Gerenciar buckets do S3

StorageGRID

NetApp
March 12, 2025

Índice

Gerenciar buckets do S3

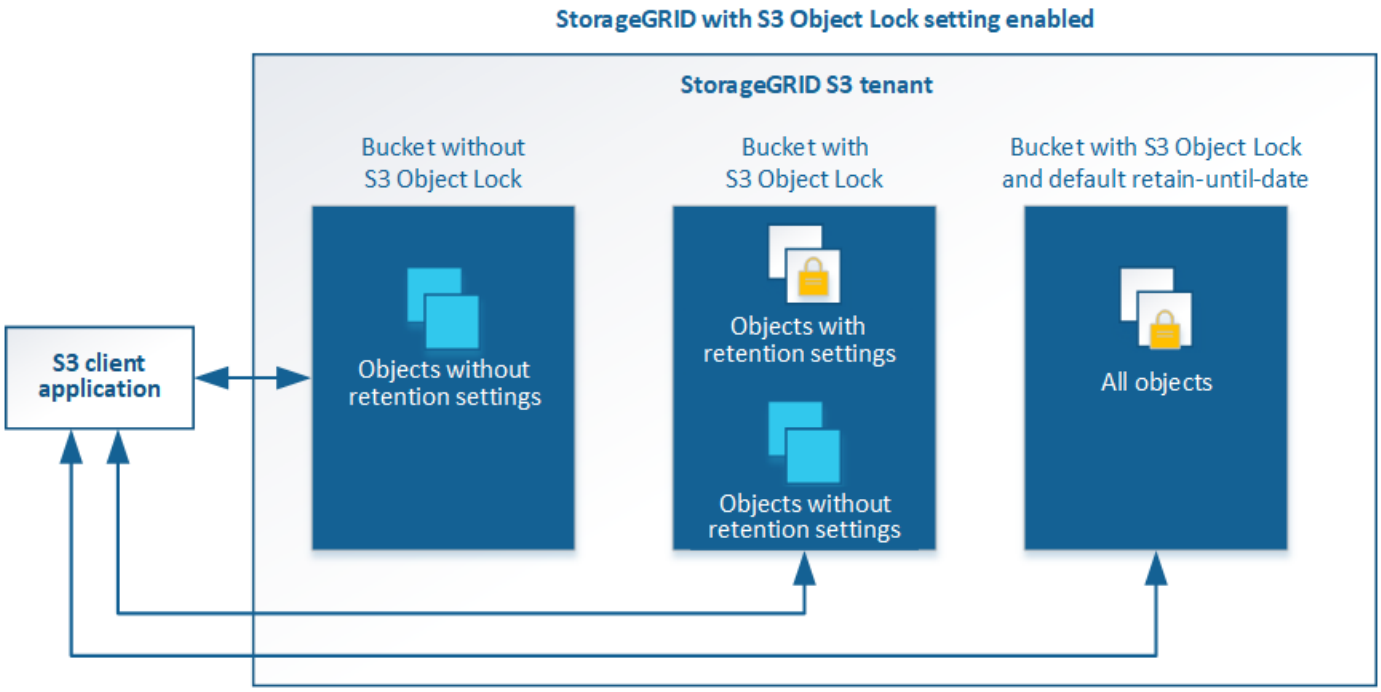
Use o bloqueio de objetos S3 com locatários

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.

