Usar bloqueio de objeto S3

StorageGRID software

NetApp
December 03, 2025

Índice

Usar bloqueio de objeto S3 . . . 1
- Gerenciar objetos com o S3 Object Lock . . . 1
  - O que é o S3 Object Lock? . . . 1
  - Comparando o bloqueio de objeto S3 com a conformidade legada . . . 2
- Tarefas de bloqueio de objeto S3 . . . 4
- Requisitos para bloqueio de objeto S3 . . . 5
  - Requisitos para usar a configuração global de bloqueio de objeto do S3 . . . 5
  - Requisitos para regras ILM compatíveis . . . 5
  - Requisitos para políticas de ILM . . . 6
  - Requisitos para buckets com bloqueio de objeto S3 habilitado . . . 6
  - Requisitos para objetos em buckets com bloqueio de objeto S3 habilitado . . . 6
  - Ciclo de vida de objetos em buckets com bloqueio de objeto S3 habilitado . . . 6
- Habilitar bloqueio de objeto S3 globalmente . . . 7
- Resolver erros de consistência ao atualizar o bloqueio de objeto S3 ou a configuração de conformidade herdada . . . 8

Usar bloqueio de objeto S3

Gerenciar objetos com o S3 Object Lock

Como administrador de grade, você pode habilitar o S3 Object Lock para seu sistema StorageGRID e implementar uma política de ILM compatível para ajudar a garantir que objetos em buckets S3 específicos não sejam excluídos ou substituídos por um período de tempo especificado.

O que é o S3 Object Lock?

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

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

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

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

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

Efetivamente, todos os objetos recém-ingeridos têm configurações de retenção quando a retenção padrão é configurada. Objetos existentes sem configurações de retenção de objetos permanecem inalterados.

Modos de retenção

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

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

Configurações de retenção para versões de objeto

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

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

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

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

Configuração de retenção padrão para buckets

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

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

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

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

Comparando o bloqueio de objeto S3 com a conformidade legada

O S3 Object Lock substitui o recurso de conformidade que estava disponível em versões anteriores do StorageGRID . Como o recurso S3 Object Lock está em conformidade com os requisitos do Amazon S3, ele descontinua o recurso proprietário StorageGRID Compliance, que agora é chamado de "Conformidade herdada".

> ⓘ A configuração global de Conformidade está obsoleta. Se você habilitou essa configuração usando uma versão anterior do StorageGRID, a configuração de Bloqueio de Objeto do S3 será habilitada automaticamente. Você pode continuar a usar o StorageGRID para gerenciar as configurações de buckets compatíveis existentes; no entanto, não é possível criar novos buckets compatíveis. Para mais detalhes, veja "Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5" .

Se você usou o recurso de conformidade legado em uma versão anterior do StorageGRID, consulte a tabela a seguir para saber como ele se compara ao recurso de bloqueio de objeto do S3 no StorageGRID.

	Bloqueio de Objeto S3	Conformidade (legado)
Como o recurso é habilitado globalmente?	No Grid Manager, selecione **CONFIGURAÇÃO** > **Sistema** > **Bloqueio de Objeto S3**.	Não é mais suportado.
Como o recurso é habilitado para um bucket?	Os usuários devem habilitar o bloqueio de objeto do S3 ao criar um novo bucket usando o Tenant Manager, a Tenant Management API ou a S3 REST API.	Não é mais suportado.
O controle de versão de bucket é suportado?	Sim. O controle de versão do bucket é necessário e é habilitado automaticamente quando o S3 Object Lock é habilitado para o bucket.	Não.
Como a retenção de objetos é definida?	Os usuários podem definir uma data de retenção para cada versão do objeto ou podem definir um período de retenção padrão para cada bucket.	Os usuários devem definir um período de retenção para todo o bucket. O período de retenção se aplica a todos os objetos no bucket.
O período de retenção pode ser alterado?	• No modo de conformidade, o período de retenção até a data para uma versão do objeto pode ser aumentado, mas nunca diminuído. • No modo de governança, usuários com permissões especiais podem diminuir ou até mesmo remover as configurações de retenção de um objeto.	O período de retenção de um bucket pode ser aumentado, mas nunca diminuído.
Onde a retenção legal é controlada?	Os usuários podem colocar ou retirar uma retenção legal para qualquer versão de objeto no bucket.	Uma retenção legal é colocada no bucket e afeta todos os objetos no bucket.

	Bloqueio de Objeto S3	Conformidade (legado)
Quando os objetos podem ser excluídos?	• No modo de conformidade, uma versão do objeto pode ser excluída após a data de retenção ser atingida, supondo que o objeto não esteja sob retenção legal. • No modo de governança, usuários com permissões especiais podem excluir um objeto antes que sua data de retenção seja atingida, supondo que o objeto não esteja sob retenção legal.	Um objeto pode ser excluído após o término do período de retenção, desde que o bucket não esteja sob retenção legal. Os objetos podem ser excluídos automática ou manualmente.
A configuração do ciclo de vida do bucket é suportada?	Sim	Não

Tarefas de bloqueio de objeto S3

Como administrador de grade, você deve coordenar-se estreitamente com os usuários locatários para garantir que os objetos sejam protegidos de uma maneira que atenda aos seus requisitos de retenção.

