Use S3 Object Lock com ILM

StorageGRID

NetApp
October 03, 2025

Índice

Use S3 Object Lock com ILM

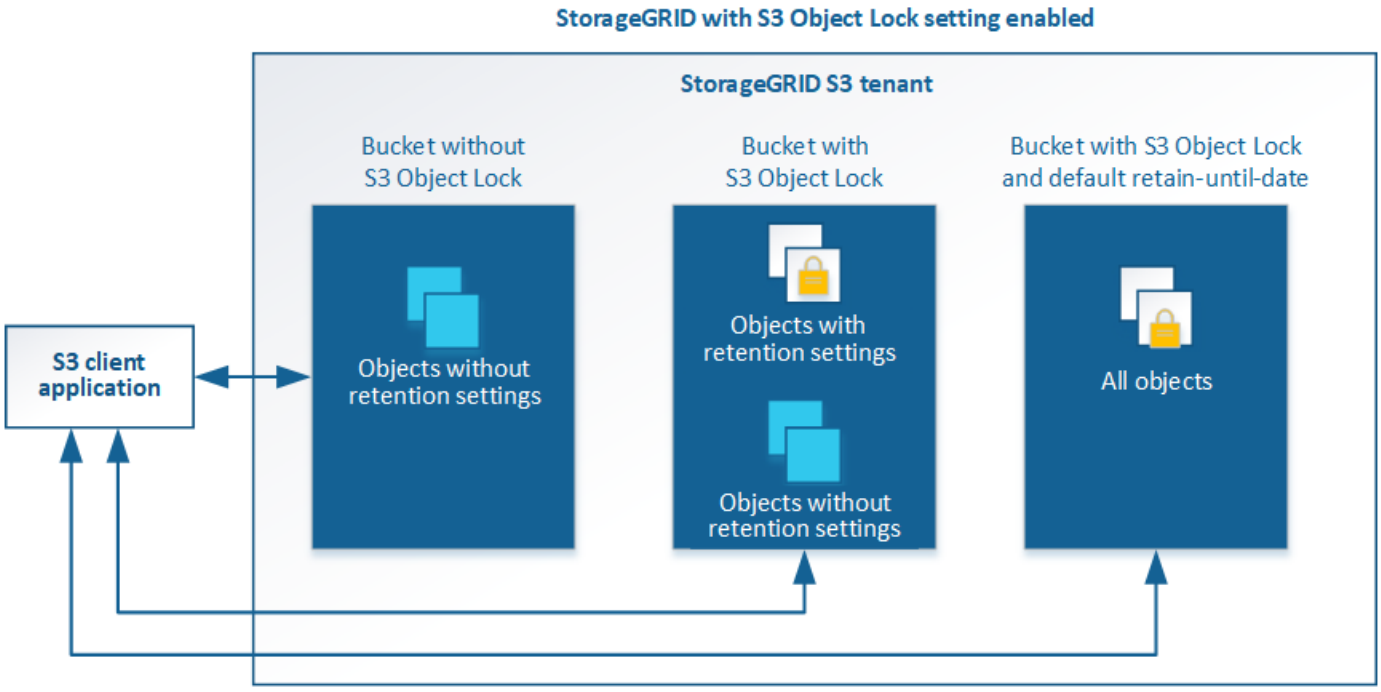
Gerencie objetos com o S3 Object Lock

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

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. Além disso, cada bucket com o bloqueio de objetos S3 ativado pode, opcionalmente, ter um modo de retenção padrão e um período de retenção, que se aplicam se objetos forem adicionados ao bucket sem suas próprias configurações de retenção.



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 as configurações de retenção de objetos, vá para Use o bloqueio de objetos S3D..

Para obter detalhes sobre as configurações padrão de retenção do balde, vá para Use retenção padrão do bucket do bloqueio de objetos S3.

Comparação do S3 Object Lock com a conformidade legada

O bloqueio de objetos S3 substitui o recurso de conformidade que estava disponível em versões anteriores do StorageGRID. Como o recurso de bloqueio de objetos S3 está em conformidade com os requisitos do Amazon S3, ele deprecia o recurso proprietário de conformidade do StorageGRID, que agora é conhecido como ""conformidade legada"".

