



Gerenciar objetos com ILM

StorageGRID

NetApp
March 12, 2025

Índice

Gerenciar objetos com ILM	1
Gerenciar objetos com ILM: Visão geral	1
Sobre estas instruções	1
Saiba mais	1
ILM e ciclo de vida do objeto	1
Como o ILM opera ao longo da vida de um objeto	1
Como os objetos são ingeridos	3
Como os objetos são armazenados (replicação ou codificação de apagamento)	8
Como a retenção de objetos é determinada	19
Como os objetos são excluídos	21
Criar e atribuir notas de armazenamento	24
Use pools de armazenamento	26
O que é um pool de storage?	26
Diretrizes para a criação de pools de armazenamento	27
Ativar a proteção contra perda de local	29
Crie um pool de armazenamento	31
Veja os detalhes do pool de armazenamento	32
Editar pool de armazenamento	33
Remova um pool de armazenamento	34
Use Cloud Storage Pools	35
O que é um Cloud Storage Pool?	35
Ciclo de vida de um objeto Cloud Storage Pool	37
Quando usar Cloud Storage Pools	40
Considerações para pools de storage em nuvem	41
Compare os pools do Cloud Storage e a replicação do CloudMirror	44
Crie um pool de storage em nuvem	46
Edite um pool de armazenamento em nuvem	51
Remova um pool de armazenamento em nuvem	52
Solucionar problemas em Cloud Storage Pools	53
Gerenciar perfis de codificação de apagamento	55
Renomear um perfil de codificação de apagamento	55
Desativar um perfil de codificação de apagamento	56
Configurar regiões (opcional e apenas S3)	59
Criar regra ILM	61
Criar uma regra ILM: Visão geral	61
Acesse o assistente criar uma regra ILM	64
Passo 1 de 3: Insira os detalhes	65
Passo 2 de 3: Definir posicionamentos	69
Use o último tempo de acesso nas regras do ILM	73
Passo 3 de 3: Selecione comportamento de ingestão	74
Crie uma regra ILM padrão	75
Criar política ILM	78
Criar uma política ILM: Visão geral	78

Crie uma política de ILM proposta	80
Simule uma política de ILM	84
Ative a política ILM.	89
Verifique uma política ILM com pesquisa de metadados de objeto	90
Trabalhe com políticas ILM e regras ILM.	93
Ver políticas ILM.	93
Clonar uma política histórica de ILM	93
Remova a política proposta de ILM	94
Exibir detalhes da regra ILM	94
Clonar uma regra ILM	95
Editar uma regra ILM	95
Remova uma regra ILM	95
Ver métricas ILM	96
Use o bloqueio de objetos S3D.	97
Gerencie objetos com o S3 Object Lock	97
Fluxo de trabalho para S3 Object Lock	101
Requisitos para o bloqueio de objetos S3	102
Ative o bloqueio de objetos S3 globalmente	104
Resolva erros de consistência ao atualizar o bloqueio de objetos S3 ou a configuração de conformidade legada	106
Exemplo de regras e políticas ILM.	106
Exemplo 1: Regras e política de ILM para armazenamento de objetos	106
Exemplo 2: Regras de ILM e política para filtragem de tamanho de objeto EC	109
Exemplo 3: Regras e política de ILM para melhor proteção para arquivos de imagem	110
Exemplo 4: Regras ILM e política para objetos com versão S3	112
Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa	114
Exemplo 6: Alterar uma política ILM.	117
Exemplo 7: Política de ILM compatível para bloqueio de objetos S3	122

Gerenciar objetos com ILM

Gerenciar objetos com ILM: Visão geral

Você gerencia os objetos em um sistema StorageGRID configurando uma política de gerenciamento do ciclo de vida das informações (ILM) que consiste em uma ou mais regras do ILM. As regras do ILM instruem o StorageGRID a criar e distribuir cópias de dados de objetos e como gerenciar essas cópias ao longo do tempo.

Sobre estas instruções

Projetar e implementar regras de ILM e a política de ILM requer um Planejamento cuidadoso. Você precisa entender seus requisitos operacionais, a topologia do sistema StorageGRID, suas necessidades de proteção de objetos e os tipos de storage disponíveis. Em seguida, você deve determinar como deseja que diferentes tipos de objetos sejam copiados, distribuídos e armazenados.

Use estas instruções para:

- Saiba mais sobre o StorageGRID ILM, "[Como o ILM opera ao longo da vida de um objeto](#)" incluindo .
- Saiba como configurar "[pools de armazenamento](#)", "[Pools de storage de nuvem](#)" e "[Regras do ILM](#)".
- Saiba como "[Crie, simule e ative uma política ILM](#)" isso protegerá os dados de objetos em um ou mais sites.
- Saiba como "[Gerencie objetos com o S3 Object Lock](#)", o que ajuda a garantir que os objetos em buckets específicos do S3 não sejam excluídos ou substituídos por um período de tempo especificado.

Saiba mais

Para saber mais, reveja estes vídeos:

- "[Vídeo: Regras de gerenciamento do ciclo de vida das informações no StorageGRID 11,7](#)".
- "[Vídeo: Políticas de gerenciamento do ciclo de vida das informações no StorageGRID 11,7](#)".

ILM e ciclo de vida do objeto

Como o ILM opera ao longo da vida de um objeto

Entender como o StorageGRID usa o ILM para gerenciar objetos durante cada estágio de sua vida pode ajudá-lo a projetar uma política mais eficaz.

- **Ingest:** O ingest começa quando um aplicativo cliente S3 ou Swift estabelece uma conexão para salvar um objeto no sistema StorageGRID, e é concluído quando o StorageGRID retorna uma mensagem "ingest successful" ao cliente. Os dados de objeto são protegidos durante a ingestão, aplicando instruções de ILM imediatamente (posicionamento síncrono) ou criando cópias provisórias e aplicando ILM mais tarde (commit duplo), dependendo de como os requisitos de ILM foram especificados.
- **Gerenciamento de cópias:** Depois de criar o número e o tipo de cópias de objetos especificados nas

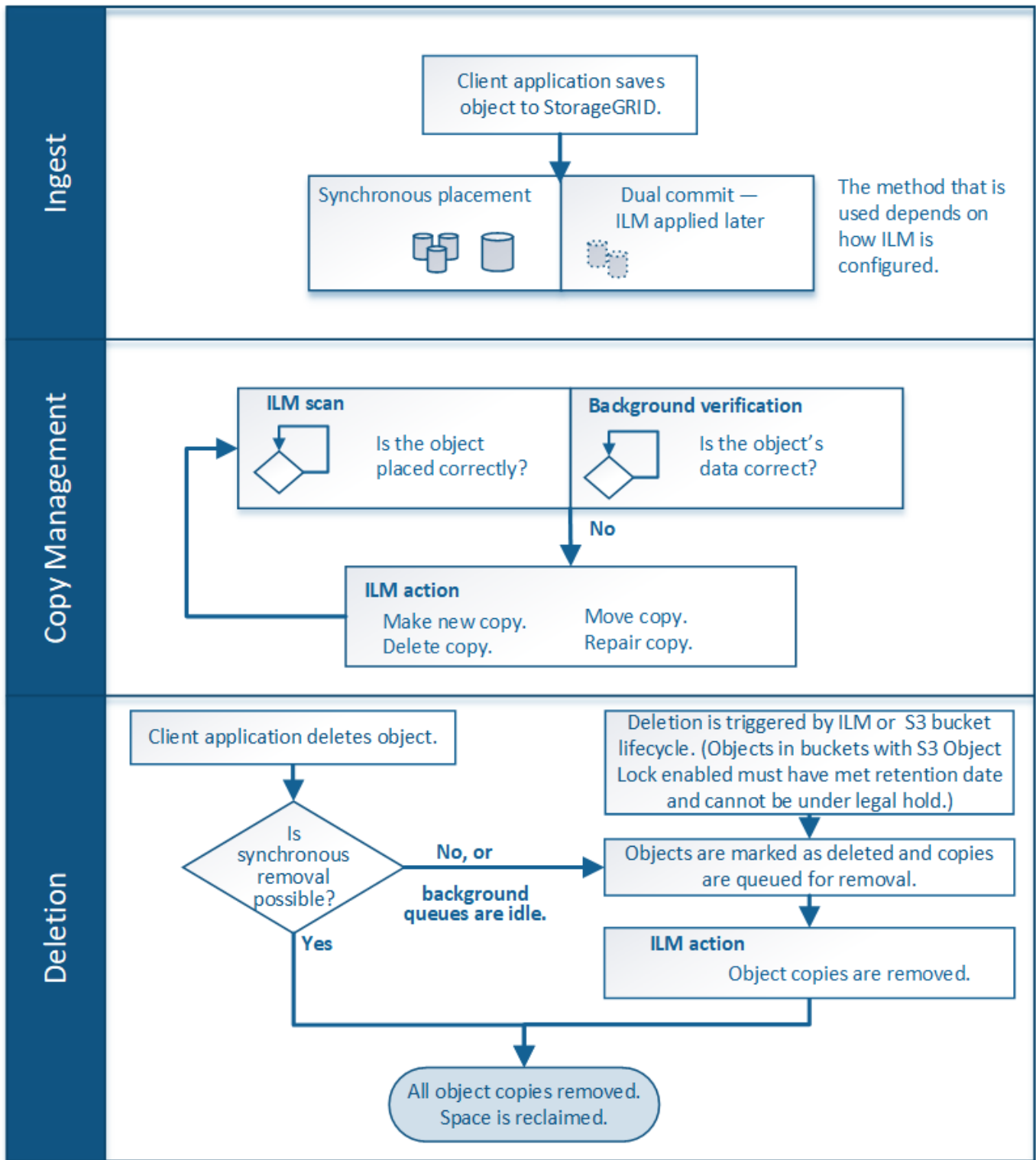
instruções de colocação do ILM, o StorageGRID gerencia locais de objetos e protege objetos contra perda.

- **Digitalização e avaliação ILM:** O StorageGRID verifica continuamente a lista de objetos armazenados na grade e verifica se as cópias atuais atendem aos requisitos do ILM. Quando diferentes tipos, números ou locais de cópias de objetos são necessários, o StorageGRID cria, exclui ou move cópias conforme necessário.
- **Verificação em segundo plano:** O StorageGRID realiza continuamente a verificação em segundo plano para verificar a integridade dos dados do objeto. Se um problema for encontrado, o StorageGRID criará automaticamente uma nova cópia de objeto ou um fragmento de objeto codificado de apagamento de substituição em um local que atenda aos requisitos atuais do ILM. ["Verifique a integridade do objeto"](#)Consulte .
- **Exclusão de objeto:** O gerenciamento de um objeto termina quando todas as cópias são removidas do sistema StorageGRID. Os objetos podem ser removidos como resultado de uma solicitação de exclusão por um cliente, ou como resultado de exclusão por ILM ou exclusão causada pela expiração de um ciclo de vida de bucket do S3.



Os objetos em um bucket que tem o bloqueio de objeto S3 ativado não podem ser excluídos se estiverem sob uma retenção legal ou se uma data de retenção até tiver sido especificada, mas ainda não cumprida.

O diagrama resume como o ILM opera ao longo do ciclo de vida de um objeto.