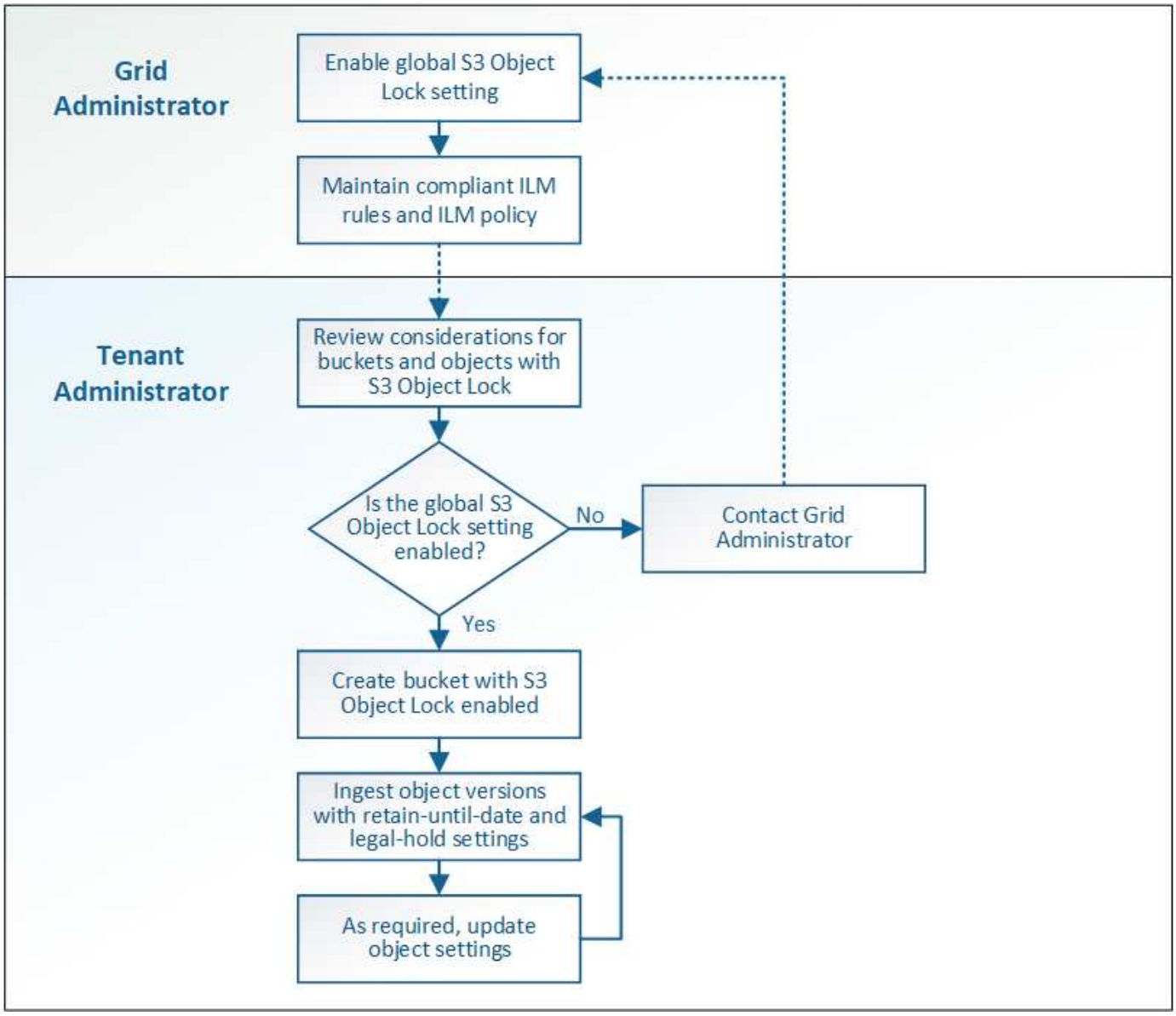
"Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"

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.



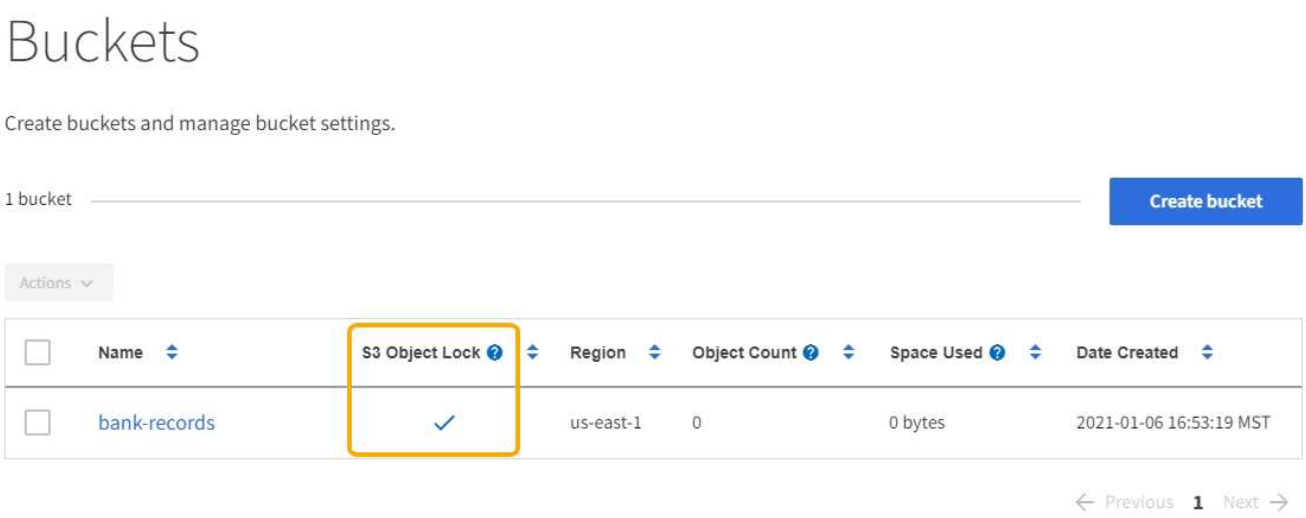
Requisitos para o bloqueio de objetos S3

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.

