação de identidade estiver ativada para a conta de locatário, forneça o nome de usuário e a senha do usuário federado do servidor LDAP. Em alternativa, forneça o nome de domínio do utilizador LDAP. Por exemplo:

  ```
  X-Auth-User: Tenant_Account_ID:Username@Domain_Name
  ```

- *Password* é a senha para o usuário do locatário. As senhas de usuário são criadas e gerenciadas no Gerenciador do locatário.

A resposta a uma solicitação de autenticação bem-sucedida retorna um URL de armazenamento e um token de autenticação, como segue:

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID

X-Auth-Token: token

X-Storage-Token: token
```

Por padrão, o token é válido por 24 horas a partir do tempo de geração.

Os tokens são gerados para uma conta de locatário específica. Um token válido para uma conta não autoriza um usuário a acessar outra conta.

URL de armazenamento

Um aplicativo cliente pode emitir chamadas de API REST Swift para executar operações de conta, contentor e objeto com suporte em um nó de gateway ou nó de storage. As solicitações de armazenamento são endereçadas ao URL de armazenamento retornado na resposta de autenticação. A solicitação também deve incluir o cabeçalho X-Auth-Token e o valor retornado da solicitação de autenticação.

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID

[/container][/object]

X-Auth-Token: token
```

Alguns cabeçalhos de resposta de armazenamento que contêm estatísticas de uso podem não refletir números precisos para objetos modificados recentemente. Pode levar alguns minutos para que números precisos apareçam nesses cabeçalhos.

Os cabeçalhos de resposta a seguir para operações de conta e contentor são exemplos daqueles que contêm estatísticas de uso:

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

Informações relacionadas

Configurar contas de inquilino e conexões

Operações de conta

Operações de contêiner

Operações de objetos

Operações de conta

As seguintes operações da API Swift são realizadas em contas.

OBTER conta

Esta operação recupera a lista de contentores associada às estatísticas de uso de conta e conta.

É necessário o seguinte parâmetro de pedido:

- `Account`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes parâmetros de consulta de solicitação suportados são opcionais:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Prefix`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta HTTP/1,1 204 no content" se a conta for encontrada e não tiver contentores ou a lista de contentores estiver vazia; ou uma resposta HTTP/1,1 200 OK se a conta for encontrada e a lista de contentores não estiver vazia:

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Conta principal

Esta operação recupera informações de conta e estatísticas de uma conta Swift.

É necessário o seguinte parâmetro de pedido:

- `Account`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "'HTTP/1,1 204 no Content'":

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Informações relacionadas

Monitorar e auditar operações

Operações de contêiner

O StorageGRID suporta um máximo de 1.000 contentores por conta Swift. As seguintes operações da API Swift são executadas em contentores.

ELIMINAR recipiente

Esta operação remove um contentor vazio de uma conta Swift em um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 204 sem conteúdo":

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

PEGUE o recipiente

Esta operação recupera a lista de objetos associada ao contentor juntamente com estatísticas de contentor e metadados em um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes parâmetros de consulta de solicitação suportados são opcionais:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Path`
- `Prefix`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 200 success" ou "HTTP/1,1 204 no content":

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Recipiente DA cabeça

Esta operação recupera estatísticas de contentor e metadados de um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 204 sem conteúdo":

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

COLOQUE o recipiente

Esta operação cria um contentor para uma conta em um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 201 criado" ou "HTTP/1,1 202 aceito" (se o contentor já existir sob esta conta):

- `Content-Length`
- `Date`
- `X-Timestamp`
- `X-Trans-Id`

Um nome de contêiner deve ser exclusivo no namespace StorageGRID. Se o contentor existir sob outra conta, o seguinte cabeçalho é retornado: "Conflito HTTP/1,1 409".

Informações relacionadas

Monitorar e auditar operações

Operações de objetos

As seguintes operações da API Swift são executadas em objetos.