Como os objetos são ingeridos

Opções de ingestão

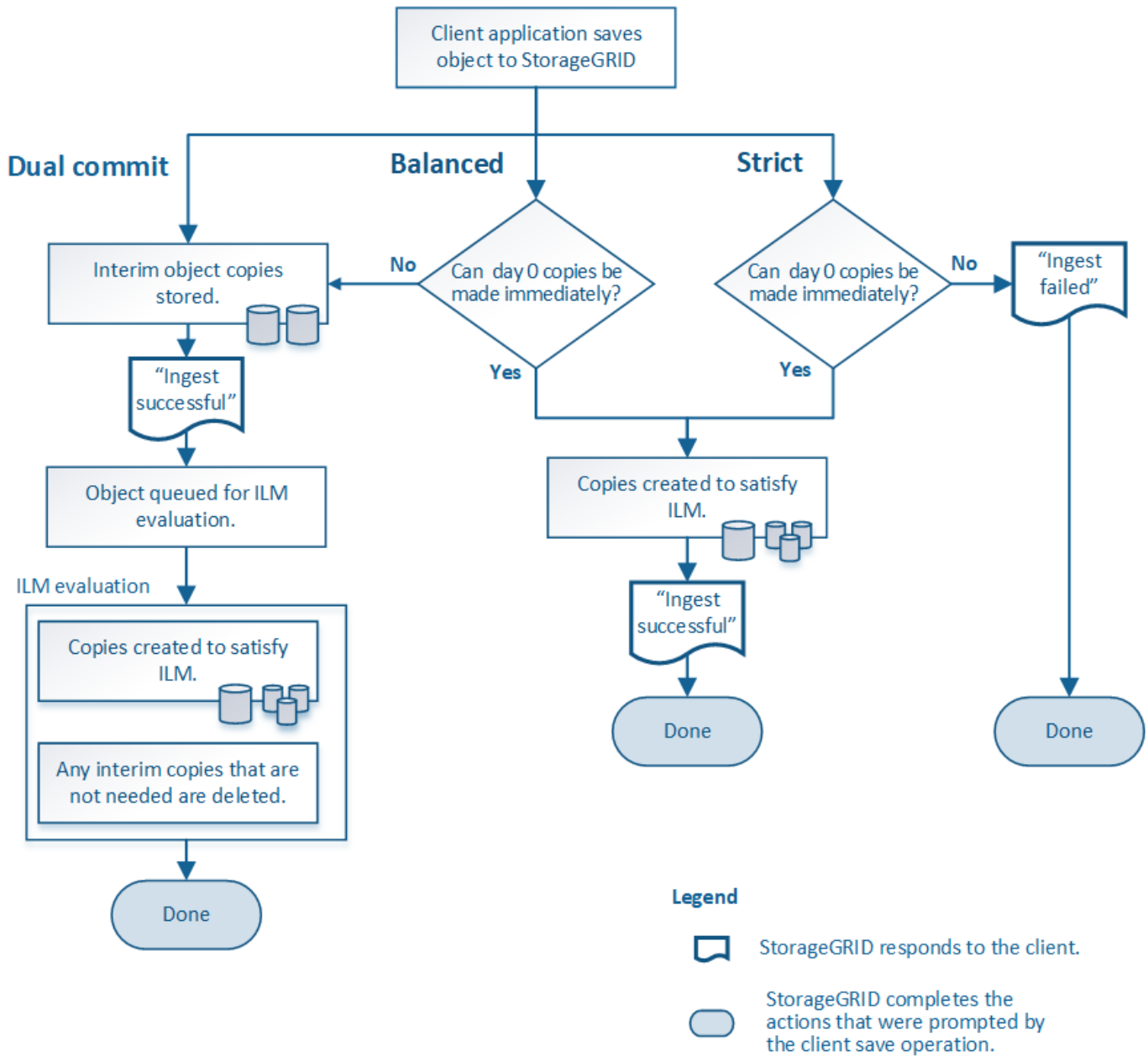
Ao criar uma regra ILM, você especifica uma das três opções para proteger objetos na ingestão: Commit duplo, estrito ou balanceado.

Dependendo de sua escolha, o StorageGRID faz cópias provisórias e coloca os objetos em fila para avaliação

do ILM mais tarde, ou usa o posicionamento síncrono e faz cópias imediatamente para atender aos requisitos do ILM.

Fluxograma das opções de ingestão

O fluxograma mostra o que acontece quando os objetos são combinados por uma regra ILM que usa cada uma das três opções de ingestão.



Commit duplo

Quando você seleciona a opção de confirmação dupla, o StorageGRID imediatamente faz cópias provisórias de objeto em dois nós de armazenamento diferentes e retorna uma mensagem de "ingestão bem-sucedida" para o cliente. O objeto é colocado em fila para avaliação ILM e cópias que atendem às instruções de colocação da regra são feitas posteriormente.

Quando usar a opção de confirmação dupla

Use a opção de confirmação dupla em qualquer um desses casos:

- Você está usando regras de ILM de vários sites e a latência de ingestão de clientes é sua principal consideração. Ao usar o Dual Commit, você deve garantir que sua grade possa executar o trabalho adicional de criar e remover as cópias de duplo commit se elas não satisfizerem o ILM. Especificamente:
 - A carga na grade deve ser baixa o suficiente para evitar um backlog ILM.
 - A grade deve ter recursos de hardware em excesso (IOPS, CPU, memória, largura de banda da rede, etc.).
- Você está usando regras ILM de vários sites e a conexão WAN entre os sites geralmente tem alta latência ou largura de banda limitada. Nesse cenário, usar a opção de confirmação dupla pode ajudar a evitar tempos limite do cliente. Antes de escolher a opção Dual Commit, você deve testar o aplicativo cliente com cargas de trabalho realistas.

Rigorous

Quando você seleciona a opção estrita, o StorageGRID usa o posicionamento síncrono na ingestão e faz imediatamente todas as cópias de objetos especificadas nas instruções de posicionamento da regra. A ingestão falha se o StorageGRID não puder criar todas as cópias, por exemplo, porque um local de armazenamento necessário está temporariamente indisponível. O cliente deve tentar novamente a operação.

Quando usar a opção estrita

Use a opção estrita se você tiver um requisito operacional ou regulamentar para armazenar imediatamente objetos apenas nos locais descritos na regra ILM. Por exemplo, para atender a um requisito regulatório, talvez seja necessário usar a opção estrita e um filtro avançado de restrição de localização para garantir que os objetos nunca sejam armazenados em determinados data centers.

["Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"](#) Consulte .

Equilibrado (padrão)

Quando você seleciona a opção equilibrada, o StorageGRID também usa o posicionamento síncrono na ingestão e faz imediatamente todas as cópias especificadas nas instruções de posicionamento da regra. Em contraste com a opção estrita, se o StorageGRID não puder fazer imediatamente todas as cópias, ele usará o Dual Commit.

Quando usar a opção equilibrada

Use a opção equilibrada para obter a melhor combinação de proteção de dados, desempenho de grade e sucesso de ingestão. Balanced é a opção padrão no assistente criar regra ILM.

Vantagens, desvantagens e limitações das opções de ingestão

Compreender as vantagens e desvantagens de cada uma das três opções de proteção de dados na ingestão (equilibrada, rigorosa ou dupla confirmação) pode ajudá-lo a decidir qual escolher para uma regra ILM.

Para obter uma visão geral das opções de ingestão, ["Opções de ingestão"](#) consulte .

Vantagens das opções equilibradas e estritas

Quando comparado ao Dual Commit, que cria cópias provisórias durante a ingestão, as duas opções de posicionamento síncrono podem oferecer as seguintes vantagens:

- **Melhor segurança de dados:** Os dados do objeto são imediatamente protegidos conforme especificado nas instruções de colocação da regra ILM, que podem ser configurados para proteger contra uma ampla variedade de condições de falha, incluindo a falha de mais de um local de armazenamento. A confirmação dupla só pode proteger contra a perda de uma única cópia local.
- **Operação de grade mais eficiente:** Cada objeto é processado apenas uma vez, pois é ingerido. Como o sistema StorageGRID não precisa rastrear ou excluir cópias provisórias, há menos carga de processamento e menos espaço no banco de dados é consumido.
- *** (Equilibrado) recomendado*:** A opção equilibrada proporciona uma eficiência ideal de ILM. O uso da opção Balanced é recomendado, a menos que um comportamento de ingestão rigoroso seja necessário ou a grade atenda a todos os critérios para usar o Dual Commit.
- **(strict) certeza sobre locais de objetos:** A opção strict garante que os objetos são imediatamente armazenados de acordo com as instruções de colocação na regra ILM.

Desvantagens das opções equilibradas e estritas

Quando comparado ao Dual Commit, as opções equilibradas e estritas têm algumas desvantagens:

- *** Maiores ingerências de clientes*:** As latências de ingestão de clientes podem ser mais longas. Quando você usa as opções balanceadas ou rigorosas, uma mensagem ""ingest successful"" não será retornada ao cliente até que todos os fragmentos codificados por apagamento ou cópias replicadas sejam criados e armazenados. No entanto, os dados de objetos provavelmente alcançarão seu posicionamento final muito mais rápido.
- **(strict) taxas mais altas de falha de ingestão:** Com a opção estrita, a ingestão falha sempre que o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra ILM. Você pode ver altas taxas de falha de ingestão se um local de armazenamento necessário estiver temporariamente off-line ou se problemas de rede causarem atrasos na cópia de objetos entre sites.
- **(strict) S3 colocações de upload de várias partes podem não ser como esperado em algumas circunstâncias:** Com strict, você espera que objetos sejam colocados como descrito pela regra ILM ou para que a ingestão falhe. No entanto, com um upload multipart S3, o ILM é avaliado para cada parte do objeto à medida que ele é ingerido e para o objeto como um todo quando o upload multipart é concluído. Nas seguintes circunstâncias, isso pode resultar em colocações que são diferentes do que você espera:
 - **Se o ILM mudar enquanto um upload multipart S3 está em andamento:** Porque cada parte é colocada de acordo com a regra que está ativa quando a peça é ingerida, algumas partes do objeto podem não atender aos requisitos atuais do ILM quando o upload multipart é concluído. Nesses casos, a ingestão do objeto não falha. Em vez disso, qualquer peça que não seja colocada corretamente é colocada na fila para reavaliação ILM e é movida para o local correto mais tarde.
 - **Quando as regras do ILM filtram no tamanho:** Ao avaliar o ILM para uma peça, o StorageGRID filtra o tamanho da peça, não o tamanho do objeto. Isso significa que partes de um objeto podem ser armazenadas em locais que não atendem aos requisitos de ILM para o objeto como um todo. Por exemplo, se uma regra especifica que todos os objetos de 10 GB ou maior são armazenados em DC1 enquanto todos os objetos menores são armazenados em DC2, na ingestão cada parte de 1 GB de um upload multipart de 10 partes é armazenado em DC2. Quando ILM é avaliado para o objeto, todas as partes do objeto são movidas para DC1.
- **(strict) ingest não falha quando tags de objeto ou metadados são atualizados e não é possível fazer posicionamentos recém-solicitados:** Com strict, você espera que objetos sejam colocados conforme descrito pela regra ILM ou para falha de ingestão. No entanto, quando você atualiza metadados ou tags

para um objeto que já está armazenado na grade, o objeto não é reingerido. Isso significa que quaisquer alterações no posicionamento de objetos que são acionadas pela atualização não são feitas imediatamente. As alterações de posicionamento são feitas quando o ILM é reavaliado por processos normais de ILM em segundo plano. Se as alterações de posicionamento necessárias não puderem ser feitas (por exemplo, porque um local recém-solicitado não está disponível), o objeto atualizado mantém seu posicionamento atual até que as alterações de posicionamento sejam possíveis.

Limitações em posicionamentos de objetos com opções equilibradas e estritas

As opções equilibradas ou estritas não podem ser usadas para regras de ILM que tenham qualquer uma destas instruções de colocação:

- Colocação em um pool de storage de nuvem no dia 0.
- Colocação em um nó de arquivo no dia 0.
- Posicionamentos em um pool de armazenamento em nuvem ou em um nó de arquivamento quando a regra tiver um tempo de criação definido pelo usuário como seu tempo de referência.

Essas restrições existem porque o StorageGRID não pode fazer cópias sincronamente para um pool de armazenamento em nuvem ou um nó de arquivamento, e um tempo de criação definido pelo usuário pode ser resolvido até o momento.

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

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

Por exemplo, o comportamento de ingestão selecionado para uma regra ILM afeta o posicionamento inicial de cópias de objetos, enquanto o controle de consistência usado quando um objeto é armazenado afeta o posicionamento inicial dos metadados de objetos. Como o StorageGRID requer acesso aos dados e metadados de um objeto para atender às solicitações do cliente, selecionar níveis de proteção correspondentes para o nível de consistência e comportamento de ingestão pode fornecer melhor proteção de dados inicial e respostas do sistema mais previsíveis.

Aqui está um breve resumo dos controles de consistência disponíveis no StorageGRID:

- **Todos:** Todos os nós recebem metadados de objeto imediatamente ou a solicitação falhará.
- **Strong-global:** Metadados de objetos são imediatamente distribuídos para todos os sites. Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
- **Strong-site:** Metadados de objetos são imediatamente distribuídos para outros nós no site. Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.
- **Read-after-novo-write:** Fornece consistência de leitura-após-gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. 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.



Antes de selecionar um nível de consistência, leia a descrição completa dos controles de consistência nas instruções ["USE A API REST DO S3"](#) do . Você deve entender os benefícios e limitações antes de alterar o valor padrão.

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

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

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

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

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

Se, em vez disso, você usou a mesma regra ILM e o nível de consistência "site-trong", o cliente poderá receber uma mensagem de sucesso depois que os dados do objeto forem replicados para o site remoto, mas antes que os metadados do objeto sejam distribuídos lá. Nesse caso, o nível de proteção dos metadados de objetos não corresponde ao nível de proteção dos dados de objeto. Se o site local for perdido logo após a ingestão, os metadados do objeto serão perdidos. O objeto não pode ser recuperado.

A inter-relação entre níveis de consistência e regras de ILM pode ser complexa. Contacte a NetApp se necessitar de assistência.

