



Gerenciamento de buckets do S3

StorageGRID

NetApp
March 10, 2025

Índice

Gerenciamento de buckets do S3	1
Usando S3 Object Lock	1
O que é S3 Object Lock?	1
Gerenciamento de buckets em conformidade com o legado	2
S3 fluxo de trabalho Object Lock	2
Requisitos para o bloqueio de objetos S3	3
Criando um bucket S3	5
Visualização dos detalhes do balde S3	8
Alterar o nível de consistência	10
Ativar ou desativar as atualizações da última hora de acesso	13
Configurando o compartilhamento de recursos entre origens (CORS)	16
Eliminar um bucket do S3	17

Gerenciamento de buckets do S3

Se você estiver usando um locatário S3 com as permissões apropriadas, você poderá criar, exibir e excluir buckets do S3, atualizar configurações de nível de consistência, configurar o Compartilhamento de recursos entre origens (CORS), ativar e desativar as configurações de atualização da última hora de acesso e gerenciar os serviços da plataforma S3.

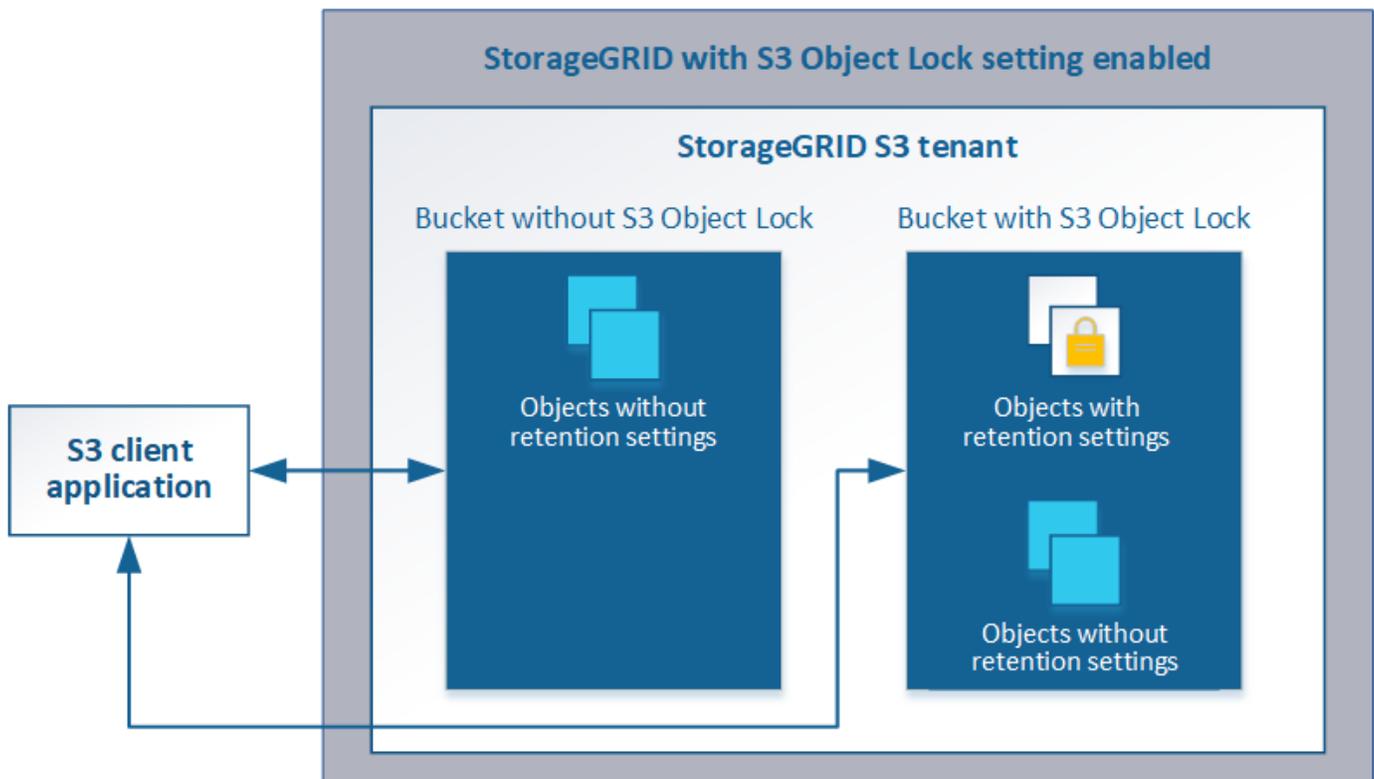
Usando S3 Object Lock

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.