ELIMINAR objeto

Esta operação exclui o conteúdo e os metadados de um objeto do sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`
- `Object`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos de resposta com uma `HTTP/1.1 204 No Content` resposta:

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Ao processar uma solicitação DE EXCLUSÃO de objetos, o StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais armazenados. Se for bem-sucedido, o StorageGRID retornará uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas dentro de 30 segundos (por exemplo, porque um local está temporariamente indisponível), o StorageGRID coloca as cópias em fila para remoção e, em seguida, indica sucesso para o cliente.

Para obter mais informações sobre como os objetos são excluídos, consulte as instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.

OBTER objeto

Esta operação recupera o conteúdo do objeto e obtém os metadados do objeto de um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`
- `Object`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes cabeçalhos de solicitação são opcionais:

- `Accept-Encoding`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`

- `If-Unmodified-Since`
- `Range`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com `HTTP/1.1 200 OK` uma resposta:

- `Accept-Ranges`
- `Content-Disposition`, retornada somente se `Content-Disposition` os metadados tiverem sido definidos
- `Content-Encoding`, retornada somente se `Content-Encoding` os metadados tiverem sido definidos
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

Objeto PRINCIPAL

Esta operação recupera metadados e propriedades de um objeto ingerido a partir de um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`
- `Object`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 200 OK":

- `Accept-Ranges`
- `Content-Disposition`, retornada somente se `Content-Disposition` os metadados tiverem sido definidos
- `Content-Encoding`, retornada somente se `Content-Encoding` os metadados tiverem sido definidos
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`

- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

COLOQUE o objeto

Essa operação cria um novo objeto com dados e metadados ou substitui um objeto existente por dados e metadados em um sistema StorageGRID.

O StorageGRID suporta objetos de até 5 TIB (5.497.558.138.880 bytes) de tamanho.

> As solicitações de cliente conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "vitórias mais recentes". O tempo para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação, e não em quando clientes Swift iniciam uma operação.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`
- `Object`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes cabeçalhos de solicitação são opcionais:

- `Content-Disposition`
- `Content-Encoding`

  Não use em pedaços `Content-Encoding` se a regra ILM que se aplica a um objeto filtra objetos com base no tamanho e usa o posicionamento síncrono na ingestão (as opções balanceadas ou rigorosas para o comportamento de ingestão).

- `Transfer-Encoding`

  Não use compactado ou dividido `Transfer-Encoding` se a regra ILM que se aplica a um objeto filtra objetos com base no tamanho e usa o posicionamento síncrono na ingestão (as opções balanceadas ou rigorosas para o comportamento de ingestão).

- `Content-Length`

  Se uma regra de ILM filtrar objetos por tamanho e usar o posicionamento síncrono na ingestão, você deverá especificar `Content-Length`.

> Se você não seguir estas diretrizes para `Content-Encoding`, `Transfer-Encoding` e `Content-Length`, o StorageGRID deve salvar o objeto antes que ele possa determinar o tamanho do objeto e aplicar a regra ILM. Em outras palavras, o StorageGRID deve criar cópias provisórias de um objeto na ingestão. Ou seja, o StorageGRID deve usar a opção de confirmação dupla para o comportamento de ingestão.

Para obter mais informações sobre o posicionamento síncrono e as regras de ILM, consulte as instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` (metadados relacionados a objetos)

  Se você quiser usar a opção **tempo de criação definido pelo usuário** como tempo de referência para uma regra ILM, você deve armazenar o valor em um cabeçalho definido pelo usuário chamado `X-Object-Meta-Creation-Time`. Por exemplo:

  ```
  X-Object-Meta-Creation-Time: 1443399726
  ```

  Este campo é avaliado em segundos desde 1 de janeiro de 1970.

- `X-Storage-Class: reduced_redundancy`

  Esse cabeçalho afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM que corresponde a um objeto ingerido especificar um comportamento de ingestão de confirmação dupla ou equilibrada.

  - **Commit duplo**: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, o StorageGRID cria uma única cópia provisória à medida que o objeto é ingerido (commit único).
  - **Balanced**: Se a regra ILM especificar a opção Balanced, 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` cabeçalho é melhor usado quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso, o uso `reduced_redundancy` elimina a criação e exclusão desnecessárias de uma cópia de objeto extra para cada operação de ingestão.