Informações relacionadas

- ["Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"](#)

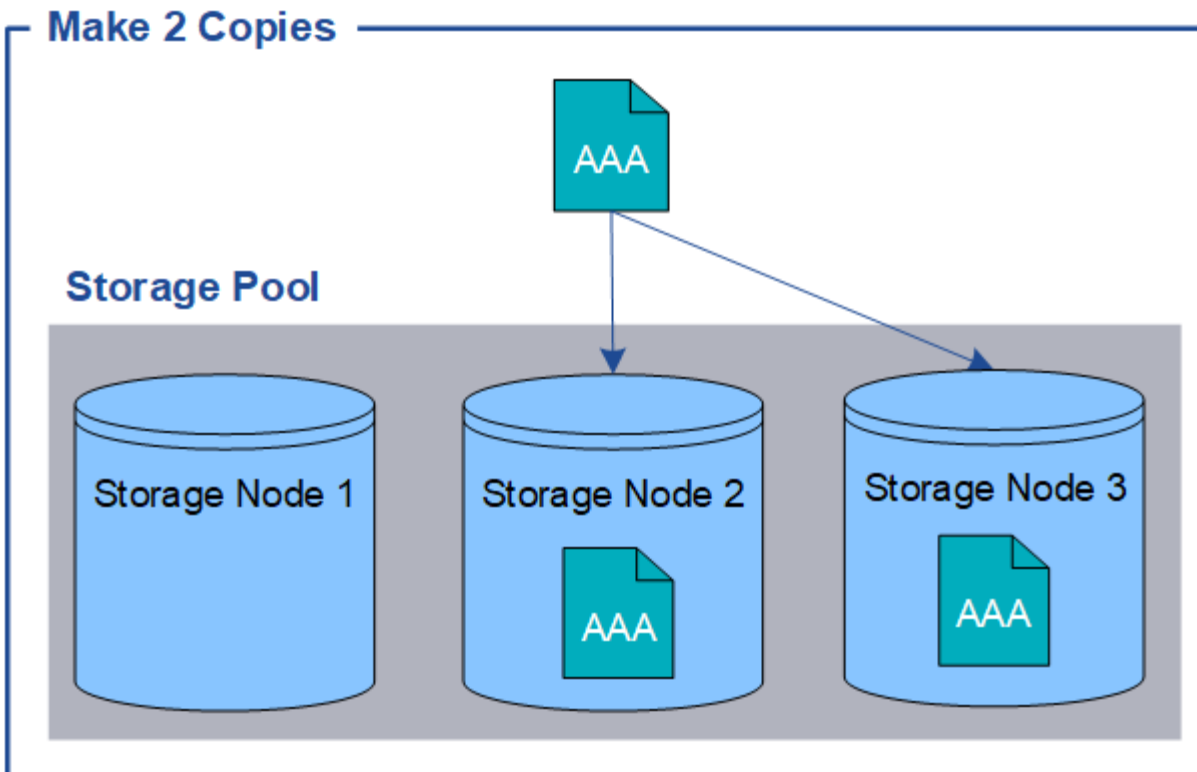
Como os objetos são armazenados (replicação ou codificação de apagamento)

O que é replicação?

A replicação é um dos dois métodos usados pelo StorageGRID para armazenar dados de objetos. Quando os objetos correspondem a uma regra de ILM que usa replicação, o sistema cria cópias exatas de dados de objetos e armazena as cópias em nós de storage ou nós de arquivamento.

Quando você configura uma regra ILM para criar cópias replicadas, você especifica quantas cópias devem ser criadas, onde essas cópias devem ser colocadas e por quanto tempo as cópias devem ser armazenadas em cada local.

No exemplo a seguir, a regra ILM especifica que duas cópias replicadas de cada objeto serão colocadas em um pool de storage que contém três nós de storage.



Quando o StorageGRID faz a correspondência de objetos a essa regra, ele cria duas cópias do objeto, colocando cada cópia em um nó de storage diferente no pool de storage. As duas cópias podem ser colocadas em qualquer um dos três nós de storage disponíveis. Nesse caso, a regra colocou cópias de objeto nos nós de storage 2 e 3. Como há duas cópias, o objeto pode ser recuperado se algum dos nós no pool de storage falhar.



O StorageGRID pode armazenar apenas uma cópia replicada de um objeto em qualquer nó de storage. Se sua grade incluir três nós de storage e você criar uma regra de ILM de 4 cópias, apenas três cópias serão feitas - uma cópia para cada nó de storage. O alerta **ILM Placement Unachievable** é acionado para indicar que a regra ILM não pôde ser completamente aplicada.

Informações relacionadas

- ["O que é codificação de apagamento?"](#)
- ["O que é um pool de storage?"](#)
- ["Habilite a proteção contra perda de site usando replicação e codificação de apagamento"](#)

Por que você não deve usar replicação de cópia única

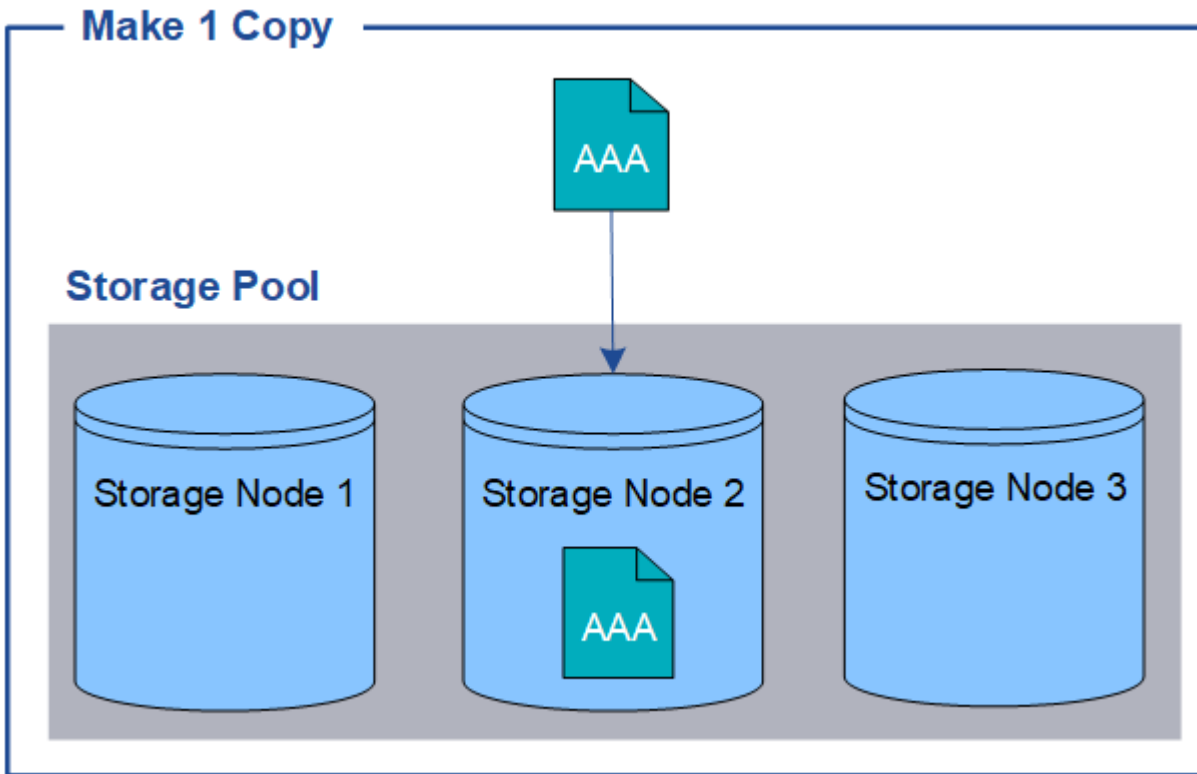
Ao criar uma regra ILM para criar cópias replicadas, você deve sempre especificar pelo menos duas cópias para qualquer período de tempo nas instruções de colocação.



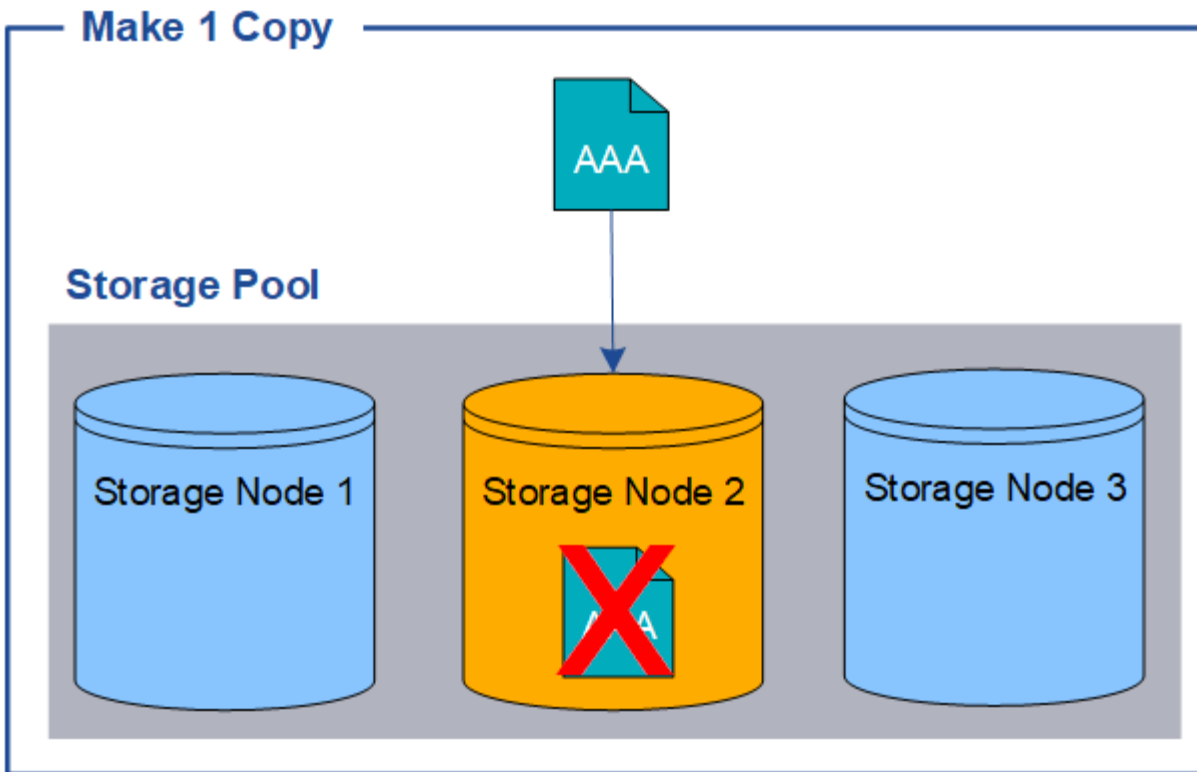
Não use uma regra ILM que crie apenas uma cópia replicada para qualquer período de tempo. Se houver apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

No exemplo a seguir, a regra Make 1 Copy ILM especifica que uma cópia replicada de um objeto seja colocada em um pool de storage que contém três nós de storage. Quando um objeto é ingerido que

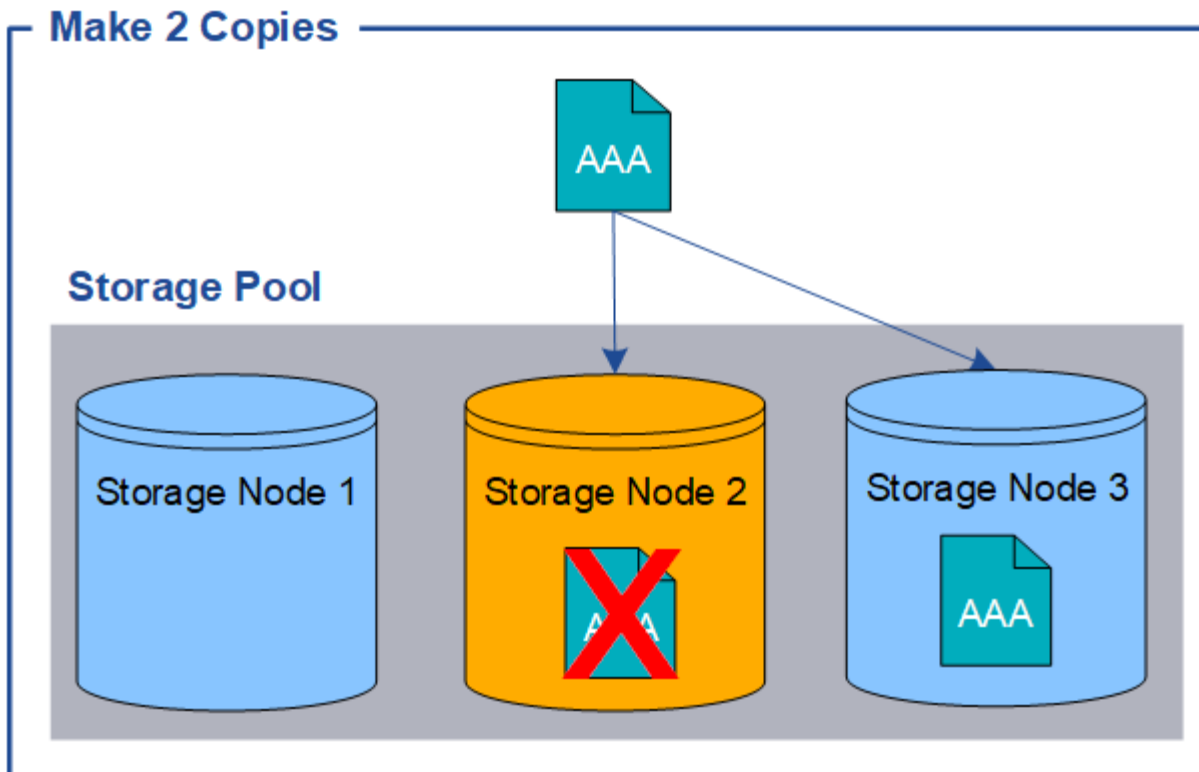
corresponde a essa regra, o StorageGRID coloca uma única cópia em apenas um nó de storage.