Para obter detalhes sobre essas configurações, vá para ["usando o bloqueio de objetos S3"](#) em ["S3 operações e limitações suportadas pela API REST"](#).

Gerenciamento de 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.

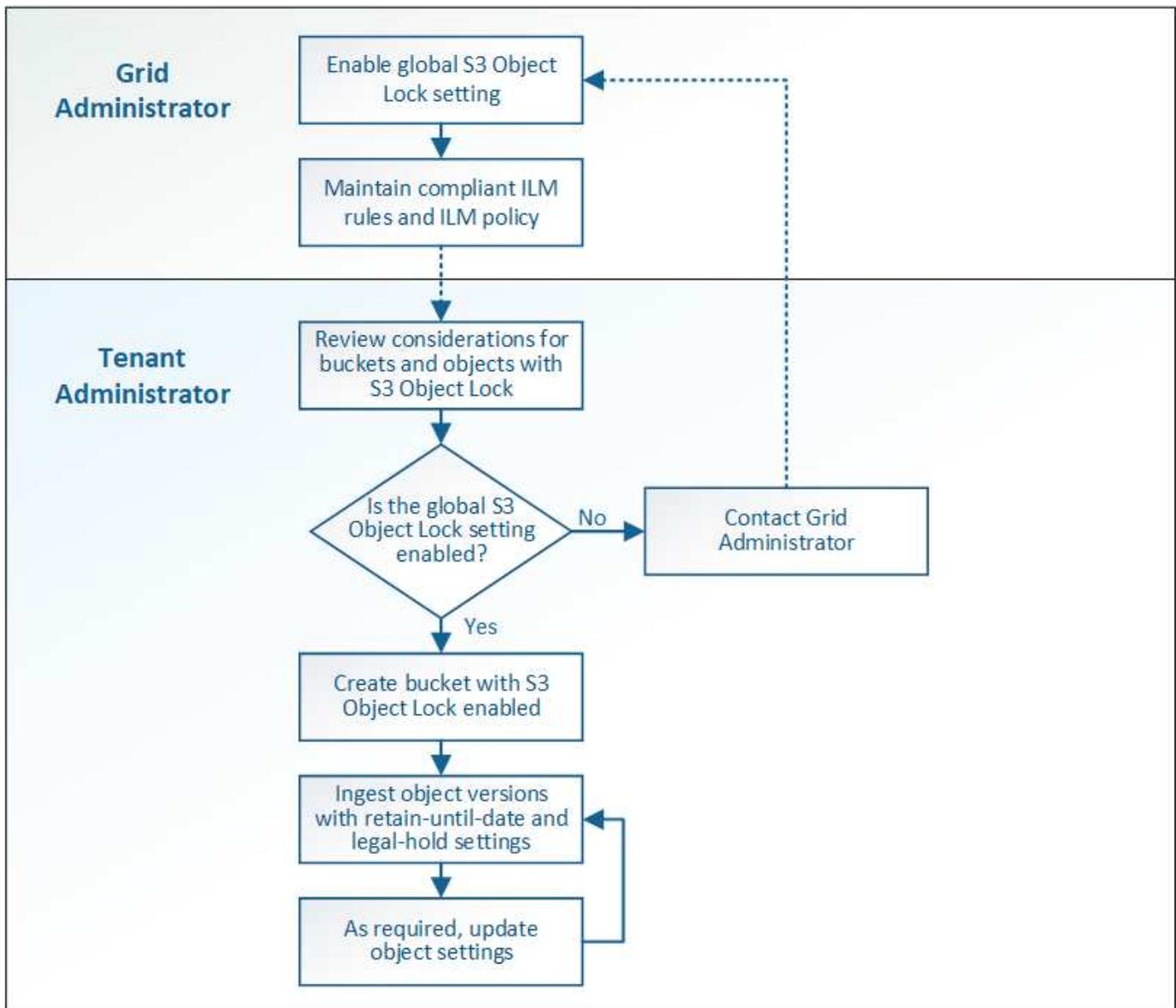
["Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"](#)

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 a política de gerenciamento do ciclo de vida das informações (ILM) seja "compatível"; ela deve atender aos requisitos dos buckets com o bloqueio de objetos 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.