    O uso do `reduced_redundancy` cabeçalho não é recomendado em outras circunstâncias porque aumenta o risco de perda de dados de objetos durante a ingestão. Por exemplo, você pode perder dados se a única cópia for inicialmente armazenada em um nó de armazenamento que falha antes que a avaliação ILM possa ocorrer.

    > Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver 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.

Observe que especificar `reduced_redundancy` apenas afeta quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Ele não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pela política ILM ativa e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 201 criado":

- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Trans-Id`

Informações relacionadas

Gerenciar objetos com ILM

Monitorar e auditar operações

Pedido de OPÇÕES

A SOLICITAÇÃO DE OPÇÕES verifica a disponibilidade de um serviço Swift individual. A SOLICITAÇÃO DE OPÇÕES é processada pelo nó de armazenamento ou nó de gateway especificado no URL.

Método de OPÇÕES

Por exemplo, os aplicativos clientes podem emitir uma SOLICITAÇÃO DE OPÇÕES para a porta Swift em um nó de armazenamento, sem fornecer credenciais de autenticação Swift, 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 storage está inativo.

Quando usado com o URL info ou o URL de armazenamento, o método OPTIONS retorna uma lista de verbos suportados para o URL dado (por exemplo, HEAD, GET, OPTIONS E PUT). O método DE OPÇÕES não pode ser usado com o URL de autenticação.

É necessário o seguinte parâmetro de pedido:

- `Account`

Os seguintes parâmetros de pedido são opcionais:

- `Container`
- `Object`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta HTTP/1,1 204 no content". A SOLICITAÇÃO DE OPÇÕES para o URL de armazenamento não exige que o destino exista.

- `Allow` (Uma lista de verbos suportados para o URL dado, por exemplo, HEAD, GET, OPTIONS e PUT)

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Informações relacionadas

Endpoints de API Swift compatíveis

Respostas de erro às operações da API Swift

Entender as possíveis respostas de erro pode ajudá-lo a solucionar problemas de operações.

Os seguintes códigos de status HTTP podem ser retornados quando erros ocorrem durante uma operação:

Nome de erro Swift	Status HTTP
AccountNameToLong, ContainerNameToLong, HeaderToBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameToLong, MetadataValueToBig, MissingSecurityHeader, ObjectNameToLong, ToManyContainers, ToManyMetadataItems, TotalMetataTooLarge	400 pedido incorreto
AccessDenied	403 proibido
ContainerNotEmpty, ContainerAlreadyExists	409 conflito
InternalError (erro internacional)	500 erro interno do servidor
Intervalo Invalidável	416 intervalo solicitado não satisfatório
MetodNotAlloved	Método 405 não permitido
MissingContentLength	411 comprimento necessário
Não encontrado	404 não encontrado
Sem Implementado	501 não implementado
Pré-condiçãoFailed	412 Pré-condição falhou
ResourceNotFound	404 não encontrado
Não autorizado	401 não autorizado

Nome de erro Swift	Status HTTP
UnprocessableEntity	422 entidade não processável

Operações da API REST do StorageGRID Swift

Há operações adicionadas à API REST do Swift que são específicas do sistema StorageGRID.

OBTER solicitação de consistência de contêiner

O nível de consistência fornece um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de storage e locais. A solicitação GET Container Consistency permite que você determine o nível de consistência que está sendo aplicado a um contentor específico.

Pedido

Solicitar cabeçalho HTTP	Descrição
`X-Auth-Token`	Especifica o token de autenticação Swift para a conta a ser usada para a solicitação.
`x-ntap-sg-consistency`	Especifica o tipo de solicitação, onde `true` OBTÉM consistência de contentor e `false` OBTÉM contentor.
`Host`	O nome do host para o qual a solicitação é direcionada.

Exemplo de solicitação

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Resposta

Cabeçalho HTTP de resposta	Descrição
`Date`	A data e a hora da resposta.
`Connection`	Se a conexão com o servidor está aberta ou fechada.
`X-Trans-Id`	O identificador de transação exclusivo para a solicitação.