Quando uma regra ILM cria apenas uma cópia replicada de um objeto, o objeto fica inacessível quando o nó de armazenamento não está disponível. Neste exemplo, você perderá temporariamente o acesso ao objeto AAA sempre que o nó de armazenamento 2 estiver offline, como durante uma atualização ou outro procedimento de manutenção. Você perderá o objeto AAA inteiramente se o nó de storage 2 falhar.



Para evitar a perda de dados de objetos, você sempre deve fazer pelo menos duas cópias de todos os objetos que deseja proteger com a replicação. Se existirem duas ou mais cópias, ainda poderá acessar ao objeto se um nó de armazenamento falhar ou ficar offline.



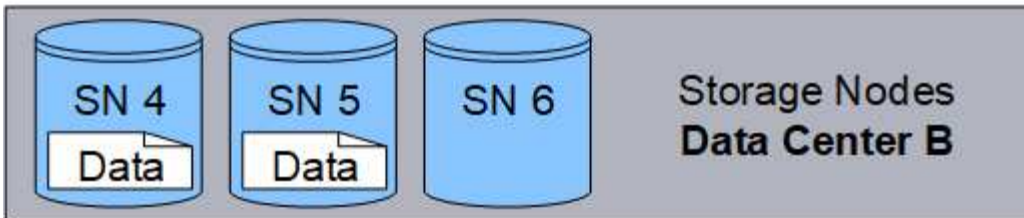
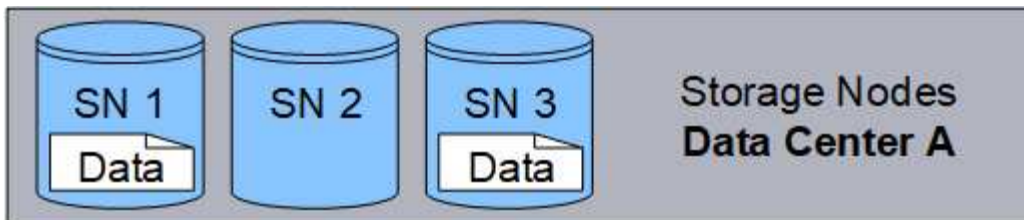
O que é codificação de apagamento?

A codificação de apagamento é um dos dois métodos que o StorageGRID usa para armazenar dados de objetos. Quando os objetos correspondem a uma regra ILM que usa codificação de apagamento, esses objetos são cortados em fragmentos de dados, fragmentos de paridade adicionais são computados e cada fragmento é armazenado em um nó de armazenamento diferente.

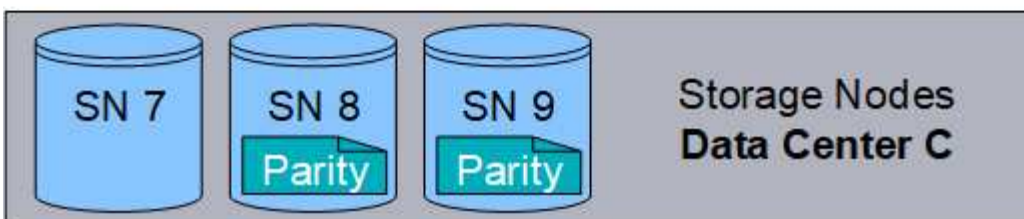
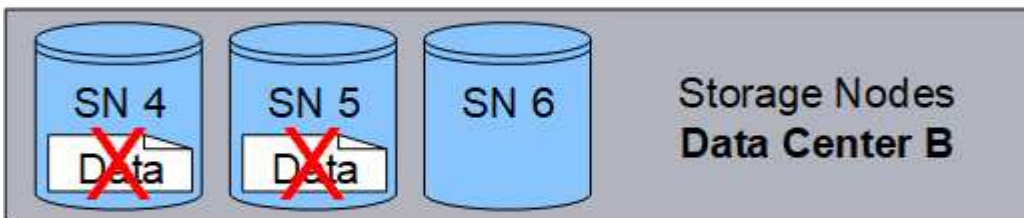
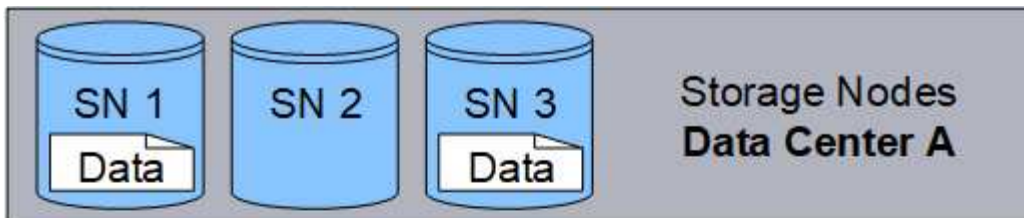
Quando um objeto é acessado, ele é remontado usando os fragmentos armazenados. Se um dado ou um fragmento de paridade ficar corrompido ou perdido, o algoritmo de codificação de apagamento pode recriar esse fragmento usando um subconjunto dos dados restantes e fragmentos de paridade.

À medida que você cria regras de ILM, o StorageGRID cria perfis de codificação de apagamento que suportam essas regras. É possível exibir uma lista de perfis de codificação de apagamento, "[renomear um perfil de codificação de apagamento](#)", ou "[Desative um perfil de codificação de apagamento se ele não for usado atualmente em nenhuma regra ILM](#)".

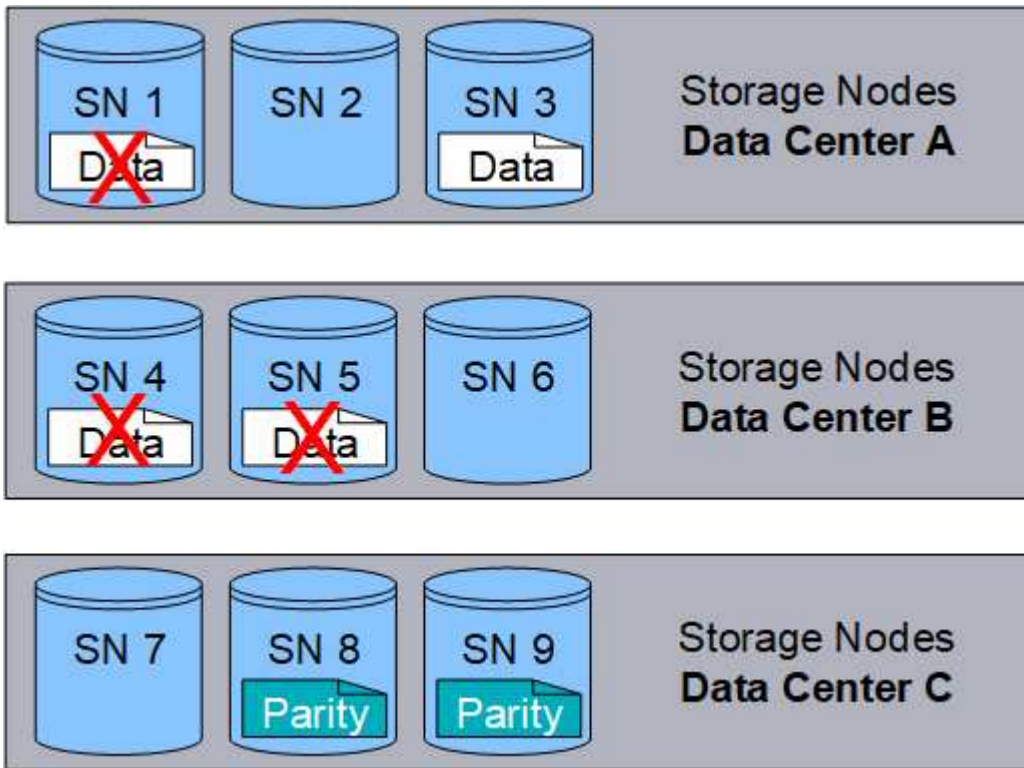
O exemplo a seguir ilustra o uso de um algoritmo de codificação de apagamento nos dados de um objeto. Neste exemplo, a regra ILM usa um esquema de codificação de apagamento 4-2. Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados do objeto. Cada um dos seis fragmentos é armazenado em um nó diferente em três locais de data center para fornecer proteção de dados para falhas de nós ou perda de local.



O esquema de codificação de apagamento 4-2 pode ser configurado de várias maneiras. Por exemplo, você pode configurar um pool de storage de um único local que contenha seis nós de storage. Para "[proteção contra perda de local](#)", você pode usar um pool de storage que contém três locais com três nós de storage em cada local. Um objeto pode ser recuperado desde que quaisquer quatro dos seis fragmentos (dados ou paridade) permaneçam disponíveis. Até dois fragmentos podem ser perdidos sem perda dos dados do objeto. Se um site inteiro for perdido, o objeto ainda pode ser recuperado ou reparado, desde que todos os outros fragmentos permaneçam acessíveis.



Se mais de dois nós de storage forem perdidos, o objeto não poderá ser recuperado.



Informações relacionadas

- ["O que é replicação?"](#)
- ["O que é um pool de storage?"](#)
- ["O que são esquemas de codificação de apagamento?"](#)
- ["Renomear um perfil de codificação de apagamento"](#)
- ["Desativar um perfil de codificação de apagamento"](#)

O que são esquemas de codificação de apagamento?

Os esquemas de codificação de apagamento controlam quantos fragmentos de dados e quantos fragmentos de paridade são criados para cada objeto.

Ao configurar o perfil de codificação de apagamento para uma regra ILM, você seleciona um esquema de codificação de apagamento disponível com base em quantos nós de storage e sites compõem o pool de storage que você planeja usar.

O sistema StorageGRID usa o algoritmo de codificação de apagamento de Reed-Solomon. O algoritmo corta um objeto em k fragmentos de dados e calcula m fragmentos de paridade. $k + m = n$. Os fragmentos são espalhados pelos n nós de storage para fornecer proteção de dados. Um objeto pode sustentar até m fragmentos perdidos ou corrompidos. Para recuperar ou reparar um objeto, k fragmentos são necessários.

Ao selecionar o pool de armazenamento a ser usado para uma regra que criará uma cópia codificada por apagamento, use as seguintes diretrizes para pools de armazenamento:

- O pool de storage deve incluir três ou mais locais, ou exatamente um local.



Não é possível usar a codificação de apagamento se o pool de armazenamento incluir dois sites.

- [Esquemas de codificação de apagamento para pools de storage que contêm três ou mais locais](#)
- [Esquemas de codificação de apagamento para pools de storage de um local](#)
- Não use um pool de armazenamento que inclua o site padrão, todos os sites.
- O pool de storage deve incluir pelo menos $k+m + 1$ nós de storage.

O número mínimo de nós de storage necessário é $k+m$. No entanto, ter pelo menos um nó de armazenamento adicional pode ajudar a evitar falhas de ingestão ou backlogs de ILM se um nó de armazenamento necessário estiver temporariamente indisponível.

A sobrecarga de armazenamento de um esquema de codificação de apagamento é calculada dividindo o número de fragmentos de paridade (m) pelo número de fragmentos de dados (k). Você pode usar a sobrecarga de storage para calcular quanto espaço em disco cada objeto com codificação de apagamento requer:

$$disk\ space = object\ size + (object\ size * storage\ overhead)$$

Por exemplo, se você armazenar um objeto de 10 MB usando o esquema 4-2 (que tem 50% de sobrecarga de armazenamento), o objeto consome 15 MB de armazenamento em grade. Se você armazenar o mesmo objeto de 10 MB usando o esquema 6-2 (que tem 33% de sobrecarga de armazenamento), o objeto consome aproximadamente 13,3 MB.