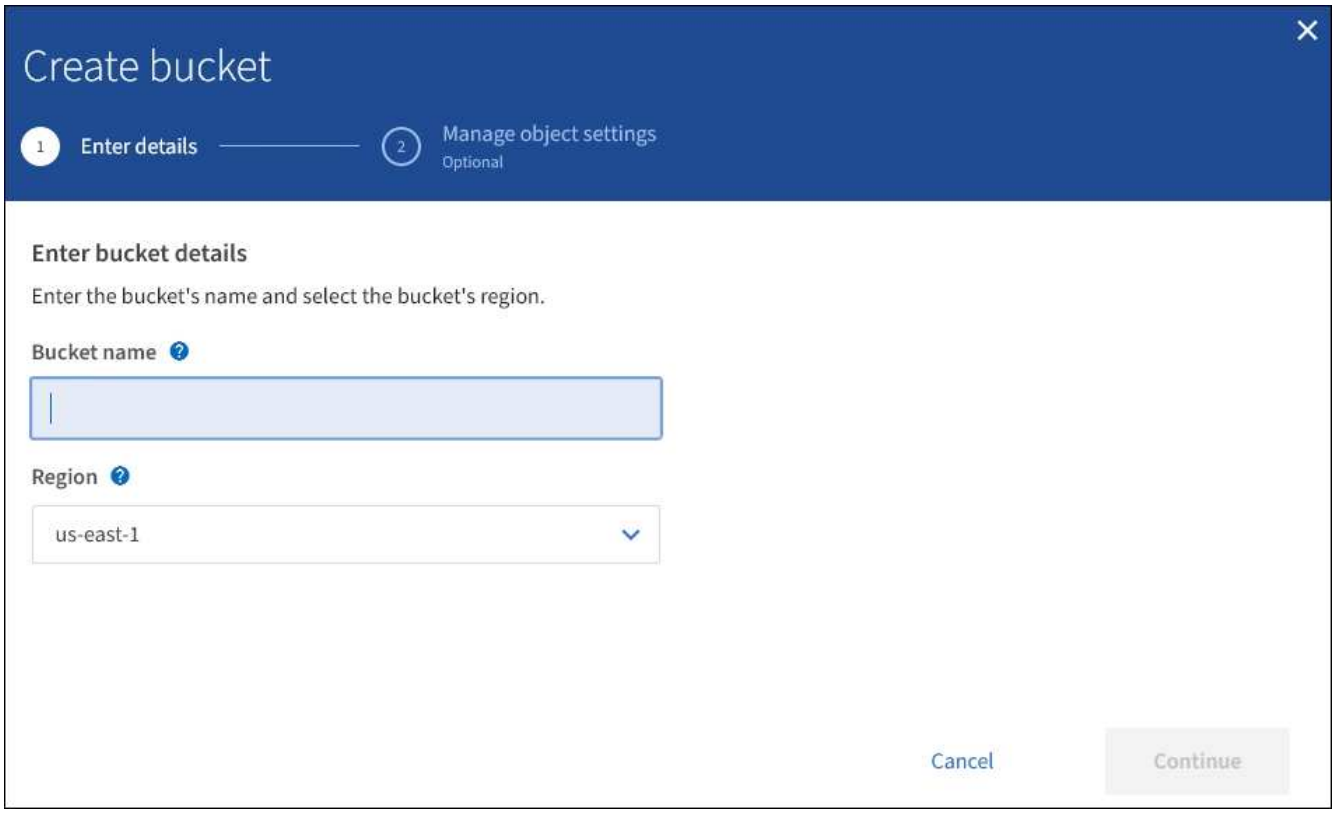
> As permissões para definir ou modificar as propriedades de bloqueio de objetos S3D de buckets ou objetos podem ser concedidas pelo política de bucket ou política de grupo.

- 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.