Cabeçalho HTTP de resposta	Descrição
`Content-Length`	O comprimento do corpo de resposta.
`x-ntap-sg-consistency`	O nível de controle de consistência que está sendo aplicado ao recipiente. Os seguintes valores são suportados: • **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. • **Read-after-novo-write**: Fornece consistência de leitura-após-gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. **Nota**: Se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, use o nível "disponível". • **Available** (eventual consistência para OPERAÇÕES DE CABEÇA): Comporta-se da mesma forma que o nível de consistência "read-after-new-write", mas apenas fornece consistência eventual para operações DE CABEÇA. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis.

Exemplo de resposta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

Informações relacionadas

COLOQUE o pedido de consistência do recipiente

A solicitação de consistência de contentor PUT permite especificar o nível de consistência a ser aplicado às operações realizadas em um contentor. Por padrão, novos contentores são criados usando o nível de consistência "read-after-new-write".

Pedido

Solicitar cabeçalho HTTP	Descrição
`X-Auth-Token`	O token de autenticação Swift para a conta a ser usada para a solicitação.
`x-ntap-sg-consistency`	O nível de controle de consistência a aplicar às operações no recipiente. Os seguintes valores são suportados: • **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. • **Read-after-novo-write**: Fornece consistência de leitura-após-gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. **Nota**: Se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, use o nível "disponível". • **Available** (eventual consistência para OPERAÇÕES DE CABEÇA): Comporta-se da mesma forma que o nível de consistência "read-after-new-write", mas apenas fornece consistência eventual para operações DE CABEÇA. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis.
`Host`	O nome do host para o qual a solicitação é direcionada.

Como os controles de consistência e as regras de ILM interagem para afetar a proteção de dados

Tanto a sua escolha de controle de consistência quanto a sua regra ILM afetam a forma como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, o controle de consistência usado 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 exige acesso aos metadados de um objeto e aos dados para atender às solicitações do cliente, selecionar níveis de proteção correspondentes para o nível de consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas do sistema mais previsíveis.

Os seguintes comportamentos de ingestão estão disponíveis para regras ILM:

- **Strict**: Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja devolvido ao cliente.
- **Balanced**: O StorageGRID tenta fazer todas as cópias especificadas na regra ILM no ingest; 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.
- * Commit duplo*: O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

> Antes de selecionar o comportamento de ingestão para uma regra ILM, leia a descrição completa dessas configurações nas instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Exemplo de como o controle de consistência e a regra ILM podem interagir

Suponha que você tenha uma grade de dois locais com a seguinte regra ILM e a seguinte configuração de nível de consistência:

- **Regra ILM**: Crie duas cópias de objeto, uma no local e outra em um local remoto. O comportamento de ingestão estrita é selecionado.
- **Nível de consistência**: "Trong-global" (metadados de objetos são imediatamente distribuídos para todos os sites.)

Quando um cliente armazena um objeto na grade, o StorageGRID faz cópias de objeto e distribui metadados para ambos os sites antes de retornar sucesso ao cliente.

O objeto é totalmente protegido contra perda no momento da mensagem de ingestão bem-sucedida. Por exemplo, se o local for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existem no local remoto. O objeto é totalmente recuperável.

Se, em vez disso, você usou a mesma regra ILM e o nível de consistência "site-trong", o cliente poderá receber uma mensagem de sucesso depois que os dados do objeto forem replicados para o site remoto, mas antes que os metadados do objeto sejam distribuídos lá. Nesse caso, o nível de proteção dos metadados de objetos não corresponde ao nível de proteção dos dados de 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 níveis de consistência e regras de ILM pode ser complexa. Contacte a NetApp se necessitar de assistência.

Exemplo de solicitação

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

Resposta

Cabeçalho HTTP de resposta	Descrição
`Date`	A data e a hora da resposta.
`Connection`	Se a conexão com o servidor está aberta ou fechada.
`X-Trans-Id`	O identificador de transação exclusivo para a solicitação.
`Content-Length`	O comprimento do corpo de resposta.