Selecione o esquema de codificação de apagamento com o menor valor total $k+m$ que atenda às suas necessidades. Em geral, os esquemas de codificação de apagamento com um número menor de fragmentos são mais eficientes em termos computacionais, pois menos fragmentos são criados e distribuídos (ou recuperados) por objeto podem mostrar melhor desempenho devido ao tamanho de fragmento maior e podem exigir menos nós adicionados em uma expansão quando mais storage é necessário. (Para obter informações sobre como Planejar uma expansão de armazenamento, consulte "[Instruções para expandir StorageGRID](#)".)

Esquemas de codificação de apagamento para pools de storage que contêm três ou mais locais

A tabela a seguir descreve os esquemas de codificação de apagamento atualmente compatíveis com o StorageGRID para pools de storage que incluem três ou mais locais. Todos esses esquemas fornecem proteção contra perda de sites. Um site pode ser perdido, e o objeto ainda estará acessível.

Para esquemas de codificação de apagamento que fornecem proteção contra perda de local, o número recomendado de nós de storage no pool de storage excede $k+m + 1$ porque cada local requer um mínimo de três nós de storage.

Esquema de codificação de apagamento (k)	Número mínimo de locais implantados	Número recomendado de nós de storage em cada local	Número total recomendado de nós de storage	Proteção contra perda de site?	Sobrecarga de storage
4-2	3	3	9	Sim	50%
6-2	4	3	12	Sim	33%

Esquema de codificação de apagamento (k)	Número mínimo de locais implantados	Número recomendado de nós de storage em cada local	Número total recomendado de nós de storage	Proteção contra perda de site?	Sobrecarga de storage
8-2	5	3	15	Sim	25%
6-+3	3	4	12	Sim	50%
9-+3	4	4	16	Sim	33%
2-+1	3	3	9	Sim	50%
4-+1	5	3	15	Sim	25%
6-+1	7	3	21	Sim	17%
7-+5	3	5	15	Sim	71%



O StorageGRID requer um mínimo de três nós de storage por local. Para usar o esquema 7-5, cada local requer um mínimo de quatro nós de storage. Recomenda-se o uso de cinco nós de storage por local.

Ao selecionar um esquema de codificação de apagamento que forneça proteção do site, equilibre a importância relativa dos seguintes fatores:

- **Número de fragmentos:** Desempenho e flexibilidade de expansão são geralmente melhores quando o número total de fragmentos é menor.
- **Tolerância a falhas:** A tolerância a falhas é aumentada por ter mais segmentos de paridade (ou seja, m quando tem um valor mais alto).
- **Tráfego de rede:** Ao recuperar de falhas, usar um esquema com mais fragmentos (ou seja, um total maior para $k+m$) cria mais tráfego de rede.
- *** Sobrecarga de armazenamento*:** Esquemas com maior sobrecarga requerem mais espaço de armazenamento por objeto.

Por exemplo, ao decidir entre um esquema 4-2 e um esquema 6-3 (que ambos têm uma sobrecarga de armazenamento de 50%), selecione o esquema 6-3 se for necessária uma tolerância de falha adicional. Selecione o esquema 4-2 se os recursos de rede forem restritos. Se todos os outros fatores forem iguais, selecione 4-2 porque ele tem um número total menor de fragmentos.



Se você não tiver certeza de qual esquema usar, selecione 4 3 ou 2 ou 6 ou entre em Contato com o suporte técnico.

Esquemas de codificação de apagamento para pools de storage de um local

Um pool de storage de um local dá suporte a todos os esquemas de codificação de apagamento definidos para três ou mais locais, desde que o local tenha nós de storage suficientes.

O número mínimo de nós de storage necessário é $k+m$, mas é recomendável usar um pool de storage com $k+m +1$ nós de storage. Por exemplo, o esquema de codificação de apagamento 2 mais de 1 requer um pool de storage com no mínimo três nós de storage, mas quatro nós de storage são recomendados.

Esquema de codificação de apagamento (k)	Número mínimo de nós de storage	Número recomendado de nós de storage	Sobrecarga de storage
4-2	6	7	50%
6-2	8	9	33%
8-2	10	11	25%
6-+3	9	10	50%
9-+3	12	13	33%
2-+1	3	4	50%
4-+1	5	6	25%
6-+1	7	8	17%
7-+5	12	13	71%

Vantagens, desvantagens e requisitos para codificação de apagamento

Antes de decidir se deve usar a replicação ou a codificação de apagamento para proteger os dados do objeto contra perda, você deve entender as vantagens, desvantagens e os requisitos para codificação de apagamento.

Vantagens da codificação de apagamento

Em comparação com a replicação, a codificação de apagamento oferece maior confiabilidade, disponibilidade e eficiência de storage.

- **Confiabilidade:** A confiabilidade é medida em termos de tolerância a falhas - ou seja, o número de falhas simultâneas que podem ser sustentadas sem perda de dados. Com a replicação, várias cópias idênticas são armazenadas em nós diferentes e em locais diferentes. Com a codificação de apagamento, um objeto é codificado em dados e fragmentos de paridade e distribuído em muitos nós e sites. Essa dispersão fornece proteção contra falha de local e nó. Em comparação com a replicação, a codificação de apagamento oferece maior confiabilidade a custos de storage comparáveis.
- **Disponibilidade:** A disponibilidade pode ser definida como a capacidade de recuperar objetos se os nós de armazenamento falharem ou ficarem inacessíveis. Em comparação com a replicação, a codificação de apagamento oferece maior disponibilidade a custos de storage comparáveis.
- **Eficiência de storage:** Para níveis semelhantes de disponibilidade e confiabilidade, os objetos protegidos por meio da codificação de apagamento consomem menos espaço em disco do que os mesmos objetos se protegidos por meio da replicação. Por exemplo, um objeto de 10 MB replicado para dois locais consome 20 MB de espaço em disco (duas cópias), enquanto um objeto que é codificado de apagamento

em três locais com um esquema de codificação de apagamento 6-3 consome apenas 15 MB de espaço em disco.



O espaço em disco para objetos codificados por apagamento é calculado como o tamanho do objeto, além da sobrecarga de storage. A porcentagem de sobrecarga de storage é o número de fragmentos de paridade divididos pelo número de fragmentos de dados.

Desvantagens da codificação de apagamento

Quando comparada à replicação, a codificação de apagamento tem as seguintes desvantagens:

- Recomenda-se um número maior de nós e sites de storage, dependendo do esquema de codificação de apagamento. Em contraste, se você replicar dados de objeto, precisará de apenas um nó de storage para cada cópia. ["Esquemas de codificação de apagamento para pools de storage que contêm três ou mais locais"](#) Consulte e ["Esquemas de codificação de apagamento para pools de storage de um local"](#).
- Aumento do custo e complexidade das expansões de armazenamento. Para expandir uma implantação que usa replicação, você adiciona capacidade de storage em todos os locais onde são feitas cópias de objetos. Para expandir uma implantação que usa codificação de apagamento, você deve considerar tanto o esquema de codificação de apagamento em uso quanto o número total de nós de storage existentes. Por exemplo, se você esperar até que os nós existentes estejam 100% cheios, será necessário adicionar pelo menos $k+m$ nós de storage. No entanto, se você expandir quando os nós existentes estiverem 70% cheios, poderá adicionar dois nós por local e ainda maximizar a capacidade de storage utilizável. Para obter mais informações, ["Adicionar capacidade de storage para objetos codificados por apagamento"](#) consulte .
- Há maiores latências de recuperação quando você usa codificação de apagamento em sites distribuídos geograficamente. Os fragmentos de objeto para um objeto que é codificado de apagamento e distribuído entre locais remotos levam mais tempo para serem recuperados por conexões WAN do que um objeto que é replicado e disponível localmente (o mesmo local ao qual o cliente se conecta).
- Quando você usa codificação de apagamento em sites distribuídos geograficamente, há maior uso de tráfego de rede WAN para recuperações e reparos, especialmente para objetos recuperados com frequência ou para reparos de objetos em conexões de rede WAN.
- Quando você usa codificação de apagamento em todos os sites, a taxa de transferência máxima de objetos diminui drasticamente à medida que a latência de rede entre sites aumenta. Esta diminuição deve-se à diminuição correspondente da taxa de transferência da rede TCP, que afeta a rapidez com que o sistema StorageGRID pode armazenar e recuperar fragmentos de objeto.
- Maior uso de recursos de computação.

Quando usar codificação de apagamento

A codificação de apagamento é mais adequada para os seguintes requisitos:

- Objetos com mais de 1 MB de tamanho.



A codificação de apagamento é mais adequada para objetos com mais de 1 MB. Não use a codificação de apagamento para objetos com menos de 200 KB para evitar a sobrecarga de gerenciamento de fragmentos codificados de apagamento muito pequenos.

- Armazenamento a longo prazo ou a frio para conteúdo pouco recuperado.
- Alta disponibilidade e confiabilidade de dados.
- Proteção contra falhas completas no local e no nó.

- Eficiência de storage.
- Implantações de um único local que exigem proteção de dados eficiente com apenas uma cópia codificada de apagamento em vez de várias cópias replicadas.
- Implantações de vários locais em que a latência entre locais é inferior a 100 ms.

Como a retenção de objetos é determinada

O StorageGRID fornece opções para administradores de grade e usuários individuais de locatários especificarem por quanto tempo armazenar objetos. Em geral, todas as instruções de retenção fornecidas por um usuário locatário têm precedência sobre as instruções de retenção fornecidas pelo administrador da grade.

Como os usuários do locatário controlam a retenção de objetos

Os usuários do locatário têm três maneiras principais de controlar por quanto tempo seus objetos são armazenados no StorageGRID:

- Se a configuração global S3 Object Lock estiver ativada para a grade, os usuários do locatário S3 poderão criar buckets com o S3 Object Lock ativado e, em seguida, usar a API REST S3 para especificar as configurações de retenção de data e retenção legal para cada versão de objeto adicionada a esse bucket.
 - Uma versão de objeto que está sob uma retenção legal não pode ser excluída por nenhum método.
 - Antes que a data de retenção de uma versão de objeto seja alcançada, essa versão não pode ser excluída por nenhum método.
 - Objetos em buckets com o S3 Object Lock ativado são retidos pelo ILM "Forever." no entanto, após a data de retenção ser alcançada, uma versão de objeto pode ser excluída por uma solicitação de cliente ou a expiração do ciclo de vida do bucket. ["Gerencie objetos com o S3 Object Lock"](#) Consulte .
- S3 os usuários de locatários podem adicionar uma configuração de ciclo de vida aos buckets que especifica uma ação de expiração. Se existir um ciclo de vida de bucket, o StorageGRID armazena um objeto até que a data ou o número de dias especificados na ação de expiração sejam atendidos, a menos que o cliente exclua o objeto primeiro. ["Crie a configuração do ciclo de vida do S3"](#) Consulte .
- Um cliente S3 ou Swift pode emitir uma solicitação de exclusão de objeto. O StorageGRID sempre prioriza solicitações de exclusão de clientes ao longo do ciclo de vida do bucket S3 ou ILM ao determinar se deseja excluir ou reter um objeto.

Como os administradores de grade controlam a retenção de objetos

Os administradores de grade usam instruções de posicionamento ILM para controlar quanto tempo os objetos são armazenados. Quando os objetos são correspondidos por uma regra ILM, o StorageGRID armazena esses objetos até que o último período de tempo na regra ILM tenha decorrido. Os objetos são mantidos indefinidamente se for especificado para as instruções de colocação.

Independentemente de quem controla por quanto tempo os objetos são retidos, as configurações do ILM controlam quais tipos de cópias de objetos (replicadas ou codificadas para apagamento) são armazenadas e onde as cópias estão localizadas (nós de storage, pools de storage de nuvem ou nós de arquivamento).

Como o ciclo de vida do bucket do S3 e o ILM interagem

A ação de expiração em um ciclo de vida do bucket do S3 sempre substitui as configurações do ILM. Como resultado, um objeto pode ser retido na grade mesmo depois que quaisquer instruções ILM para colocar o objeto tenham expirado.

Exemplos para retenção de objetos

Para entender melhor as interações entre o bloqueio de objetos S3, as configurações do ciclo de vida do bucket, as solicitações de exclusão do cliente e o ILM, considere os exemplos a seguir.

Exemplo 1: O ciclo de vida do bucket S3 mantém objetos mais longos do que o ILM

ILM

Armazenar duas cópias por 1 ano (365 dias)

Ciclo de vida do balde

Expira objetos em 2 anos (730 dias)

Resultado

O StorageGRID armazena o objeto por 730 dias. O StorageGRID usa as configurações do ciclo de vida do bucket para determinar se deseja excluir ou reter um objeto.