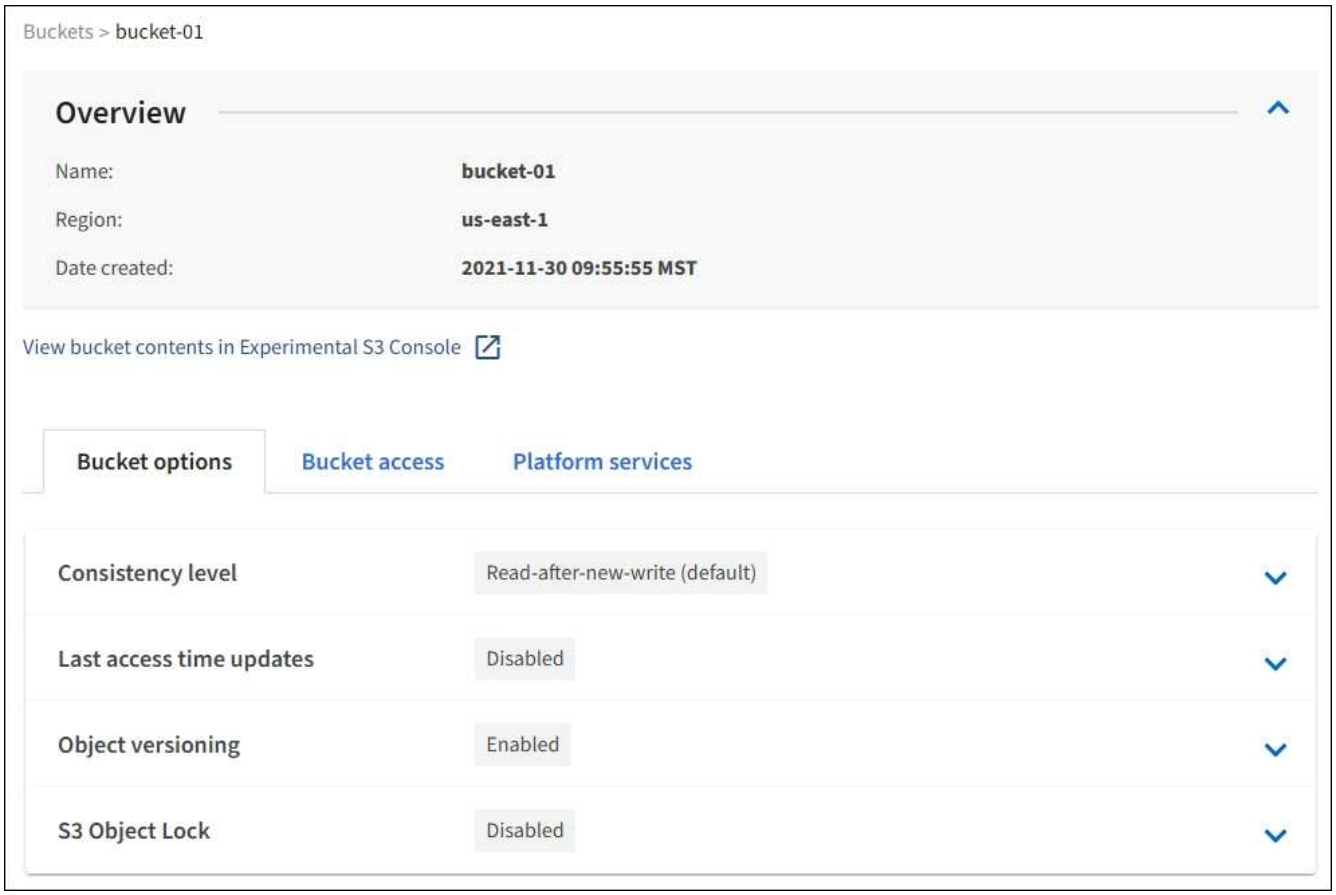
     Esta coluna não será exibida se a configuração global de bloqueio de objetos S3D estiver desativada. Esta coluna também mostra informações para quaisquer buckets em conformidade com o legado.