Informações relacionadas

["Gerenciar objetos com ILM"](#)

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.

Buckets

Create buckets and manage bucket settings.

1 bucket

Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock  ▾	Region ▾	Object Count  ▾	Space Used  ▾	Date Created ▾
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

- 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.
- Um bucket do StorageGRID que tenha o bloqueio de objetos S3 ativado não tem um período de retenção padrão. Em vez disso, o aplicativo cliente S3 pode, opcionalmente, especificar uma data de retenção e uma configuração de retenção legal para cada versão de objeto adicionada a esse bucket.
- 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

- O aplicativo cliente S3 deve especificar configurações de retenção para cada objeto que precisa ser protegido pelo bloqueio de objetos S3.
- 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.

Criando um bucket S3

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

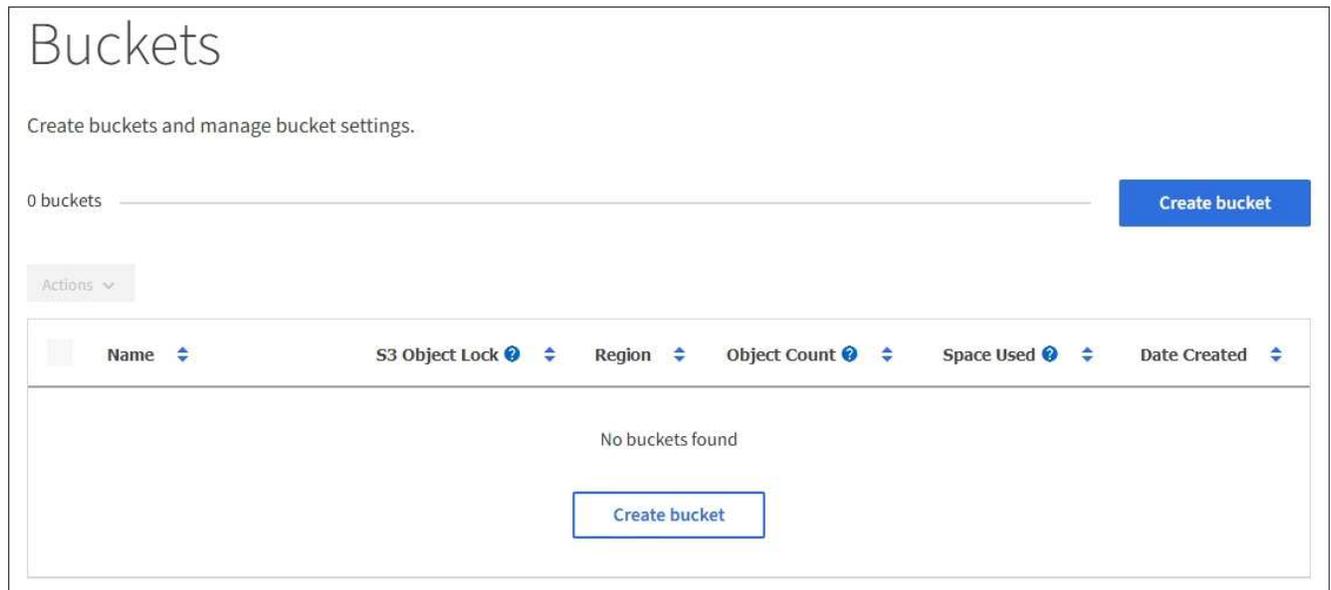
- Você deve estar conectado ao Gerenciador do Locatário usando um navegador compatível.
- Você deve pertencer a um grupo de usuários que tenha a permissão Gerenciar todos os buckets ou acesso root. Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Se você planeja criar um bucket com o bloqueio de objeto S3, a configuração global bloqueio de objeto S3 deve ter sido ativada para o sistema StorageGRID e você deve ter revisado os requisitos para buckets e objetos do bloqueio de objeto S3.