Se você ativou anteriormente a configuração de conformidade global, a configuração global S3 Object Lock foi ativada automaticamente. Os usuários do locatário não poderão mais criar novos buckets com a conformidade ativada. No entanto, conforme necessário, os usuários do locatário podem continuar a usar e gerenciar quaisquer buckets em conformidade existentes, o que inclui a execução das seguintes tarefas:

- Inserir novos objetos em um bucket existente que tenha a conformidade legada habilitada.
- Aumento do período de retenção de um bucket existente que tem a conformidade legada habilitada.
- Alterar a configuração de exclusão automática para um bucket existente que tenha conformidade legada ativada.
- Colocar uma retenção legal em um bucket existente que tenha a conformidade legada habilitada.
- Levantar uma retenção legal.

```
https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"^]Consulte para obter instruções.
```

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 bloqueio de objetos S3 no StorageGRID.

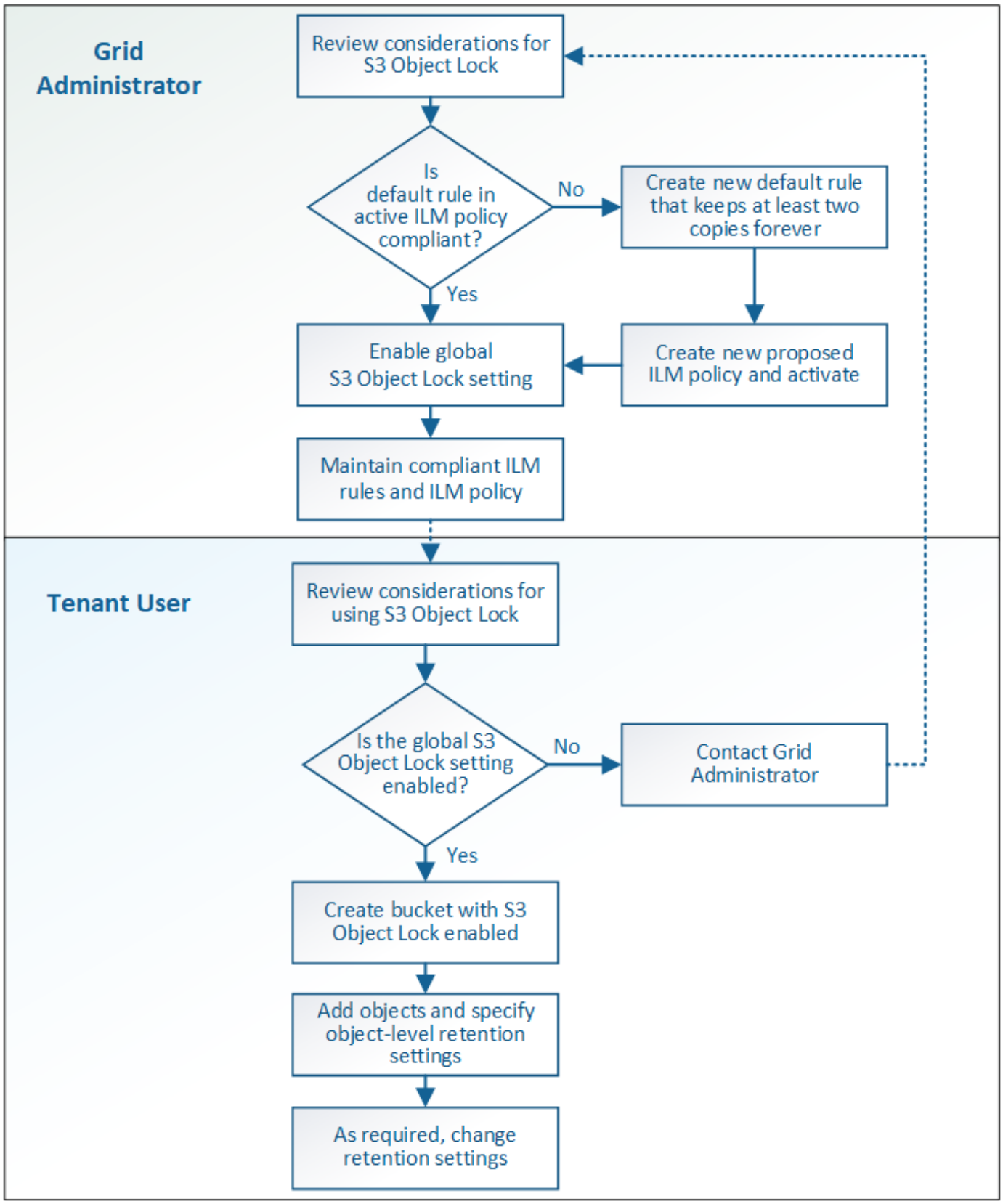
	S3 bloqueio de objetos (novo)	Conformidade (legado)
Como o recurso é ativado globalmente?	No Gerenciador de Grade, selecione **CONFIGURATION** > **System** > **S3 Object Lock**.	Já não é suportado. **Observação:** se você ativou a configuração de conformidade global usando uma versão anterior do StorageGRID, a configuração bloqueio de objeto S3 será ativada no StorageGRID 11,6. Você pode continuar usando o StorageGRID para gerenciar as configurações dos buckets em conformidade existentes. No entanto, não é possível criar novos buckets em conformidade.
Como o recurso está habilitado para um bucket?	Os usuários devem habilitar o bloqueio de objeto S3 ao criar um novo bucket usando o Gerenciador de locatário, a API de gerenciamento de locatário ou a API REST S3.	Os usuários não podem mais criar novos buckets com a conformidade ativada. No entanto, eles podem continuar adicionando novos objetos aos buckets em conformidade existentes.
O controle de versão do bucket é suportado?	Sim. O controle de versão do bucket é necessário e é ativado automaticamente quando o bloqueio de objetos S3 é ativado para o bucket.	Não. O recurso de conformidade legado não permite o controle de versão do bucket.
Como a retenção de objetos é definida?	Os usuários podem definir uma data de retenção até cada versão do objeto.	Os usuários devem definir um período de retenção para todo o bucket. O período de retenção aplica-se a todos os objetos no balde.
Um bucket pode ter configurações padrão para retenção e retenção legal?	Sim. Os buckets do StorageGRID que têm o bloqueio de objeto S3 ativado podem ter um período de retenção padrão que é aplicado a versões de objetos que não têm suas próprias configurações de retenção especificadas durante a ingestão.	Sim
O período de retenção pode ser alterado?	A data de retenção até uma versão de objeto pode ser aumentada, mas nunca diminuída.	O período de retenção do balde pode ser aumentado, mas nunca diminuído.