   - 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

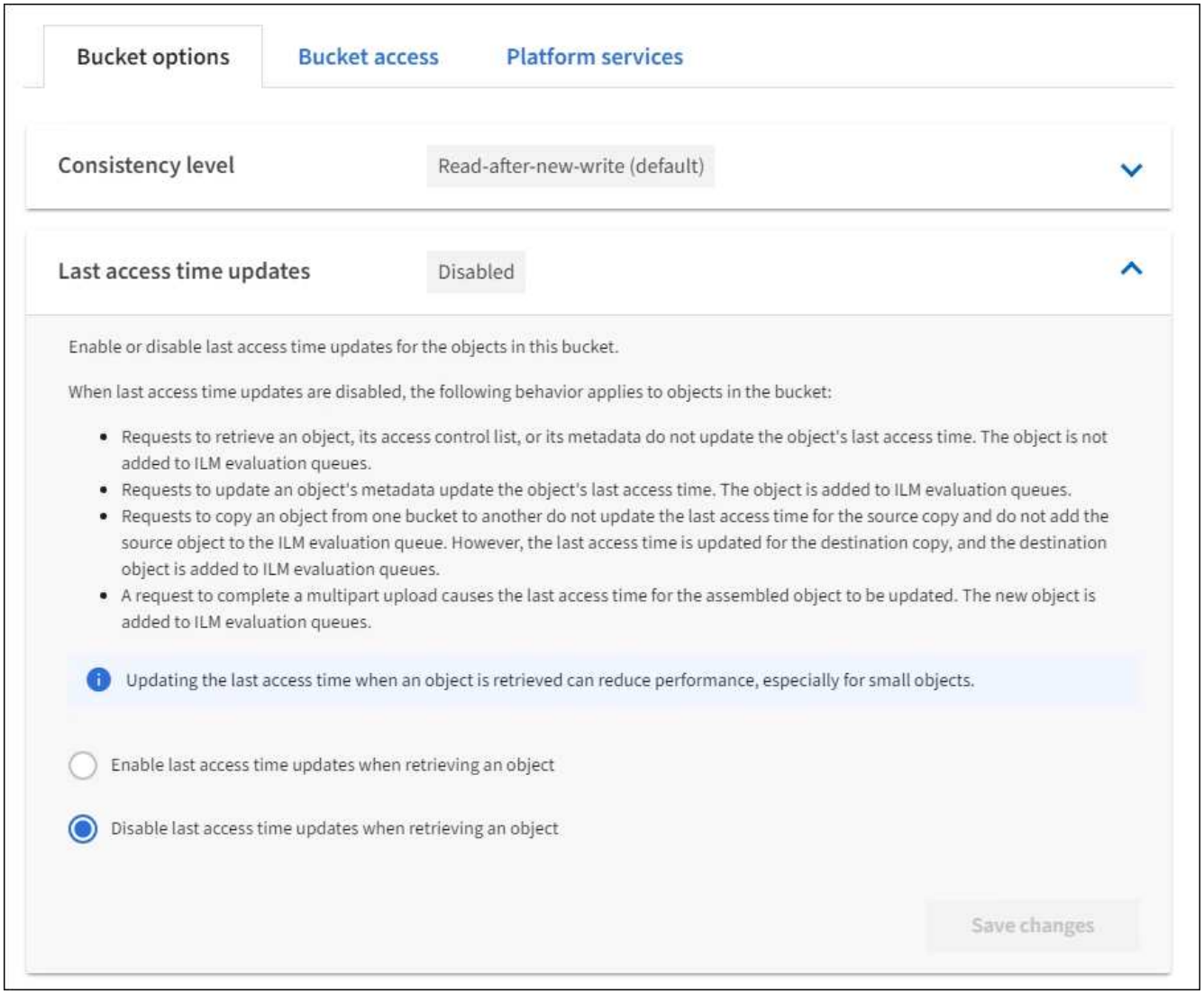
Pedido para concluir um carregamento multipart	Sim, para o objeto montado	Sim, para o objeto montado	Sim, para o objeto montado	Sim, para o objeto montado

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.