A aplicação das configurações do locatário na grade pode levar 15 minutos ou mais, dependendo da conectividade da rede, do status do nó e das operações do Cassandra.

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

Administrador de rede

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

Usuário locatário

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

    - Período de retenção padrão: deve ser menor ou igual ao período máximo de retenção definido pelo administrador da grade.
- Use o aplicativo cliente S3 para adicionar objetos e, opcionalmente, definir a retenção específica do objeto:
    - Modo de retenção. Governança ou conformidade, se permitido pelo administrador da rede.
    - Data de retenção: deve ser menor ou igual ao que é permitido pelo período máximo de retenção definido pelo administrador da grade.

Requisitos para bloqueio de objeto S3

Você deve revisar os requisitos para habilitar a configuração global do S3 Object Lock, os requisitos para criar regras e políticas de ILM compatíveis e as restrições que o StorageGRID impõe aos buckets e objetos que usam o S3 Object Lock.

Requisitos para usar a configuração global de bloqueio de objeto do S3

- Você deve habilitar a configuração global de Bloqueio de Objeto do S3 usando o Grid Manager ou a API de Gerenciamento de Grade antes que qualquer locatário do S3 possa criar um bucket com o Bloqueio de Objeto do S3 habilitado.
- Habilitar a configuração global de Bloqueio de Objeto S3 permite que todas as contas de locatários do S3 criem buckets com o Bloqueio de Objeto S3 habilitado.
- Depois de habilitar a configuração global de Bloqueio de Objeto do S3, você não poderá desabilitá-la.
- Não é possível habilitar o bloqueio de objeto S3 global, a menos que a regra padrão em todas as políticas ativas do ILM seja *compatível* (ou seja, a regra padrão deve estar em conformidade com os requisitos de buckets com o bloqueio de objeto S3 habilitado).
- Quando a configuração global de Bloqueio de Objeto S3 estiver habilitada, você não poderá criar uma nova política de ILM ou ativar uma política de ILM existente, a menos que a regra padrão na política esteja em conformidade. Depois que a configuração global de Bloqueio de Objeto do S3 for habilitada, as páginas de regras e políticas do ILM indicam quais regras do ILM são compatíveis.

Requisitos para regras ILM compatíveis

Se você quiser habilitar a configuração global de Bloqueio de Objeto do S3, deverá garantir que a regra padrão em todas as políticas ativas do ILM esteja em conformidade. Uma regra compatível satisfaz os requisitos de ambos os buckets com o Bloqueio de Objeto S3 habilitado e de quaisquer buckets existentes que tenham a Conformidade herdada habilitada:

- Ele deve criar pelo menos duas cópias de objetos replicados ou uma cópia codificada para eliminação.
- Essas cópias devem existir nos Nós de Armazenamento durante toda a duração de cada linha nas instruções de posicionamento.
- Cópias de objetos não podem ser salvas em um pool de armazenamento em nuvem.
- Pelo menos uma linha das instruções de posicionamento deve começar no dia 0, usando **Horário de ingestão** como horário de referência.
- Pelo menos uma linha das instruções de posicionamento deve ser "para sempre".

Requisitos para políticas de ILM

Quando a configuração global de Bloqueio de Objeto do S3 está habilitada, as políticas ativas e inativas do ILM podem incluir regras compatíveis e não compatíveis.

- A regra padrão em uma política de ILM ativa ou inativa deve ser compatível.
- Regras não compatíveis só se aplicam a objetos em buckets que não têm o Bloqueio de Objeto do S3 habilitado ou que não têm o recurso de Conformidade legado habilitado.
- Regras de conformidade podem ser aplicadas a objetos em qualquer bucket; o bloqueio de objeto S3 ou a conformidade herdada não precisam ser habilitados para o bucket.

"Exemplo de uma política de ILM compatível para bloqueio de objeto S3"

Requisitos para buckets com bloqueio de objeto S3 habilitado

- Se a configuração global do S3 Object Lock estiver habilitada para o sistema StorageGRID , você poderá usar o Tenant Manager, a Tenant Management API ou a S3 REST API para criar buckets com o S3 Object Lock habilitado.
- Se você planeja usar o S3 Object Lock, deverá habilitar o S3 Object Lock ao criar o bucket. Não é possível habilitar o S3 Object Lock para um bucket existente.
- Quando o S3 Object Lock é habilitado para um bucket, o StorageGRID habilita automaticamente o controle de versão para esse bucket. Não é possível desabilitar o bloqueio de objeto do S3 ou suspender o controle de versão do bucket.
- Opcionalmente, você pode especificar um modo de retenção padrão e um período de retenção para cada bucket usando o Tenant Manager, a Tenant Management API ou a S3 REST API. As configurações de retenção padrão do bucket se aplicam somente a novos objetos adicionados ao bucket que não têm suas próprias configurações de retenção. Você pode substituir essas configurações padrão especificando um modo de retenção e retenção até a data para cada versão do objeto quando ele for carregado.
- A configuração do ciclo de vida do bucket é suportada para buckets com o S3 Object Lock habilitado.
- A replicação do CloudMirror não é suportada para buckets com S3 Object Lock habilitado.