Se o ciclo de vida do bucket especificar que os objetos devem ser mantidos por mais tempo do que o especificado pelo ILM, o StorageGRID continuará a usar as instruções de colocação do ILM ao determinar o número e o tipo de cópias a armazenar. Neste exemplo, duas cópias do objeto continuarão sendo armazenadas no StorageGRID de dias 366 a 730.

Exemplo 2: O ciclo de vida do bucket S3 expira objetos antes do ILM

ILM

Armazenar duas cópias por 2 anos (730 dias)

Ciclo de vida do balde

Expira objetos em 1 ano (365 dias)

Resultado

O StorageGRID exclui ambas as cópias do objeto após o dia 365.

Exemplo 3: A exclusão do cliente substitui o ciclo de vida do bucket e o ILM

ILM

Armazenar duas cópias em nós de storage para sempre

Ciclo de vida do balde

Expira objetos em 2 anos (730 dias)

Solicitação de exclusão do cliente

Emitido no dia 400

Resultado

O StorageGRID exclui ambas as cópias do objeto no dia 400 em resposta à solicitação de exclusão do cliente.

Exemplo 4: S3 Object Lock substitui a solicitação de exclusão do cliente

S3 bloqueio de objetos

Reter-até-data para uma versão de objeto é 2026-03-31. Uma retenção legal não está em vigor.

Regra ILM compatível

Armazene duas cópias em nós de storage para sempre.

Solicitação de exclusão do cliente

Emitido em 2024-03-31.

Resultado

O StorageGRID não excluirá a versão do objeto porque a data de retenção ainda está a 2 anos de distância.

Como os objetos são excluídos

O StorageGRID pode excluir objetos em resposta direta a uma solicitação de cliente ou automaticamente como resultado da expiração de um ciclo de vida de bucket do S3 ou dos requisitos da política do ILM. Entender as diferentes maneiras pelas quais os objetos podem ser excluídos e como o StorageGRID lida com solicitações de exclusão pode ajudar você a gerenciar objetos com mais eficiência.

O StorageGRID pode usar um dos dois métodos para excluir objetos:

- **Exclusão síncrona:** Quando o StorageGRID recebe uma solicitação de exclusão de cliente, todas as cópias de objeto são removidas imediatamente. O cliente é informado de que a exclusão foi bem-sucedida após as cópias terem sido removidas.
- **Os objetos são enfileirados para exclusão:** Quando o StorageGRID recebe uma solicitação de exclusão, o objeto é enfileirado para exclusão e o cliente é informado imediatamente de que a exclusão foi bem-sucedida. Cópias de objeto são removidas posteriormente pelo processamento ILM em segundo plano.

Ao excluir objetos, o StorageGRID usa o método que otimiza o desempenho de exclusão, minimiza possíveis backlogs de exclusão e libera espaço mais rapidamente.

A tabela resume quando o StorageGRID usa cada método.

Método de execução da exclusão	Quando utilizado
Os objetos estão na fila para exclusão	<p>Quando qualquer das seguintes condições for verdadeira:</p> <ul style="list-style-type: none"> • A exclusão automática de objetos foi acionada por um dos seguintes eventos: <ul style="list-style-type: none"> ◦ A data de expiração ou o número de dias na configuração do ciclo de vida de um bucket do S3 é atingida. ◦ O último período de tempo especificado em uma regra ILM decorre. <p>Observação: objetos em um bucket que tenha o bloqueio de objeto S3 ativado não podem ser excluídos se estiverem sob uma retenção legal ou se uma data de retenção até tiver sido especificada, mas ainda não cumprida.</p> <ul style="list-style-type: none"> • Um cliente S3 ou Swift solicita a exclusão e uma ou mais destas condições é verdadeira: <ul style="list-style-type: none"> ◦ As cópias não podem ser excluídas dentro de 30 segundos porque, por exemplo, um local de objeto está temporariamente indisponível. ◦ As filas de exclusão em segundo plano estão ociosas.
Os objetos são removidos imediatamente (exclusão síncrona)	<p>Quando um cliente S3 ou Swift faz uma solicitação de exclusão e todas das seguintes condições são atendidas:</p> <ul style="list-style-type: none"> • Todas as cópias podem ser removidas dentro de 30 segundos. • As filas de exclusão em segundo plano contêm objetos a serem processados.

Quando os clientes S3 ou Swift fazem solicitações de exclusão, o StorageGRID começa adicionando objetos à fila de exclusão. Em seguida, ele alterna para executar a exclusão síncrona. Certificar-se de que a fila de exclusão em segundo plano tem objetos para processar permite que o StorageGRID processe exclusões de forma mais eficiente, especialmente para clientes de baixa simultaneidade, ao mesmo tempo que ajuda a impedir que o cliente exclua backlogs.

Tempo necessário para excluir objetos

A forma como o StorageGRID exclui objetos pode afetar o desempenho do sistema:

- Quando o StorageGRID executa a exclusão síncrona, pode levar StorageGRID até 30 segundos para retornar um resultado ao cliente. Isso significa que a exclusão pode parecer estar acontecendo mais lentamente, mesmo que as cópias estejam sendo removidas mais rapidamente do que quando o StorageGRID coloca objetos em fila para exclusão.
- Se você estiver monitorando de perto o desempenho de exclusão durante uma exclusão em massa, você pode notar que a taxa de exclusão parece diminuir depois que um certo número de objetos foi excluído. Essa alteração ocorre quando o StorageGRID muda de enfileirar objetos para exclusão para a execução da exclusão síncrona. A aparente redução na taxa de exclusão não significa que as cópias de objetos estejam sendo removidas mais lentamente. Pelo contrário, indica que, em média, o espaço está agora a ser libertado mais rapidamente.

Se você estiver excluindo grandes números de objetos e sua prioridade for liberar espaço rapidamente, considere usar uma solicitação de cliente para excluir objetos em vez de excluí-los usando ILM ou outros métodos. Em geral, o espaço é liberado mais rapidamente quando a exclusão é realizada pelos clientes porque o StorageGRID pode usar a exclusão síncrona.

A quantidade de tempo necessário para liberar espaço depois que um objeto é excluído depende de vários fatores:

- Se as cópias de objetos são removidas de forma síncrona ou estão em fila para serem removidas posteriormente (para solicitações de exclusão de clientes).
- Outros fatores, como o número de objetos na grade ou a disponibilidade de recursos da grade quando as cópias de objetos são enfileiradas para remoção (para exclusões de clientes e outros métodos).

Como objetos com versão S3 são excluídos

Quando o controle de versão está habilitado para um bucket do S3, o StorageGRID segue o comportamento do Amazon S3 ao responder a solicitações de exclusão, sejam elas provenientes de um cliente S3, a expiração de um ciclo de vida de bucket do S3 ou os requisitos da política do ILM.

Quando os objetos são versionados, as solicitações de exclusão de objetos não excluem a versão atual do objeto e não libertam espaço. Em vez disso, uma solicitação de exclusão de objeto cria um marcador de exclusão como a versão atual do objeto, o que torna a versão anterior do objeto "não atual".

Mesmo que o objeto não tenha sido removido, o StorageGRID se comporta como se a versão atual do objeto não estivesse mais disponível. Solicitações para esse objeto retornam 404 Not Found. No entanto, como os dados de objetos não atuais não foram removidos, as solicitações que especificam uma versão não atual do objeto podem ser bem-sucedidas.

Para liberar espaço ao excluir objetos com controle de versão, use um dos seguintes itens:

- **Solicitação de cliente S3:** Especifique o ID da versão do objeto na solicitação DE EXCLUSÃO de objeto S3 (`DELETE /object?versionId=ID`). Tenha em mente que essa solicitação só remove cópias de objetos para a versão especificada (as outras versões ainda estão ocupando espaço).
- **Ciclo de vida do bucket:** Use a `NoncurrentVersionExpiration` ação na configuração do ciclo de vida do bucket. Quando o número de dias não-correntes especificado é atendido, o StorageGRID remove permanentemente todas as cópias de versões de objetos não-atuais. Essas versões de objeto não podem ser recuperadas.

A `NewerNoncurrentVersions` ação na configuração do ciclo de vida do bucket especifica o número de versões não atuais retidas em um bucket S3 com versão. Se houver mais versões não atuais do que `NewerNoncurrentVersions` o especificado, o StorageGRID removerá as versões mais antigas assim que o valor não-atual tiver decorrido. O `NewerNoncurrentVersions` limite substitui as regras de ciclo de vida fornecidas pelo ILM, o que significa que um objeto não atual com uma versão dentro do `NewerNoncurrentVersions` limite é retido se o ILM solicitar sua exclusão.

- **ILM: "Clonar a política ativa"** E adicione duas regras ILM à nova política proposta:
 - Primeira regra: Use ""hora não atual" como tempo de referência para corresponder às versões não atuais do objeto. No ["Etapa 1 \(Digite detalhes\) do assistente criar uma regra ILM"](#), selecione **Sim** para a pergunta, ""aplicar esta regra apenas a versões de objetos mais antigas (em buckets do S3 com controle de versão habilitado)?"
 - Segunda regra: Use **tempo de ingestão** para corresponder à versão atual. A regra "hora não atual" deve aparecer na política acima da regra **tempo de ingestão**.

Como S3 excluir marcadores são excluídos

Quando um objeto com controle de versão é excluído, o StorageGRID cria um marcador de exclusão como a versão atual do objeto. Para remover o marcador de exclusão de byte zero do intervalo, o cliente S3 deve excluir explicitamente a versão do objeto. Os marcadores de exclusão não são removidos pelo ILM, regras de ciclo de vida do bucket ou Excluir objetos em operações de bucket.

Informações relacionadas

- ["USE A API REST DO S3"](#)
- ["Exemplo 4: Regras ILM e política para objetos com versão S3"](#)

Criar e atribuir notas de armazenamento

Os graus de armazenamento identificam o tipo de armazenamento usado por um nó de armazenamento. Você pode criar classes de storage se quiser que as regras do ILM coloquem determinados objetos em determinados nós de storage.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem permissões de acesso específicas.

Sobre esta tarefa

Quando você instala o StorageGRID pela primeira vez, o nível de armazenamento **padrão** é atribuído automaticamente a cada nó de armazenamento no sistema. Conforme necessário, você pode, opcionalmente, definir categorias de storage personalizadas e atribuí-las a diferentes nós de storage.

O uso de classes de armazenamento personalizadas permite criar pools de armazenamento ILM que contêm apenas um tipo específico de nó de armazenamento. Por exemplo, você pode querer que certos objetos sejam armazenados em seus nós de storage mais rápidos, como dispositivos de storage all-flash StorageGRID.

Se o grau de armazenamento não for um problema (por exemplo, todos os nós de armazenamento são idênticos), você pode ignorar este procedimento e usar a seleção **inclui todas as classes de armazenamento** para o grau de armazenamento quando ["crie pools de armazenamento"](#) você . O uso dessa seleção garante que o pool de armazenamento incluirá todos os nós de armazenamento no local, independentemente de seu nível de armazenamento.



Não crie mais notas de armazenamento do que o necessário. Por exemplo, não crie um nível de armazenamento para cada nó de armazenamento. Em vez disso, atribua cada nível de storage a dois ou mais nós. Os graus de armazenamento atribuídos a apenas um nó podem causar backlogs de ILM se esse nó ficar indisponível.

Passos

1. Selecione **ILM > classes de armazenamento**.
2. Definir graus de armazenamento personalizados:
 - a. Para cada grau de armazenamento personalizado que você deseja adicionar, selecione **Inserir**
 - b. Introduza uma etiqueta descritiva.



Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	<input type="text" value="disk"/>	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

c. Selecione **aplicar alterações**.

d. Opcionalmente, se você precisar modificar um rótulo salvo, selecione **Editar** e selecione **aplicar alterações**.



Não é possível excluir graus de armazenamento.

3. Atribuir novos graus de storage aos nós de storage:

a. Localize o nó de armazenamento na lista LDR e selecione o ícone **Editar** .

b. Selecione o grau de armazenamento adequado na lista.



LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default disk	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes



Atribua um nível de storage a um determinado nó de storage somente uma vez. Um nó de armazenamento recuperado de falha mantém o grau de armazenamento atribuído anteriormente. Não altere esta atribuição depois de a política ILM estar ativada. Se a atribuição for alterada, os dados serão armazenados com base no novo nível de armazenamento.

- Selecione **aplicar alterações**.

Use pools de armazenamento

O que é um pool de storage?

Um pool de storage é um agrupamento lógico de nós de storage ou nós de arquivamento.

Quando você instala o StorageGRID, um pool de storage por site é criado automaticamente. Você pode configurar pools de storage adicionais conforme necessário para seus requisitos de storage.