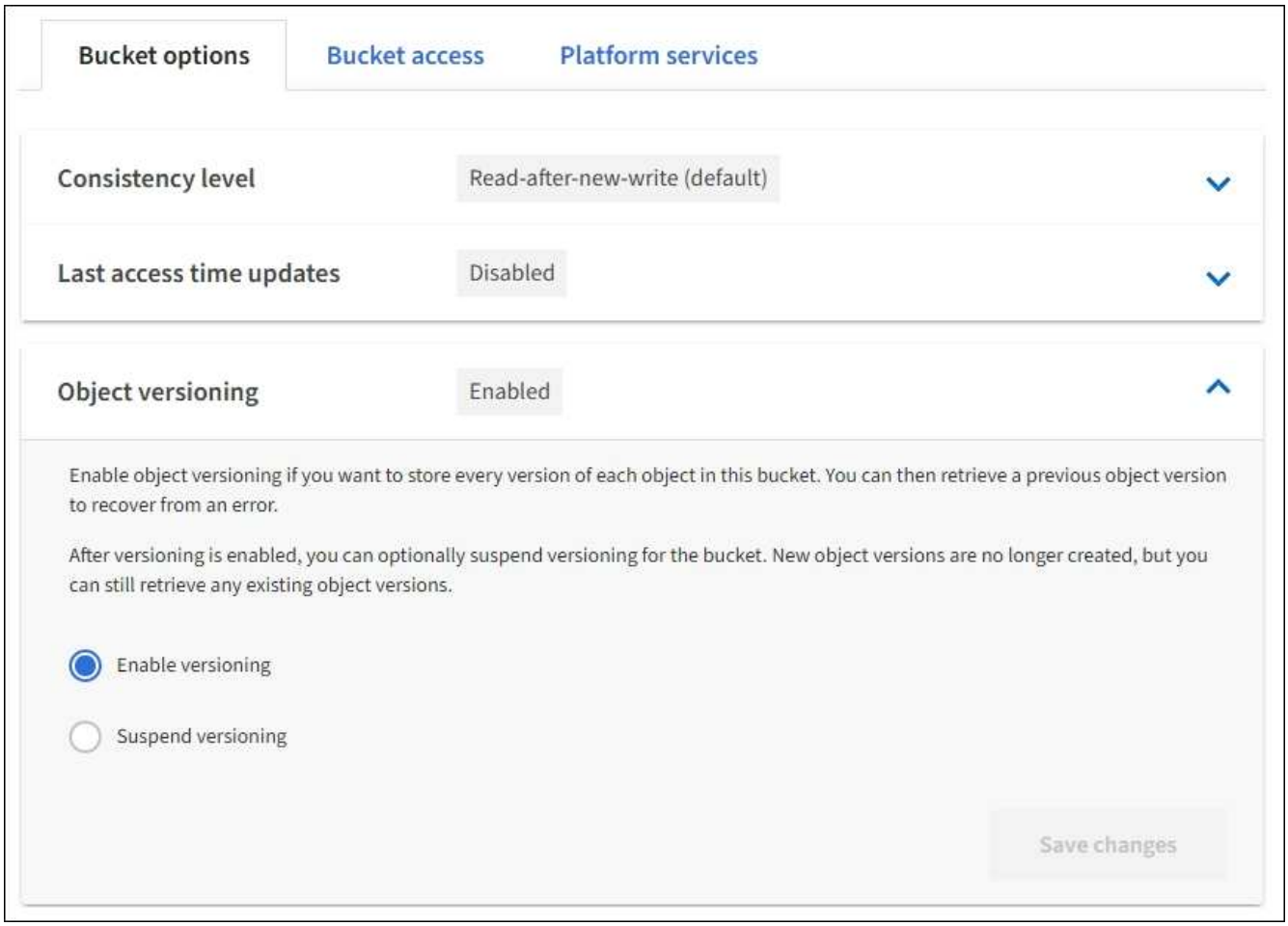
- Desativado: O controle de versão nunca foi habilitado
- Habilitado: O controle de versão está habilitado
- Suspenso: O controle de versão foi ativado anteriormente e está suspenso

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.