["Usando S3 Object Lock"](#)

Passos

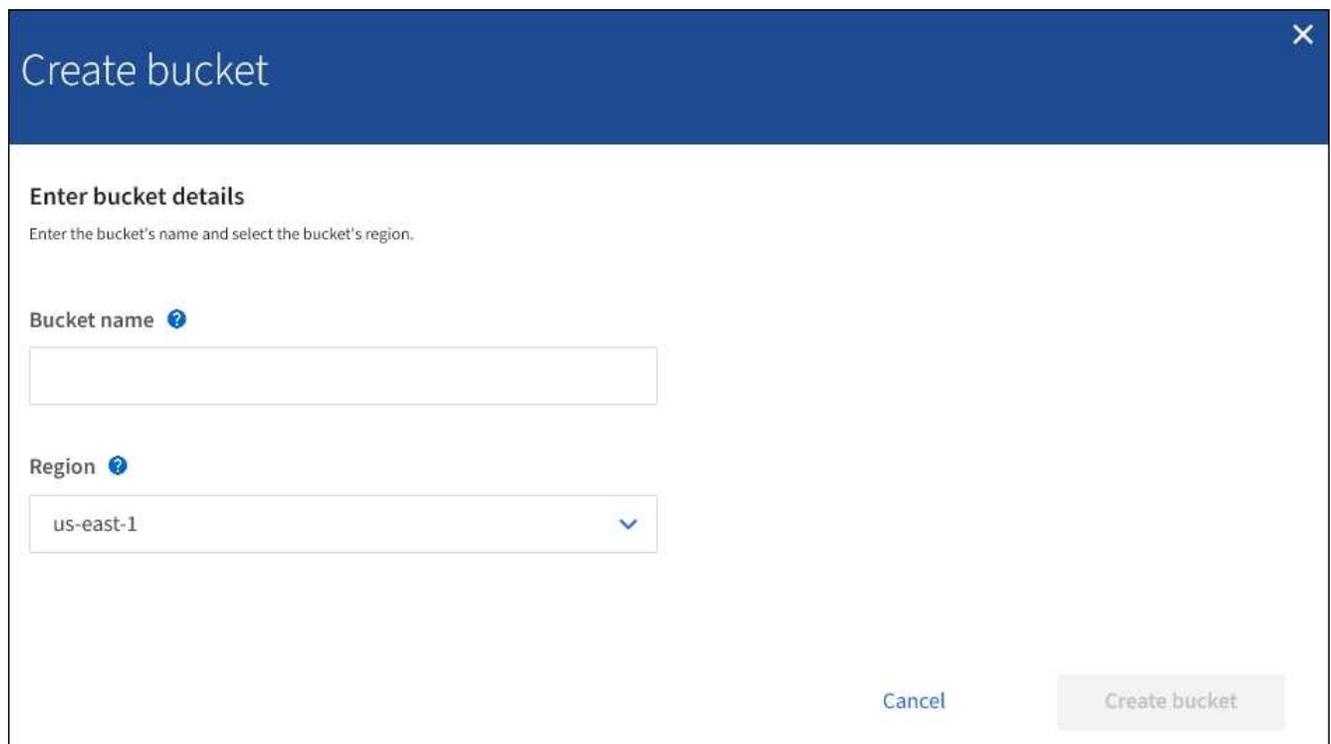
1. Selecione **STORAGE (S3) > Buckets**.

A página Buckets é exibida e lista todos os buckets que já foram criados.



2. Selecione **criar bucket**.

O assistente criar bucket é exibido.



Se a configuração global S3 Object Lock estiver ativada, Create bucket inclui uma segunda etapa para gerenciar o S3 Object Lock para o 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 caracteres.
- 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 hífen.
- 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.



Consulte a documentação do Amazon Web Services (AWS) para obter mais informações.

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 **criar bucket** ou **continuar**.

- Se a configuração global S3 Object Lock não estiver ativada, selecione **Create bucket**. O bucket é criado e adicionado à tabela na página Buckets.
- Se a configuração global S3 Object Lock estiver ativada, selecione **Continue**. O passo 2, Gerenciar bloqueio de objetos S3, aparece.

The screenshot shows a 'Create bucket' wizard with two steps: 'Enter details' (completed) and 'Manage S3 Object Lock' (optional, current step). The 'Manage S3 Object Lock' section explains that S3 Object Lock allows specifying retention and legal hold settings, and that it must be enabled at creation. Below this, there is a checkbox labeled 'Enable S3 Object Lock' which is checked. At the bottom right, there are 'Previous' and 'Create bucket' buttons.

6. Opcionalmente, marque a caixa de seleção para ativar o bloqueio de objetos S3D para este bucket.

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.



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



Se você ativar o bloqueio de objeto S3 para um bucket, o controle de versão do bucket será ativado automaticamente.