Exemplo de resposta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

Informações relacionadas

Use a conta de locatário

Configurar a segurança para API REST

Você deve analisar as medidas de segurança implementadas para a API REST e entender como proteger seu sistema.

Como o StorageGRID fornece segurança para API REST

Você deve entender como o sistema StorageGRID implementa segurança, autenticação e autorização para a API REST.

O StorageGRID usa as seguintes medidas de segurança.

- As comunicações do cliente com o serviço Load Balancer usam HTTPS se o HTTPS estiver configurado para o ponto de extremidade do balanceador de carga.

  Quando você configura um ponto de extremidade do balanceador de carga, o HTTP pode ser habilitado

opcionalmente. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

- Por padrão, o StorageGRID usa HTTPS para comunicações de clientes com nós de armazenamento e o serviço CLB em nós de gateway.

  O HTTP pode, opcionalmente, ser habilitado para essas conexões. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

  O serviço CLB está obsoleto.

- As comunicações entre o StorageGRID e o cliente são criptografadas usando TLS.
- As comunicações entre o serviço Load Balancer e os nós de armazenamento dentro da grade são criptografadas se o ponto de extremidade do balanceador de carga está configurado para aceitar conexões HTTP ou HTTPS.
- Os clientes devem fornecer cabeçalhos de autenticação HTTP ao StorageGRID para executar operações de API REST.

Certificados de segurança e aplicativos de cliente

Os clientes podem se conetar ao serviço Load Balancer em nós de gateway ou nós de administrador, diretamente aos nós de armazenamento ou ao serviço CLB obsoleto em nós de gateway.

Em todos os casos, os aplicativos clientes podem fazer conexões TLS usando um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado gerado pelo sistema StorageGRID:

- Quando os aplicativos cliente se conetam ao serviço do Load Balancer, eles fazem isso usando o certificado que foi configurado para o ponto de extremidade do balanceador de carga específico usado para fazer a conexão. Cada endpoint tem seu próprio certificado, que é um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado que o administrador da grade gerou no StorageGRID ao configurar o endpoint.
- Quando os aplicativos cliente se conetam diretamente a um nó de armazenamento ou ao serviço CLB nos nós de gateway, eles usam os certificados de servidor gerados pelo sistema que foram gerados para nós de armazenamento quando o sistema StorageGRID foi instalado (que são assinados pela autoridade de certificação do sistema) ou um único certificado de servidor personalizado fornecido para a grade por um administrador de grade.

Os clientes devem ser configurados para confiar na autoridade de certificação que assinou qualquer certificado que usam para estabelecer conexões TLS.

Consulte as instruções de administração do StorageGRID para obter informações sobre a configuração de pontos de extremidade do balanceador de carga e para obter instruções sobre como adicionar um único certificado de servidor personalizado para conexões TLS diretamente aos nós de armazenamento ou ao serviço CLB nos nós de gateway.

Resumo

A tabela a seguir mostra como os problemas de segurança são implementados nas APIs REST S3 e Swift:

Problema de segurança	Implementação da API REST
Segurança da ligação	TLS
Autenticação do servidor	Certificado de servidor X,509 assinado pela CA do sistema ou certificado de servidor personalizado fornecido pelo administrador
Autenticação de cliente	• S3: Conta S3 (ID da chave de acesso e chave de acesso secreta) • Swift: Conta Swift (nome de usuário e senha)
Autorização do cliente	• S3: Propriedade do bucket e todas as políticas de controle de acesso aplicáveis • Swift: Acesso à função de administrador

Informações relacionadas

Administrar o StorageGRID

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID suporta um conjunto limitado de conjuntos de codificação que os aplicativos clientes podem usar ao estabelecer uma sessão de Segurança da camada de Transporte (TLS).

Versões suportadas do TLS

O StorageGRID é compatível com TLS 1,2 e TLS 1,3.

SSLv3 e TLS 1,1 (ou versões anteriores) não são mais compatíveis.

Suítes de cifra suportadas

Versão TLS	IANA nome do conjunto de cifra
1,2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1,3	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

Conjuntos de codificação obsoletos

Os seguintes conjuntos de codificação são obsoletos. O suporte para essas cifras será removido em uma versão futura.