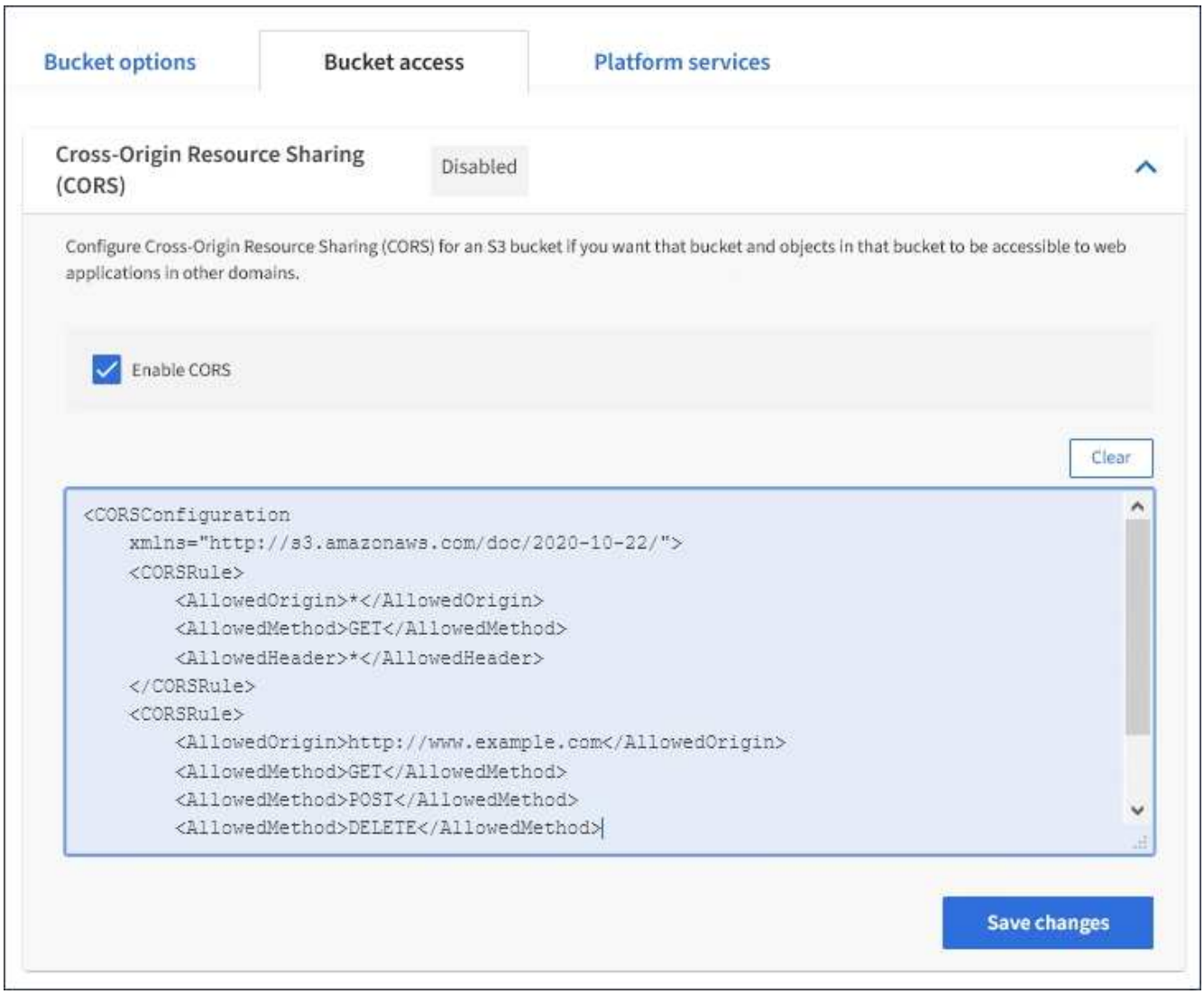
   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com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

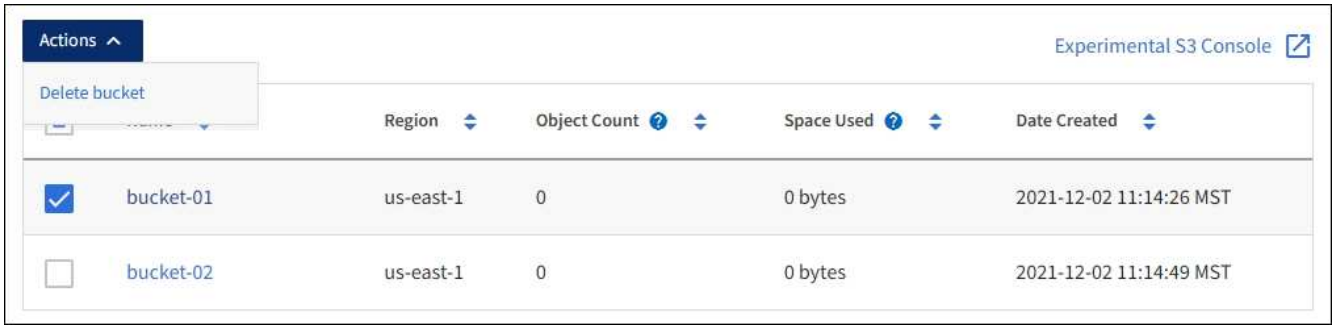
1. Selecione **STORAGE (S3)** > **Buckets**.