	S3 bloqueio de objetos (novo)	Conformidade (legado)
Onde é controlada a guarda legal?	Os usuários podem colocar uma retenção legal ou levantar uma retenção legal para qualquer versão de objeto no bucket.	Uma retenção legal é colocada no balde e afeta todos os objetos no balde.
Quando os objetos podem ser excluídos?	Uma versão de objeto pode ser excluída após a data de retenção ser alcançada, assumindo que o objeto não está sob retenção legal.	Um objeto pode ser excluído após o período de retenção expirar, supondo que o intervalo não esteja sob retenção legal. Os objetos podem ser excluídos automaticamente ou manualmente.
A configuração do ciclo de vida do bucket é suportada?	Sim	Não

Fluxo de trabalho para S3 Object Lock

Como administrador de grade, você deve coordenar estreitamente com os usuários do locatário para garantir que os objetos estejam protegidos de uma maneira que atenda aos requisitos de retenção.

O diagrama de fluxo de trabalho mostra as etapas de alto nível para usar o bloqueio de objetos S3D. Estas etapas são executadas pelo administrador da grade e pelos usuários do locatário.



Tarefas de administração de grade

Como mostra o diagrama de fluxo de trabalho, um administrador de grade deve executar duas tarefas de alto nível antes que os usuários de S3 locatários possam usar o bloqueio de objeto S3:

1. Crie pelo menos uma regra ILM compatível e torne essa regra a regra padrão na política ILM ativa.
2. Ative a configuração global de bloqueio de objetos S3D para todo o sistema StorageGRID.

Tarefas do usuário do locatário

Depois que a configuração global S3 Object Lock for ativada, os locatários podem executar estas tarefas:

1. Crie buckets que tenham o bloqueio de objeto S3 ativado.
2. Especifique as configurações de retenção padrão para o bucket, que são aplicadas a objetos adicionados ao bucket que não especificam suas próprias configurações de retenção.
3. Adicione objetos a esses buckets e especifique períodos de retenção no nível do objeto e configurações de retenção legal.
4. Conforme necessário, atualize um período de retenção ou altere a configuração de retenção legal para um objeto individual.