Nome IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Informações relacionadas

Configurar contas de inquilino e conexões

Monitorar e auditar operações

Você pode monitorar workloads e eficiências das operações do cliente visualizando tendências de transações para toda a grade ou para nós específicos. Você pode usar mensagens de auditoria para monitorar operações e transações do cliente.

Monitorar taxas de ingestão e recuperação de objetos

Você pode monitorar taxas de ingestão e recuperação de objetos, bem como métricas para contagens de objetos, consultas e verificação. Você pode exibir o número de tentativas bem-sucedidas e com falha por aplicativos clientes para ler, gravar e modificar objetos no sistema StorageGRID.

Passos

1. Faça login no Gerenciador de Grade usando um navegador da web suportado.
2. No painel de instrumentos, localize a secção Protocol Operations (operações de protocolo).

   Esta seção resume o número de operações do cliente realizadas pelo seu sistema StorageGRID. As taxas de protocolo são médias nos últimos dois minutos.

3. Selecione **NODES**.
4. Na página inicial dos nós (nível de implantação), clique na guia **Load Balancer**.

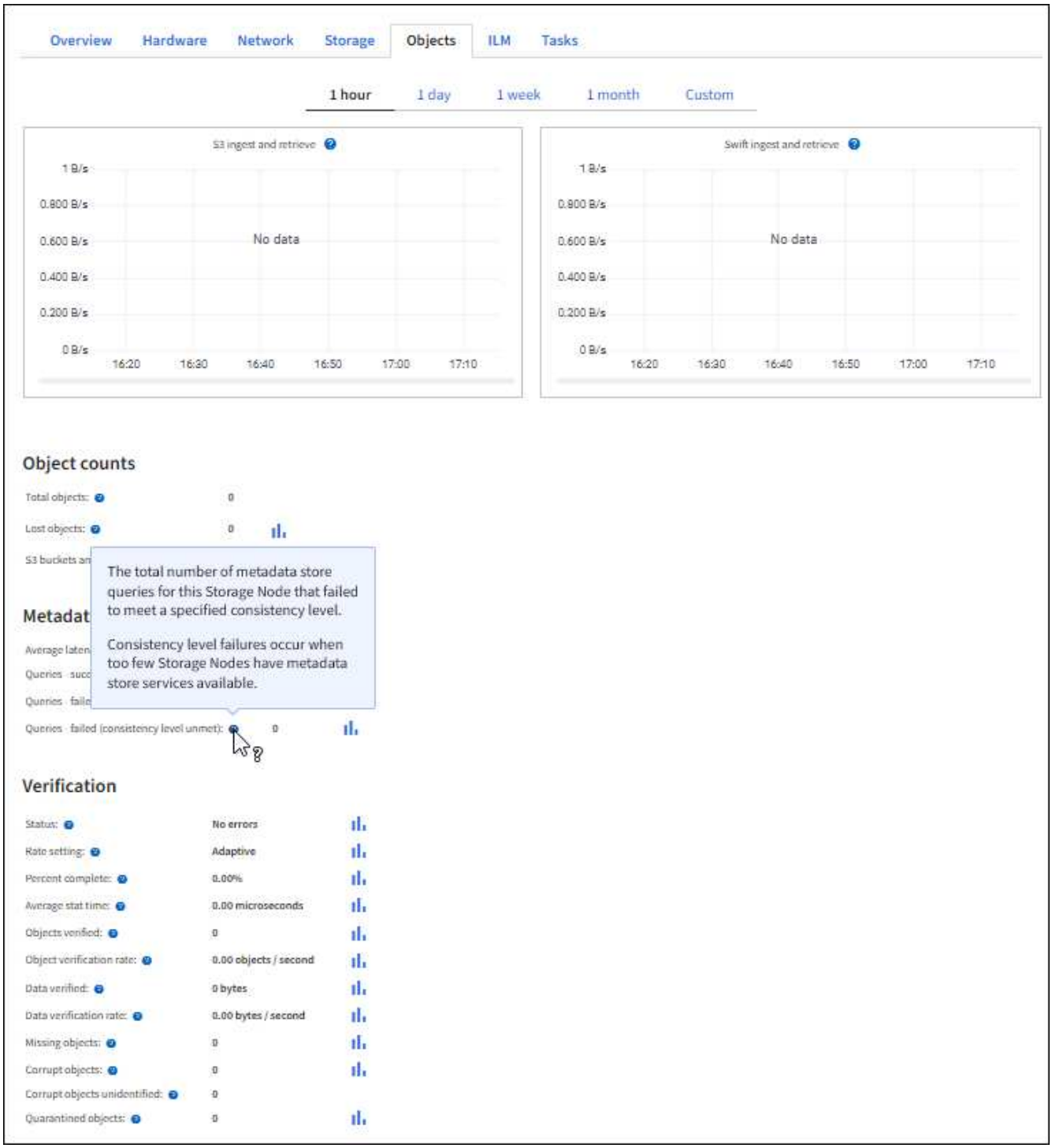
   Os gráficos mostram tendências para todo o tráfego do cliente direcionado para pontos de extremidade do balanceador de carga dentro da grade. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