   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

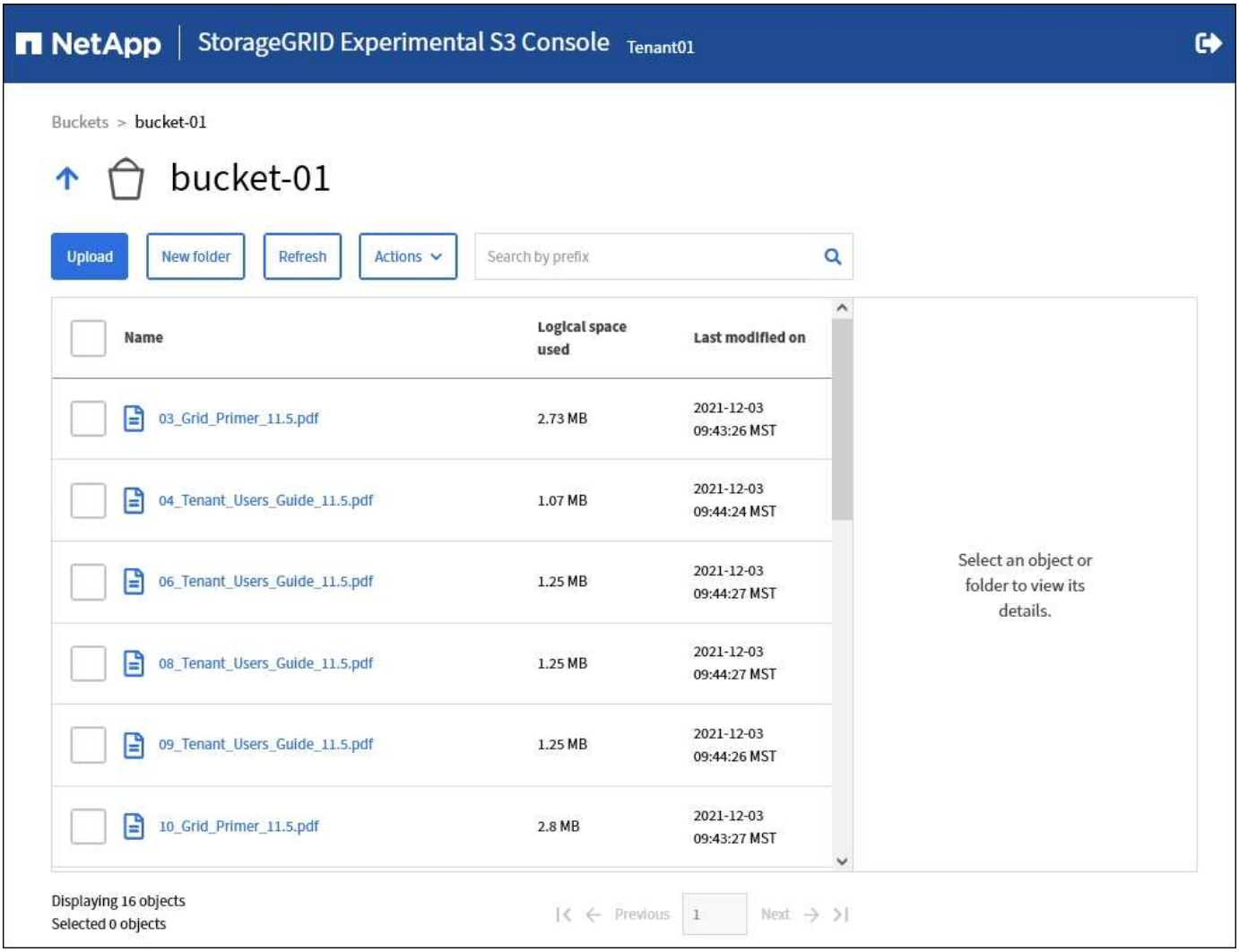
> ⓘ O console S3 não foi totalmente testado e está marcado como "experimental". Não se destina ao gerenciamento em massa de objetos ou para uso em um ambiente de produção. Os locatários só devem usar o Console S3 ao executar funções para um pequeno número de objetos, como ao carregar objetos para simular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


NetApp | StorageGRID Experimental S3 Console Tenant01
Buckets > bucket-01
bucket-01
Upload
New folder
Refresh
Actions
Search by prefix
Name
Logical space used
Last modified on
03_Grid_Primer_11.5.pdf
2.73 MB
2021-12-03 09:43:26 MST
04_Tenant_Users_Guide_11.5.pdf
1.07 MB
2021-12-03 09:44:24 MST
06_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:27 MST
08_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:27 MST
09_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:26 MST
10_Grid_Primer_11.5.pdf
2.8 MB
2021-12-03 09:43:27 MST
Select an object or folder to view its details.
Displaying 16 objects
Selected 0 objects
Previous
1
Next

Informações sobre direitos autorais

Informações sobre marcas comerciais