Requisitos para objetos em buckets com bloqueio de objeto S3 habilitado

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

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

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

1. **Ingestão de objetos**

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

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

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

2. **Retenção e exclusão de objetos**

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

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

Informações relacionadas

- "Criar um bucket S3"
- "Atualizar retenção padrão do bloqueio de objeto S3"
- "Use a API REST do S3 para configurar o bloqueio de objeto do S3"
- "Exemplo 7: Política ILM compatível para bloqueio de objeto S3"

Habilitar bloqueio de objeto S3 globalmente

Se uma conta de locatário do S3 precisar estar em conformidade com requisitos regulatórios ao salvar dados de objeto, você deverá habilitar o Bloqueio de Objeto do S3 para todo o seu sistema StorageGRID . Habilitar a configuração global do S3 Object Lock permite que qualquer usuário locatário do S3 crie e gerencie buckets e objetos com o S3 Object Lock.

Antes de começar

- Você tem o"Permissão de acesso root" .
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você revisou o fluxo de trabalho do S3 Object Lock e entende as considerações.
- Você confirmou que a regra padrão na política ILM ativa é compatível. Ver"Criar uma regra ILM padrão" para mais detalhes.

Sobre esta tarefa

Um administrador de grade deve habilitar a configuração global de Bloqueio de Objeto S3 para permitir que usuários locatários criem novos buckets que tenham o Bloqueio de Objeto S3 habilitado. Depois que essa configuração for ativada, ela não poderá ser desativada.

Revise as configurações de conformidade dos locatários existentes depois de habilitar a configuração global de Bloqueio de Objeto do S3. Quando você habilita essa configuração, as configurações por locatário do S3 Object Lock dependem da versão do StorageGRID no momento em que o locatário foi criado.

A configuração global de Conformidade está obsoleta. Se você habilitou essa configuração usando uma versão anterior do StorageGRID, a configuração de Bloqueio de Objeto do S3 será habilitada automaticamente. Você pode continuar a usar o StorageGRID para gerenciar as configurações de buckets compatíveis existentes; no entanto, não é possível criar novos buckets compatíveis. Para mais detalhes, veja "Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5" .

Passos

1. Selecione **CONFIGURAÇÃO** > **Sistema** > **Bloqueio de Objeto S3**.

   A página Configurações de bloqueio de objeto do S3 é exibida.

2. Selecione **Ativar bloqueio de objeto S3**.
3. Selecione **Aplicar**.

   Uma caixa de diálogo de confirmação é exibida e lembra que não é possível desabilitar o S3 Object Lock depois que ele for habilitado.

4. Se você tiver certeza de que deseja habilitar permanentemente o S3 Object Lock para todo o seu sistema, selecione **OK**.

   Quando você seleciona **OK**:

   - Se a regra padrão na política ILM ativa estiver em conformidade, o Bloqueio de Objeto S3 agora estará habilitado para toda a grade e não poderá ser desabilitado.
   - Se a regra padrão não for compatível, um erro será exibido. Você deve criar e ativar uma nova política de ILM que inclua uma regra compatível como regra padrão. Selecione **OK**. Em seguida, crie uma nova política, simule-a e ative-a. Ver"Criar política de ILM" para obter instruções.

Resolver erros de consistência ao atualizar o bloqueio de objeto S3 ou a configuração de conformidade herdada

Se um site de data center ou vários nós de armazenamento em um site ficarem indisponíveis, talvez seja necessário ajudar os usuários do locatário do S3 a aplicar alterações no bloqueio de objeto do S3 ou na configuração de conformidade herdada.

Usuários locatários que têm buckets com o Bloqueio de Objeto S3 (ou Conformidade herdada) habilitado podem alterar determinadas configurações. Por exemplo, um usuário locatário que utiliza o S3 Object Lock pode precisar colocar uma versão do objeto em retenção legal.

Quando um usuário locatário atualiza as configurações de um bucket do S3 ou uma versão de objeto, o StorageGRID tenta atualizar imediatamente os metadados do bucket ou do objeto na grade. Se o sistema não conseguir atualizar os metadados porque um site de data center ou vários nós de armazenamento não estão disponíveis, ele retornará um erro:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Para resolver esse erro, siga estas etapas:

1. Tente tornar todos os nós de armazenamento ou sites disponíveis novamente o mais rápido possível.
2. Se você não conseguir disponibilizar nós de armazenamento suficientes em cada site, entre em contato com o suporte técnico, que pode ajudar você a recuperar nós e garantir que as alterações sejam aplicadas de forma consistente em toda a grade.
3. Depois que o problema subjacente for resolvido, lembre o usuário locatário de tentar novamente as alterações de configuração.

Informações relacionadas

- "Use uma conta de inquilino"
- "Usar API REST do S3"
- "Recuperar e manter"

Informações sobre direitos autorais

Informações sobre marcas comerciais