O suporte para nós de arquivamento (tanto para arquivamento na nuvem usando a API S3 como para arquivamento em fita usando middleware TSM) está obsoleto e será removido em uma versão futura. Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo foi substituído pelo ILM Cloud Storage Pools, que oferece mais funcionalidade.

["Use Cloud Storage Pools"](#) Consulte .

Os pools de armazenamento têm dois atributos:

- **Storage grade:** Para nós de storage, o desempenho relativo do armazenamento de backup.
- **Site:** O centro de dados onde os objetos serão armazenados.

Os pools de armazenamento são usados em regras ILM para determinar onde os dados do objeto são armazenados e o tipo de armazenamento usado. Ao configurar regras de ILM para replicação, você seleciona um ou mais pools de storage que incluem nós de storage ou nós de arquivamento. Ao criar perfis de codificação de apagamento, você seleciona um pool de storage que inclui nós de storage.

Diretrizes para a criação de pools de armazenamento

Configure e use pools de storage para se proteger contra a perda de dados, distribuindo dados em vários locais. As cópias replicadas e as cópias codificadas por apagamento exigem configurações de pool de storage diferentes.

["Exemplos de ativação da proteção contra perda de sites usando replicação e codificação de apagamento"](#) Consulte .

Diretrizes para todos os pools de armazenamento

- Mantenha as configurações do pool de storage o mais simples possível. Não crie mais pools de armazenamento do que o necessário.
- Crie pools de storage com tantos nós quanto possível. Cada pool de storage deve conter dois ou mais nós. Um pool de storage com nós insuficientes pode causar backlogs de ILM se um nó ficar indisponível.
- Evite criar ou usar pools de storage que se sobrepõem (contêm um ou mais dos mesmos nós). Se os pools de armazenamento se sobrepuserem, mais de uma cópia dos dados de objeto poderá ser salva no mesmo nó.
- Em geral, não use o pool de storage todos os nós de storage (StorageGRID 11,6 e anterior) ou o site todos os sites. Esses itens são atualizados automaticamente para incluir novos sites adicionados em uma expansão, o que pode não ser o comportamento desejado.

Diretrizes para pools de storage usados para cópias replicadas

- Para proteção contra perda de local usando ["replicação"](#)o , especifique um ou mais pools de armazenamento específicos do local no ["Instruções de colocação para cada regra ILM"](#).

Um pool de storage é criado automaticamente para cada local durante a instalação do StorageGRID.

O uso de um pool de storage para cada local garante que as cópias de objetos replicadas sejam colocadas exatamente onde você espera (por exemplo, uma cópia de cada objeto em cada local para proteção contra perda de local).

- Se você adicionar um site em uma expansão, crie um novo pool de armazenamento que contenha apenas o novo site. Em seguida ["Atualizar regras ILM"](#), para controlar quais objetos são armazenados no novo site.
- Se o número de cópias for menor que o número de pools de storage, o sistema as distribuirá para equilibrar a utilização de disco entre os pools.
- Se os pools de storage se sobreporem (contiverem os mesmos nós de storage), todas as cópias do objeto poderão ser salvas em apenas um local. Você deve garantir que os pools de storage selecionados não contenham os mesmos nós de storage.

Diretrizes para pools de storage usados para cópias codificadas por apagamento

- Para proteção contra perda de local usando ["codificação de apagamento"](#)o , crie pools de armazenamento que consistem em pelo menos três locais. Se um pool de armazenamento incluir apenas dois sites, você não poderá usar esse pool de armazenamento para codificação de apagamento. Não há esquemas de

codificação de apagamento disponíveis para um pool de storage que tenha dois locais.

- O número de nós de storage e sites contidos no pool de storage determina quais ["esquemas de codificação de apagamento"](#) estão disponíveis.
- Se possível, um pool de storage deve incluir mais do que o número mínimo de nós de storage necessário para o esquema de codificação de apagamento selecionado. Por exemplo, se você usar um 3 esquema de codificação de apagamento de mais de 6 anos, precisará ter pelo menos nove nós de storage. No entanto, é recomendável ter pelo menos um nó de armazenamento adicional por local.
- Distribua os nós de storage entre locais da forma mais uniforme possível. Por exemplo, para dar suporte a um 3 esquema de codificação de apagamento de mais de 6 horas por dia, configure um pool de storage que inclua pelo menos três nós de storage em três locais.
- Se você tiver altos requisitos de taxa de transferência, usar um pool de armazenamento que inclua vários locais não é recomendado se a latência de rede entre locais for maior que 100 ms. À medida que a latência aumenta, a taxa na qual o StorageGRID pode criar, colocar e recuperar fragmentos de objetos diminui drasticamente devido à diminuição da taxa de transferência da rede TCP.

A diminuição na taxa de transferência afeta as taxas máximas alcançáveis de ingestão e recuperação de objetos (quando balanceado ou rigoroso são selecionados como o comportamento de ingestão) ou pode levar a backlogs de fila ILM (quando Dual Commit é selecionado como o comportamento de ingestão). ["Comportamento de ingestão de regra de ILM"](#) Consulte .



Se a grade incluir apenas um local, você será impedido de usar o pool de storage todos os nós de storage (StorageGRID 11,6 e anterior) ou o site padrão todos os sites em um perfil de codificação de apagamento. Esse comportamento impede que o perfil se torne inválido se um segundo site for adicionado.

- Não é possível usar nós de arquivamento para dados codificados por apagamento.

Diretrizes para pools de storage usados para cópias arquivadas



O suporte para nós de arquivamento (tanto para arquivamento na nuvem usando a API S3 como para arquivamento em fita usando middleware TSM) está obsoleto e será removido em uma versão futura. Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo foi substituído pelo ILM Cloud Storage Pools, que oferece mais funcionalidade.

["Migre objetos para um Cloud Storage Pool"](#) Consulte .

Além disso, você deve remover nós de arquivamento da política ILM ativa no StorageGRID 11,7 ou anterior. A remoção de dados de objetos armazenados nos nós de arquivamento simplificará futuras atualizações. ["Trabalhando com regras de ILM e políticas de ILM"](#) Consulte .

- Não é possível criar um pool de storage que inclua nós de storage e nós de arquivamento. As cópias arquivadas exigem um pool de storage que inclua apenas nós de arquivamento.
- Ao usar um pool de storage que inclua nós de arquivamento, você também deve manter pelo menos uma cópia replicada ou codificada de apagamento em um pool de storage que inclua nós de storage.
- Se a configuração global S3 Object Lock estiver ativada e você estiver criando uma regra ILM compatível, não será possível usar um pool de armazenamento que inclua nós de arquivamento. Consulte as instruções para gerenciar objetos com o S3 Object Lock.
- Se o tipo de destino de um nó de arquivamento for Cloud Tiering - Simple Storage Service (S3), o nó de arquivamento deverá estar em seu próprio pool de storage.

Ativar a proteção contra perda de local

Se a implantação do StorageGRID incluir mais de um local, você poderá usar a replicação e a codificação de apagamento com pools de storage configurados adequadamente para habilitar a proteção contra perda de site.

A replicação e a codificação de apagamento exigem configurações diferentes de pool de storage:

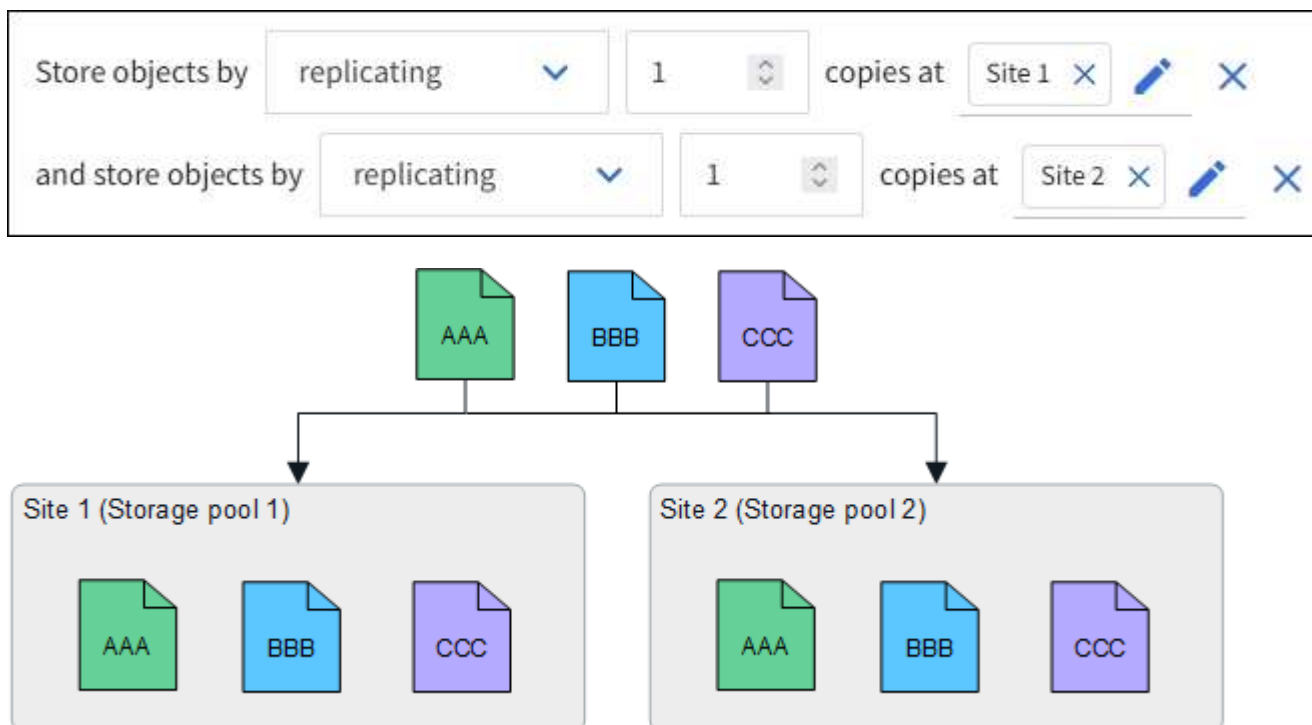
- Para usar a replicação para proteção contra perda de site, use os pools de storage específicos do local que são criados automaticamente durante a instalação do StorageGRID. Em seguida, crie regras ILM com "instruções de colocação" que especificam vários pools de armazenamento de modo que uma cópia de cada objeto seja colocada em cada local.
- Para usar a codificação de apagamento para proteção contra perda de site "crie pools de armazenamento que consistem em vários locais", . Em seguida, crie regras ILM que usam um pool de armazenamento que consiste em vários sites e qualquer esquema de codificação de apagamento disponível.

Exemplo de replicação

Por padrão, um pool de armazenamento é criado para cada local durante a instalação do StorageGRID. Ter pools de storage que consistem em apenas um local permite configurar regras de ILM que usam replicação para proteção contra perda de site. Neste exemplo:

- O pool de armazenamento 1 contém o local 1
- O pool de armazenamento 2 contém o local 2
- A regra ILM contém dois posicionamentos:
 - Armazene objetos replicando cópia 1 no local 1
 - Armazene objetos replicando cópia 1 no local 2

Colocações de regra ILM:



Se um site for perdido, cópias dos objetos estarão disponíveis no outro site.

Exemplo de codificação de apagamento

Ter pools de storage compostos por mais de um local por pool de storage permite configurar regras de ILM que usam codificação de apagamento para proteção contra perda de site. Neste exemplo:

- O pool de armazenamento 1 contém os locais 1 a 3
- A regra ILM contém um posicionamento: Armazenar objetos por codificação de apagamento usando um esquema EC 4-2 no pool de armazenamento 1, que contém três locais

Colocações de regra ILM:



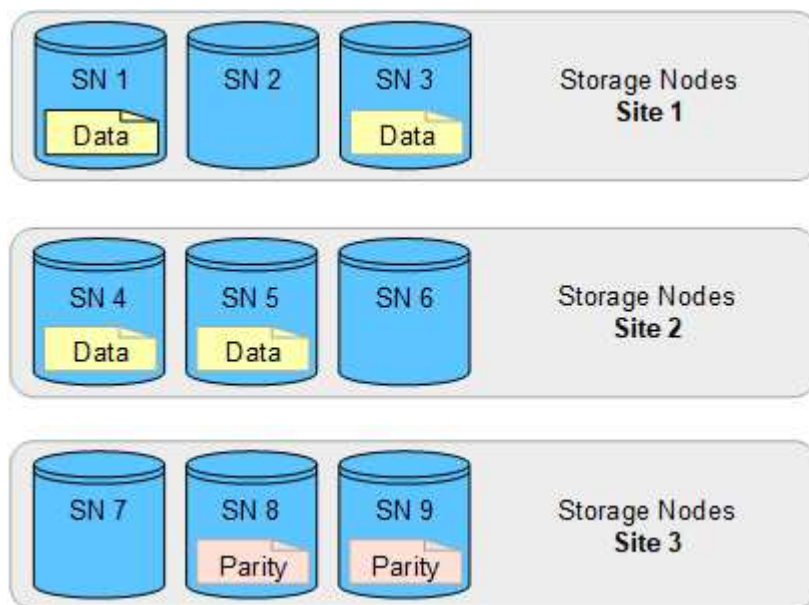
Neste exemplo:

- A regra ILM usa um esquema de codificação de apagamento 4-2.
- Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados do objeto.
- Cada um dos seis fragmentos é armazenado em um nó diferente em três locais de data center para fornecer proteção de dados para falhas de nós ou perda de local.