5. Na home page dos nós (nível de implantação), clique na guia **objetos**.

   O gráfico mostra as taxas de ingestão e recuperação de todo o seu sistema StorageGRID em bytes por segundo e total de bytes. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

6. Para ver as informações de um nó de armazenamento específico, selecione o nó na lista à esquerda e clique na guia **Objects**.

   O gráfico mostra as taxas de ingestão e recuperação de objetos para este nó de armazenamento. A guia também inclui métricas para contagens de objetos, consultas e verificação. Você pode clicar nos rótulos para ver as definições dessas métricas.



7. Se você quiser ainda mais detalhes:
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   b. Selecione ***site* Visão geral Principal**.

      A seção operações da API exibe informações resumidas para toda a grade.

   c. Selecione ***Storage Node* LDR *client Application* Overview Main**

      A seção operações exibe informações resumidas para o nó de armazenamento selecionado.

Acesse e revise logs de auditoria

As mensagens de auditoria são geradas pelos serviços do StorageGRID e armazenadas em arquivos de log de texto. As mensagens de auditoria específicas da API nos logs de auditoria fornecem dados críticos de monitoramento de segurança, operação e desempenho que podem ajudá-lo a avaliar a integridade do sistema.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

Sobre esta tarefa

O arquivo de log de auditoria ativo é `audit.log` chamado , e é armazenado em nós de administração.

Uma vez por dia, o arquivo audit.log ativo é salvo e um novo arquivo audit.log é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato `yyyy-mm-dd.txt`.

Após um dia, o arquivo salvo é compactado e renomeado, no formato `yyyy-mm-dd.txt.gz`, que preserva a data original.

Este exemplo mostra o arquivo audit.log ativo, o arquivo do dia anterior (2018-04-15.txt) e o arquivo compactado para o dia anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Vá para o diretório que contém os arquivos de log de auditoria:`cd /var/local/audit/export`
3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.

Informações relacionadas

Rever registos de auditoria

Operações rápidas rastreadas nos logs de auditoria

Todas as operações bem-sucedidas de EXCLUSÃO, RECEBIMENTO, CABEÇALHO, POST e PUT DE armazenamento são rastreadas no log de auditoria do StorageGRID. As falhas não são registradas, nem são solicitações de informações, autenticação ou OPÇÕES.

Consulte *Entendendo mensagens de auditoria* para obter detalhes sobre as informações rastreadas para as seguintes operações do Swift.

Operações de conta

- OBTER conta
- Conta principal

Operações de contêiner

- ELIMINAR recipiente
- PEGUE o recipiente
- Recipiente DA cabeça
- COLOQUE o recipiente

Operações de objetos

- ELIMINAR objeto
- OBTER objeto
- Objeto PRINCIPAL
- COLOQUE o objeto

Informações relacionadas

Rever registos de auditoria

Operações de conta

Operações de contêiner

Operações de objetos

Informações sobre direitos autorais

Informações sobre marcas comerciais