Informações relacionadas

- Use uma conta de locatário
- Use S3
- Use retenção padrão do bucket do bloqueio de objetos S3

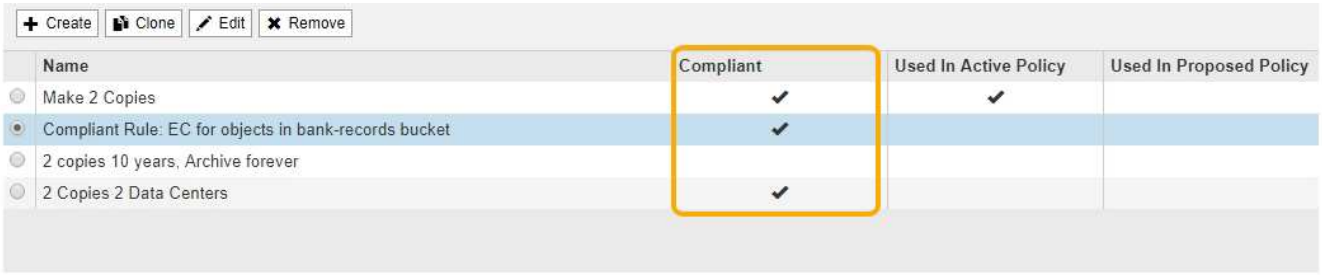
Requisitos para o bloqueio de objetos S3

Você deve analisar os requisitos para ativar a configuração global de bloqueio de objetos S3, os requisitos para criar regras de ILM e políticas de ILM compatíveis e as restrições que o StorageGRID coloca em buckets e objetos que usam o bloqueio de objetos S3.

Requisitos para usar a configuração global S3 Object Lock

- Você deve ativar a configuração global de bloqueio de objetos S3 usando o Gerenciador de Grade ou a API de Gerenciamento de Grade antes que qualquer locatário S3 possa criar um bucket com o bloqueio de objetos S3 ativado.
- Ativar a configuração global S3 Object Lock permite que todas as contas de locatário do S3 criem buckets com o S3 Object Lock ativado.
- Depois de ativar a definição global S3 Object Lock, não pode desativar a definição.
- Você não pode ativar o bloqueio de objetos S3 global a menos que a regra padrão na política ILM ativa seja *compliant* (ou seja, a regra padrão deve cumprir com os requisitos de buckets com o bloqueio de objetos S3 ativado).
- Quando a configuração global S3 Object Lock está ativada, não é possível criar uma nova política ILM proposta ou ativar uma política ILM proposta existente, a menos que a regra padrão da política seja compatível. Depois que a configuração global S3 Object Lock tiver sido ativada, as páginas ILM Rules e ILM Policies indicam quais regras ILM são compatíveis.

  No exemplo a seguir, a página regras ILM lista três regras que são compatíveis com buckets com o bloqueio de objeto S3 ativado.

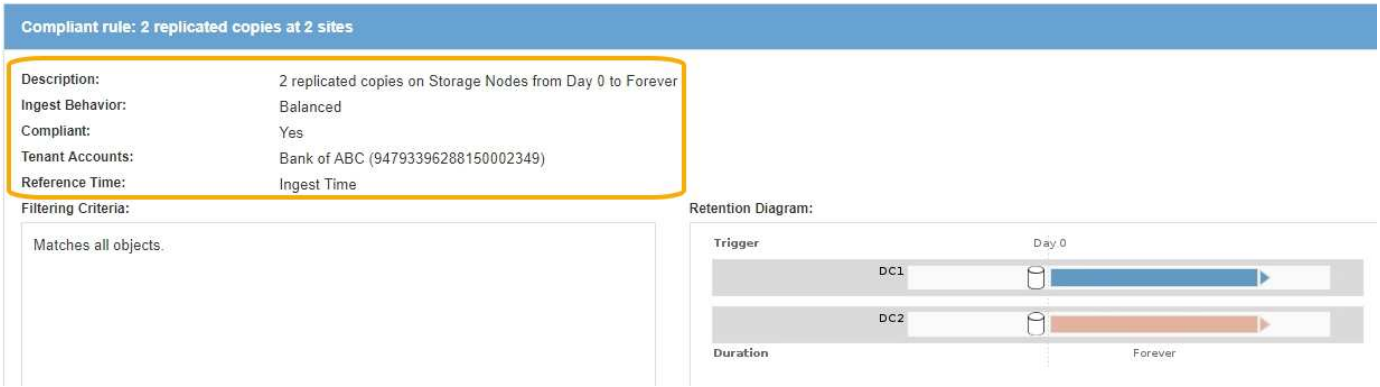


Requisitos para regras ILM compatíveis

Se você quiser ativar a configuração global S3 Object Lock, certifique-se de que a regra padrão na política ILM ativa seja compatível. Uma regra em conformidade satisfaz os requisitos de ambos os buckets com o S3 Object Lock ativado e quaisquer buckets existentes que tenham a conformidade legada ativada:

- Ele precisa criar pelo menos duas cópias de objeto replicadas ou uma cópia codificada por apagamento.
- Essas cópias devem existir nos nós de storage durante toda a duração de cada linha nas instruções de posicionamento.
- As cópias de objeto não podem ser salvas em um pool de storage de nuvem.
- As cópias de objeto não podem ser guardadas nos nós de arquivo.
- Pelo menos uma linha das instruções de colocação deve começar no dia 0, usando **tempo de ingestão** como hora de referência.
- Pelo menos uma linha das instruções de colocação deve ser "para sempre".

Por exemplo, esta regra satisfaz os requisitos de buckets com o bloqueio de objeto S3 ativado. Ele armazena duas cópias de objeto replicadas do tempo de ingestão (dia 0) para "eternamente". Os objetos serão armazenados em nós de storage em dois data centers.



Requisitos para políticas de ILM ativas e propostas

Quando a configuração global S3 Object Lock está ativada, as políticas ILM ativas e propostas podem incluir

regras compatíveis e não compatíveis.

- A regra padrão na política de ILM ativa ou proposta deve ser compatível.
- Regras não compatíveis aplicam-se apenas a objetos em buckets que não tenham o bloqueio de objetos S3 ativado ou que não tenham o recurso de conformidade legado habilitado.
- Regras compatíveis podem se aplicar a objetos em qualquer bucket; o bloqueio de objetos do S3 ou a conformidade legada não precisam ser ativados para o bucket.

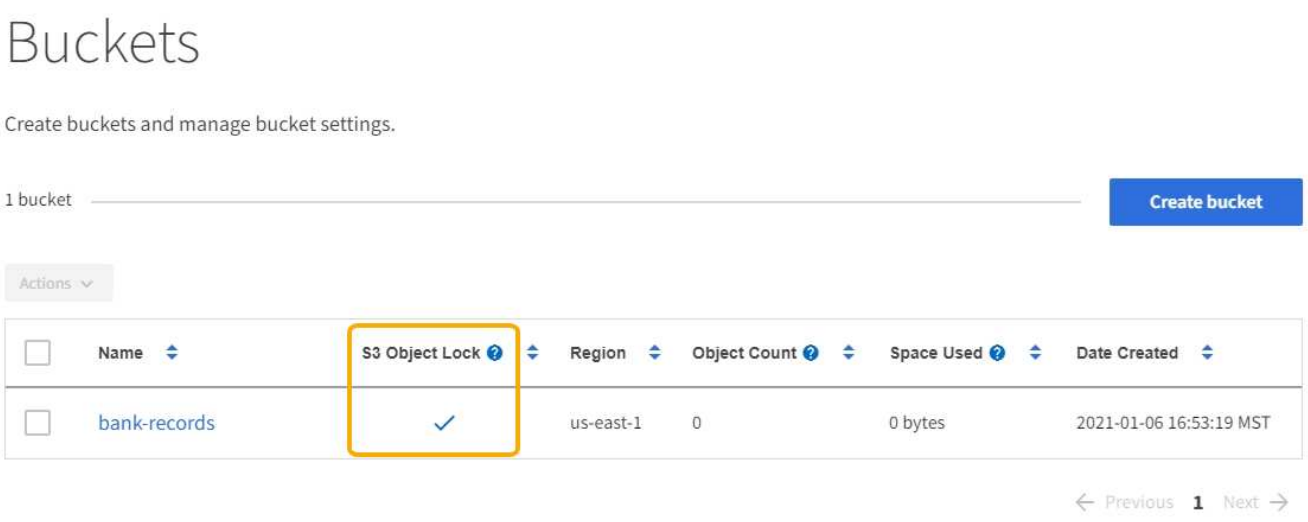
Uma política de ILM compatível pode incluir estas três regras:

1. Uma regra em conformidade que cria cópias codificadas de apagamento dos objetos em um bucket específico com o bloqueio de objeto S3 ativado. As cópias de EC são armazenadas nos nós de storage do dia 0 para sempre.
2. Regra não compatível que cria duas cópias de objetos replicadas em nós de storage por um ano e move uma cópia de objeto para nós de arquivamento e armazenamentos que são copiados para sempre. Esta regra só se aplica a buckets que não têm o bloqueio de objeto S3 ou a conformidade legada ativada porque armazena apenas uma cópia de objeto para sempre e usa nós de arquivo.
3. Regra padrão em conformidade que cria duas cópias de objetos replicadas nos nós de storage do dia 0 para sempre. Esta regra se aplica a qualquer objeto em qualquer bucket que não tenha sido filtrado pelas duas primeiras regras.

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 usar as configurações padrão de retenção de bucket ou, opcionalmente, especificar configurações de retenção para o objeto (retenção 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.

Informações relacionadas

- Use uma conta de locatário
- Use S3

- Comparação do S3 Object Lock com a conformidade legada
- Exemplo 7: Política de ILM compatível para bloqueio de objetos S3
- Rever registos de auditoria
- Use retenção padrão do bucket do bloqueio de objetos S3.

Ative o bloqueio de objetos S3 globalmente

Se uma conta de locatário do S3 precisar atender aos requisitos regulatórios ao salvar dados de objeto, você deverá ativar o bloqueio de objeto do S3 para todo o seu sistema StorageGRID. Ativar a configuração global S3 Object Lock permite que qualquer usuário do locatário do S3 crie e gerencie buckets e objetos com o S3 Object Lock.

O que você vai precisar

- Você tem a permissão de acesso root.
- Você está conetado ao Gerenciador de Grade usando um navegador da web suportado.
- Você revisou o fluxo de trabalho do S3 Object Lock e deve entender as considerações.
- A regra padrão na política ILM ativa é compatível.
  - Crie uma regra ILM padrão
  - Crie uma política ILM

Sobre esta tarefa

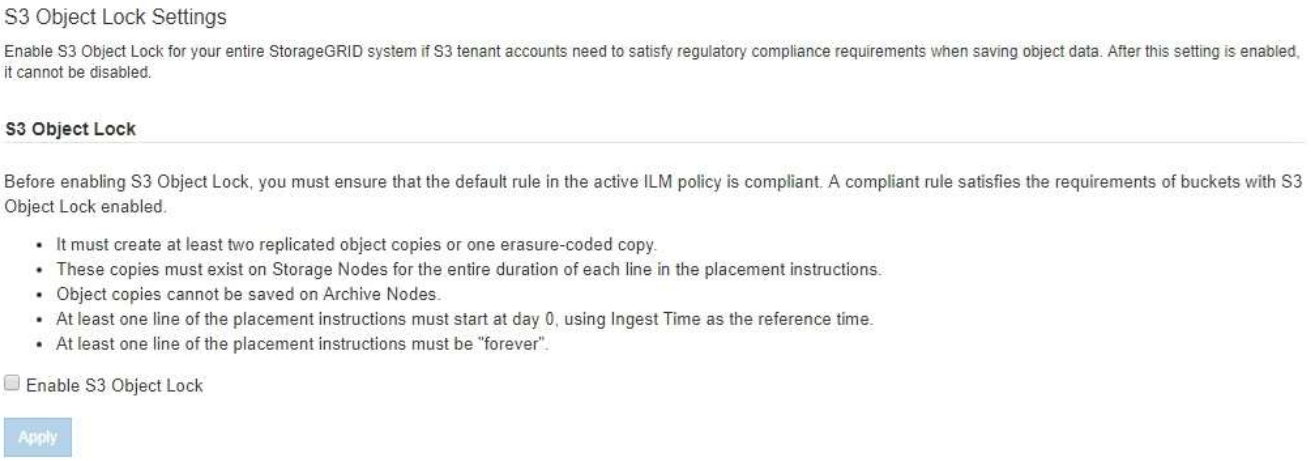
Um administrador de grade deve habilitar a configuração global S3 Object Lock para permitir que os usuários do locatário criem novos buckets com o S3 Object Lock ativado. Depois que esta definição estiver ativada, não poderá ser desativada.

> Se você ativou a configuração de conformidade global usando uma versão anterior do StorageGRID, a configuração bloqueio de objeto S3 será ativada no StorageGRID 11,6. Você pode continuar usando o StorageGRID para gerenciar as configurações dos buckets em conformidade existentes. No entanto, não é possível criar novos buckets em conformidade. "Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"Consulte .