7. Selecione **criar bucket**.

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

Informações relacionadas

["Gerenciar objetos com ILM"](#)

["Entendendo a API de gerenciamento do locatário"](#)

["Use S3"](#)

Visualização dos 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 conectado ao Gerenciador do Locatário usando um navegador compatível.

Passos

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

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

Buckets

Create buckets and manage bucket settings.

2 buckets Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock	Region ▾	Object Count	Space Used	Date Created ▾
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

← Previous **1** Next →

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, conectividade de rede e status de nó.

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

É apresentada a página de detalhes do balde.

Esta página permite visualizar e editar as definições de opções de intervalo, acesso a intervalos e serviços de plataforma.

Consulte as instruções para configurar cada configuração ou serviço de plataforma.

Buckets > bucket-02

Overview

Name:	bucket-02
Region:	us-east-1
S3 Object Lock:	Disabled
Date created:	2020-11-04 14:51:59 MST

Bucket options Bucket access Platform services

Consistency level	Read-after-new-write	▼
Last access time updates	Disabled	▼

Informações relacionadas

["Alterar o nível de consistência"](#)

["Ativar ou desativar as atualizações da última hora de acesso"](#)

["Configurando o compartilhamento de recursos entre origens \(CORS\)"](#)

["Configurando a replicação do CloudMirror"](#)

["Configurando notificações de eventos"](#)

["Configurando o serviço de integração de pesquisa"](#)

Alterar o nível de consistência

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

O que você vai precisar

- Você deve estar conectado ao Gerenciador do Localitório usando um navegador compatível.
- 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 nível de consistência faz uma troca entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós e sites de storage. 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**.

Bucket options
Bucket access
Platform services

Consistency level
Read-after-new-write (default)
⤴

Change the consistency control for operations performed on the objects in the bucket. Consistency level makes a trade-off between the availability of the objects and the consistency of those objects across different Storage Nodes and sites.

In general, use the **Read-after-new-write** consistency level for your buckets. Then, if objects do not meet availability or consistency requirements, change the client application's behavior, or set the Consistency-Control header for an individual API request, which overrides the bucket setting.

- All**
Provides the highest guarantee of consistency. All nodes receive the data immediately, or the request will fail.
- Strong-global**
Guarantees read-after-write consistency for all client requests across all sites.
- Strong-site**
Guarantees read-after-write consistency for all client requests within a site.
- Read-after-new-write (default)**
Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability, and data protection guarantees.

Note: If your application attempts HEAD operations on keys that do not exist, set the Consistency Level to **Available**, unless you require AWS S3 consistency guarantees. Otherwise, a high number of 500 Internal Server errors can result if one or more Storage Nodes are unavailable.

- Available**
Behaves the same as the **Read-after-new-write** consistency level, but only provides eventual consistency for HEAD operations. Offers higher availability for HEAD operations than **Read-after-new-write** if Storage Nodes are unavailable. Differs from AWS S3 consistency guarantees for HEAD operations only.

Save changes

4. Selecione um nível de consistência para as operações realizadas nos objetos neste intervalo.

Nível 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.

Nível de consistência	Descrição
Forte local	Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.
Leitura-após-nova-gravação (padrão)	<p>Fornecer consistência de leitura após gravação para novos objetos e consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Corresponde às garantias de consistência do Amazon S3.</p> <p>Observação: se o aplicativo tentar operações DE CABEÇA em chaves que não existem, defina o nível de consistência como disponível, a menos que você exija garantias de consistência do Amazon S3. Caso contrário, um grande número de erros de servidor interno do 500 pode resultar se um ou mais nós de storage não estiverem disponíveis.</p>
Disponível (eventual consistência para OPERAÇÕES DE CABEÇA)	Comporta-se da mesma forma que o nível de consistência Read-after-new-write , mas fornece apenas consistência para operações HEAD. Oferece maior disponibilidade para OPERAÇÕES PRINCIPAIS do que leitura após nova gravação se os nós de storage não estiverem disponíveis. Difere das garantias de consistência do Amazon S3 apenas para operações PRINCIPAIS.

5. Selecione **Salvar alterações**.

Informações relacionadas

["Permissões de gerenciamento do locatário"](#)

Ativar ou desativar 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 conectado ao Gerenciador do Locatário usando um navegador compatível.
- 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.