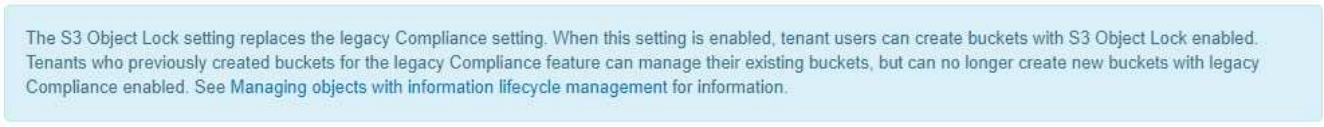
Passos

1. Selecione **CONFIGURATION** > **System** > **S3 Object Lock**.

   A página Configurações de bloqueio de objetos S3 é exibida.

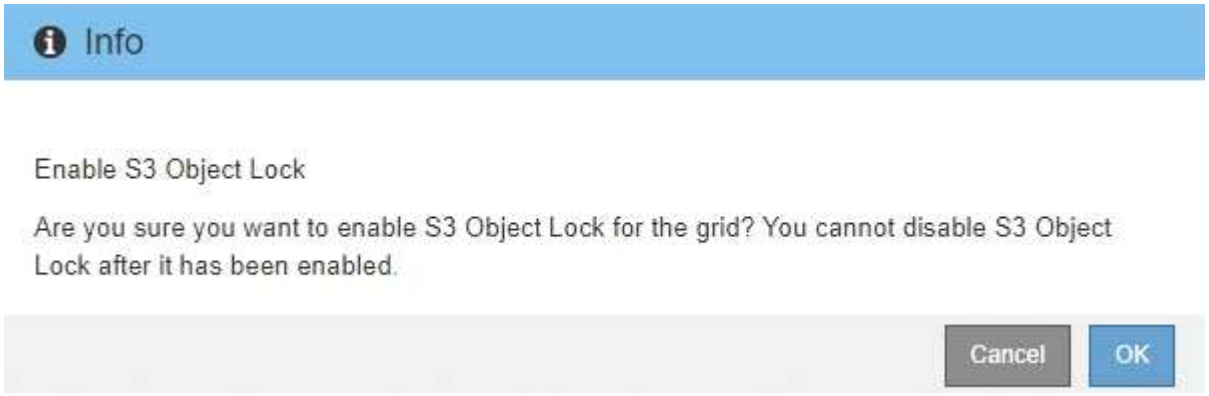


Se você ativou a configuração de conformidade global usando uma versão anterior do StorageGRID, a página inclui a seguinte nota:



2. Selecione **Ativar bloqueio de objetos S3**.
3. Selecione **aplicar**.

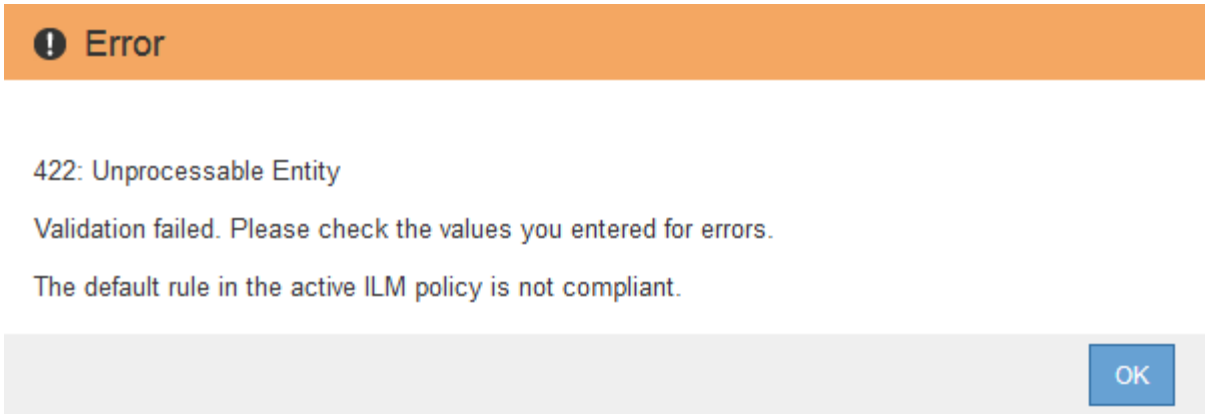
   Uma caixa de diálogo de confirmação é exibida e lembra que você não pode desativar o bloqueio de objeto S3 depois que ele estiver ativado.



4. Se tiver a certeza de que pretende ativar permanentemente o bloqueio de objetos S3D para todo o seu sistema, selecione **OK**.

   Quando você seleciona **OK**:

   - Se a regra padrão na política ILM ativa for compatível, o bloqueio de objetos S3 agora está ativado para toda a grade e não pode ser desativado.
   - Se a regra padrão não for compatível, um erro será exibido, indicando que você deve criar e ativar uma nova política ILM que inclua uma regra compatível como regra padrão. Selecione **OK** e crie uma nova política proposta, simule-a e ative-a.



Depois de terminar

Depois de ativar a configuração global S3 Object Lock, talvez seja necessário que crie uma regra padrão ela seja compatível e Crie uma política ILM que seja compatível. Depois que a configuração estiver ativada, a política ILM pode incluir opcionalmente uma regra padrão compatível e uma regra padrão não compatível. Por exemplo, você pode querer usar uma regra não compatível que não tenha filtros para objetos em buckets que não tenham o bloqueio de objeto S3 ativado.

Informações relacionadas

- Compare o S3 Object Lock com a conformidade legada

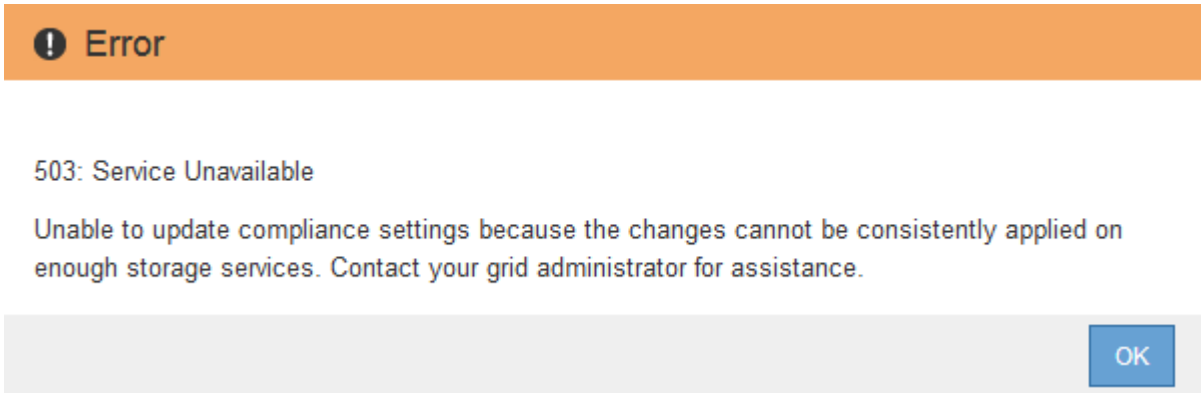
Resolva erros de consistência ao atualizar o bloqueio de objetos S3 ou a configuração de conformidade legada

Se um site de data center ou vários nós de storage em um local ficarem indisponíveis, talvez seja necessário ajudar S3 usuários de locatários a aplicar alterações ao bloqueio de objetos S3 ou à configuração de conformidade legada.

Os usuários locatários que têm buckets com o bloqueio de objeto S3 (ou conformidade legada) habilitado podem alterar determinadas configurações. Por exemplo, um usuário de locatário usando o bloqueio de objeto S3 pode precisar colocar uma versão de objeto em retenção legal.

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

- Os usuários do Gerenciador de locatários veem a seguinte mensagem de erro:



- Usuários de API de Gerenciamento de locatários e usuários de API S3 recebem um código de resposta de `503 Service Unavailable` texto de mensagem semelhante.

Para resolver esse erro, siga estas etapas:

1. Tente disponibilizar novamente todos os nós de storage ou locais o mais rápido possível.
2. Se você não conseguir disponibilizar suficientes nós de storage em cada local, entre em Contato com o suporte técnico, que pode ajudá-lo a recuperar nós e garantir que as alterações sejam aplicadas consistentemente na grade.
3. Depois que o problema subjacente for resolvido, lembre o usuário do locatário de tentar novamente suas alterações de configuração.

Informações relacionadas

- Use uma conta de locatário
- Use S3
- Recuperar e manter

Informações sobre direitos autorais

Informações sobre marcas comerciais