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	<ul style="list-style-type: none"> • Não, para a cópia de origem • Sim, para a cópia de destino 	<ul style="list-style-type: none"> • Não, para a cópia de origem • Sim, para a cópia de destino 	<ul style="list-style-type: none"> • Sim, para a cópia de origem • Sim, para a cópia de destino 	<ul style="list-style-type: none"> • Sim, para a cópia de origem • Sim, para a cópia de destino
Pedido para concluir um carregamento multipart	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.

The screenshot shows the 'Bucket options' tab in the AWS S3 console. Under 'Last access time updates', the status is 'Disabled'. A yellow highlight contains the following information:

- i** Updating the last access time when an object is retrieved can reduce performance, especially for small objects.

Below this, there are two radio button options:

- Enable last access time updates when retrieving an object
- Disable last access time updates when retrieving an object

A 'Save changes' button is located at the bottom right of the configuration area.

5. Selecione **Salvar alterações**.

Informações relacionadas

["Permissões de gerenciamento do locatário"](#)

["Gerenciar objetos com ILM"](#)

Configurando o compartilhamento 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 conectado ao Gerenciador do Locatário usando um navegador compatível.
- 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**.

Bucket options | **Bucket access** | **Platform services**

Cross-Origin Resource Sharing (CORS) Disabled

Configure Cross-Origin Resource Sharing (CORS) for an S3 bucket if you want that bucket and objects in that bucket to be accessible to web applications in other domains.

Enable CORS

Clear

```
<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>
  </CORSRule>
</CORSConfiguration>
```

Save changes

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 um bucket do S3

Você pode usar o Gerenciador do Locatário para excluir um bucket do S3 vazio.

O que você vai precisar

- Você deve estar conectado ao Gerenciador do Locatário usando um navegador compatível.
- 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

Estas instruções descrevem como excluir um bucket do S3 usando o Gerenciador do locatário. Você também pode excluir buckets do S3 usando a API de gerenciamento do locatário ou a API REST do S3.

Não é possível excluir um bucket do S3 se ele contiver objetos ou versões de objetos não atuais. Para obter informações sobre como objetos com versão S3 são excluídos, consulte as 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.

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

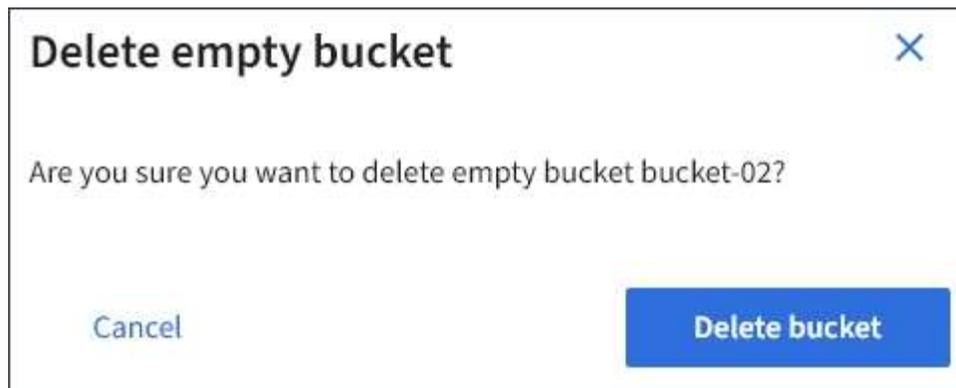
2. Marque a caixa de seleção do intervalo vazio que deseja excluir.

O menu ações está ativado.

3. No menu ações, selecione **Excluir bucket vazio**.

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input checked="" type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

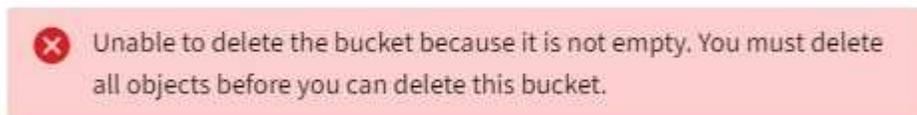
É apresentada uma mensagem de confirmação.



4. Se tiver certeza de que deseja excluir o intervalo, selecione **Excluir intervalo**.

O StorageGRID confirma que o balde está vazio e, em seguida, elimina o balde. Esta operação pode demorar alguns minutos.

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



Informações relacionadas

["Gerenciar objetos com ILM"](#)

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.