A codificação de apagamento é permitida em pools de armazenamento contendo qualquer número de sites *exceto* dois sites.

Regra ILM usando o esquema de codificação de apagamento 4-2:



Se um site for perdido, os dados ainda podem ser recuperados:

Crie um pool de armazenamento

Você cria pools de storage para determinar onde o sistema StorageGRID armazena dados de objetos e o tipo de storage usado. Cada pool de storage inclui um ou mais locais e um ou mais tipos de storage.



Quando você instala o StorageGRID 11,7 em uma nova grade, os pools de armazenamento são criados automaticamente para cada local para reduzir o número de etapas necessárias para criar novas regras de ILM. No entanto, durante as atualizações para o StorageGRID 11,7, os pools de armazenamento não são criados para cada local.

Se você quiser criar pools de armazenamento em nuvem para armazenar dados de objetos fora do sistema StorageGRID, consulte "[Informações sobre como usar Cloud Storage Pools](#)".

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador da web suportado](#)".
- Você tem permissões de acesso específicas.
- Você revisou as diretrizes para a criação de pools de armazenamento.

Sobre esta tarefa

Os pools de storage determinam onde os dados do objeto são armazenados. O número de pools de storage de que você precisa depende do número de locais na grade e dos tipos de cópias que você deseja: Replicados ou codificados para apagamento.

- Para replicação e codificação de apagamento de um único local, crie um pool de storage para cada local. Por exemplo, se você quiser armazenar cópias de objetos replicadas em três locais, crie três pools de storage.
- Para codificação de apagamento em três ou mais locais, crie um pool de storage que inclua uma entrada para cada local. Por exemplo, se você quiser apagar objetos de código em três locais, crie um pool de storage.



Não inclua o site todos os sites em um pool de armazenamento que será usado em um perfil de codificação de apagamento. Em vez disso, adicione uma entrada separada ao pool de storage para cada local que armazenará dados codificados de apagamento. [este passo](#) Consulte para obter um exemplo.

- Se você tiver mais de um nível de armazenamento, não crie um pool de armazenamento que inclua diferentes graus de armazenamento em um único local. Consulte "[Diretrizes para a criação de pools de armazenamento](#)".

Passos

1. Selecione **ILM > Storage Pools**.

A guia pools de armazenamento lista todos os pools de armazenamento definidos.



Para novas instalações do StorageGRID 11,6 ou anterior, o pool de storage de todos os nós de storage é atualizado automaticamente sempre que você adiciona novos locais de data center. Não use esse pool nas regras do ILM.

2. Para criar um novo pool de armazenamento, selecione **criar**.

3. Insira um nome exclusivo para o pool de armazenamento. Use um nome que será fácil de identificar quando você configurar perfis de codificação de apagamento e regras ILM.
4. Na lista suspensa **Site**, selecione um site para esse pool de armazenamento.

Quando você seleciona um site, o número de nós de storage e nós de arquivamento na tabela é atualizado automaticamente.

Em geral, não use o site todos os sites em nenhum pool de armazenamento. As regras de ILM que usam um pool de armazenamento de todos os sites colocam objetos em qualquer site disponível, proporcionando menos controle sobre o posicionamento de objetos. Além disso, um pool de storage All Sites usa os nós de storage em um novo local imediatamente, o que pode não ser o comportamento esperado.

5. Na lista suspensa **Storage grade**, selecione o tipo de armazenamento que será usado se uma regra ILM usar esse pool de armazenamento.

O nível de storage, inclui todos os tipos de storage, inclui todos os nós de storage no local selecionado. O grau de storage padrão dos nós de arquivamento inclui todos os nós de arquivamento no local selecionado. Se você criou graus de storage adicionais para os nós de storage na grade, eles serão listados na lista suspensa.

6. se você quiser usar o pool de armazenamento em um perfil de codificação de apagamento de vários sites, selecione **Add More Nodes** para adicionar uma entrada para cada site ao pool de armazenamento.



Não é possível criar entradas duplicadas ou criar um pool de storage que inclua o nível de storage dos nós de arquivamento e qualquer tipo de storage que contenha nós de storage.

Você será avisado se você adicionar mais de uma entrada com diferentes graus de armazenamento para um site.

Para remover uma entrada, selecione o ícone de exclusão **X**.

7. Quando estiver satisfeito com suas seleções, selecione **Salvar**.

O novo pool de armazenamento é adicionado à lista.

Veja os detalhes do pool de armazenamento

Você pode visualizar os detalhes de um pool de storage para determinar onde o pool de storage é usado e ver quais nós e categorias de storage estão incluídos.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem permissões de acesso específicas.

Passos

1. Selecione **ILM > Storage Pools**.

A tabela Storage Pools inclui as seguintes informações para cada pool de storage que inclui nós de storage:

- **Nome:** O nome de exibição exclusivo do pool de armazenamento.

- **Contagem de nós:** O número de nós no pool de storage.
- **Uso do armazenamento:** A porcentagem do espaço utilizável total que foi usado para dados de objeto neste nó. Esse valor não inclui metadados de objetos.
- **Capacidade total:** O tamanho do pool de armazenamento, que é igual à quantidade total de espaço utilizável para dados de objetos para todos os nós no pool de armazenamento.
- **Uso de ILM:** Como o pool de armazenamento está sendo usado atualmente. Um pool de storage pode não ser usado ou pode ser usado em uma ou mais regras do ILM, perfis de codificação de apagamento ou ambos.



Você não pode remover um pool de armazenamento se ele estiver sendo usado.

2. Para exibir detalhes sobre um pool de armazenamento específico, selecione seu nome.

A página de detalhes do pool de armazenamento é exibida.

3. Exiba a guia **nós** para saber mais sobre os nós de armazenamento ou nós de arquivamento incluídos no pool de armazenamento.

A tabela inclui as seguintes informações para cada nó:

- Nome do nó
- Nome do local
- Grau de armazenamento
- Uso de storage (%): A porcentagem do espaço utilizável total para dados de objetos que foi usado para o nó de storage. Este campo não está visível para pools de nós de arquivo.



O mesmo valor de uso de armazenamento (%) também é mostrado no gráfico armazenamento usado - dados de objetos para cada nó de armazenamento (selecione **NÓS > Storage Node > Storage**).

4. Selecione a guia **uso de ILM** para determinar se o pool de armazenamento está sendo usado atualmente em quaisquer regras de ILM ou perfis de codificação de apagamento.
5. Opcionalmente, vá para a página **regras ILM** para saber mais e gerenciar quaisquer regras que usem o pool de armazenamento.

Consulte "[Instruções para trabalhar com regras ILM](#)".

Editar pool de armazenamento

Você pode editar um pool de armazenamento para alterar seu nome ou atualizar sites e classes de armazenamento.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador da web suportado](#)".
- Você tem permissões de acesso específicas.
- Você revisou o "[diretrizes para a criação de pools de armazenamento](#)".
- Se você planeja editar um pool de armazenamento que é usado por uma regra na política ILM ativa, você considerou como suas alterações afetarão o posicionamento dos dados do objeto.

Sobre esta tarefa

Se você estiver adicionando um novo local ou nível de storage a um pool de storage usado na política de ILM ativa, saiba que os nós de storage no novo local ou nível de storage não serão usados automaticamente. Para forçar o StorageGRID a usar um novo local ou nível de armazenamento, você deve ativar uma nova política de ILM depois de salvar o pool de armazenamento editado.

Passos

1. Selecione **ILM > Storage Pools**.
2. Marque a caixa de seleção do pool de armazenamento que deseja editar.

Não é possível editar o pool de storage de todos os nós de storage (StorageGRID 11,6 e anterior).

3. Selecione **Editar**.
4. Conforme necessário, altere o nome do pool de armazenamento.
5. Conforme necessário, selecione outros locais e categorias de armazenamento.



Você é impedido de alterar o local ou o nível de armazenamento se o pool de armazenamento for usado em um perfil de codificação de apagamento e a alteração fizer com que o esquema de codificação de apagamento se torne inválido. Por exemplo, se um pool de armazenamento usado em um perfil de codificação de apagamento incluir atualmente um grau de armazenamento com apenas um local, você será impedido de usar um grau de armazenamento com dois sites porque a alteração tornaria o esquema de codificação de apagamento inválido.

6. Selecione **Guardar**.

Depois de terminar

Se você adicionou um novo local ou nível de armazenamento a um pool de armazenamento usado na política ILM ativa, ative uma nova política ILM para forçar o StorageGRID a usar o novo local ou nível de armazenamento. Por exemplo, clone sua política ILM existente e, em seguida, ative o clone. ["Trabalhe com regras ILM e políticas ILM"](#) Consulte .

Remova um pool de armazenamento

Você pode remover um pool de armazenamento que não está sendo usado.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["permissões de acesso necessárias"](#).

Passos

1. Selecione **ILM > Storage Pools**.
2. Observe a coluna de uso do ILM na tabela para determinar se você pode remover o pool de armazenamento.

Não é possível remover um pool de armazenamento se ele estiver sendo usado em uma regra ILM ou em um perfil de codificação de apagamento. Conforme necessário, selecione **storage pool name > ILM usage** para determinar onde o pool de armazenamento é usado.

3. Se o pool de armazenamento que você deseja remover não estiver sendo usado, marque a caixa de

seleção.

4. Selecione **Remove**.

5. Selecione **OK**.

Use Cloud Storage Pools

O que é um Cloud Storage Pool?

Um pool de armazenamento em nuvem permite que você use o ILM para mover dados de objetos para fora do seu sistema StorageGRID. Por exemplo, você pode migrar objetos acessados com pouca frequência para storage de nuvem de baixo custo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou a categoria Acesso de arquivamento no storage de Blobs do Microsoft Azure. Ou, talvez você queira manter um backup na nuvem de objetos do StorageGRID para aprimorar a recuperação de desastres.

Do ponto de vista do ILM, um Cloud Storage Pool é semelhante a um pool de storage. Para armazenar objetos em qualquer local, selecione o pool ao criar as instruções de posicionamento para uma regra ILM. No entanto, embora os pools de storage consistam em nós de storage ou nós de arquivamento no sistema StorageGRID, um pool de storage de nuvem consiste em um bucket externo (S3) ou contêiner (storage Blob do Azure).



Mover objetos de um nó de arquivo para um sistema de armazenamento de arquivamento externo por meio da API S3 foi obsoleto e foi substituído por ILM Cloud Storage Pools, que oferecem mais funcionalidade. Se você estiver usando um nó de arquivamento com a opção Cloud Tiering - Simple Storage Service (S3), ["Migre seus objetos para um Cloud Storage Pool"](#) em vez disso.

A tabela compara pools de armazenamento com pools de armazenamento em nuvem e mostra as semelhanças e diferenças de alto nível.

	Pool de storage	Cloud Storage Pool
Como é criado?	Usando a opção ILM > Storage Pools no Gerenciador de Grade.	Usando a opção ILM > Storage Pools > Cloud Storage Pools no Grid Manager. Você deve configurar o bucket externo ou o contêiner antes de criar o pool de storage de nuvem.
Quantas piscinas você pode criar?	Ilimitado.	Até 10 TB.

	Pool de storage	Cloud Storage Pool
Onde os objetos são armazenados?	Em um ou mais nós de storage ou nós de arquivamento no StorageGRID.	<p>No bucket do Amazon S3, o contêiner de storage do Azure Blob ou o Google Cloud externo ao sistema StorageGRID.</p> <p>Se o Cloud Storage Pool for um bucket do Amazon S3:</p> <ul style="list-style-type: none"> • Opcionalmente, é possível configurar um ciclo de vida do bucket para migrar objetos para storage de baixo custo e longo prazo, como Amazon S3 Glacier ou S3 Glacier Deep Archive. O sistema de storage externo deve oferecer suporte à classe de storage Glacier e à API de restauração PÓS-objeto S3. • Você pode criar pools de armazenamento na nuvem para uso com os Serviços comerciais da AWS (C2S), que oferecem suporte à região secreta da AWS. <p>Se o pool de storage de nuvem for um contêiner de storage de Blob do Azure, o StorageGRID fará a transição do objeto para a categoria Archive.</p> <p>Observação: em geral, não configure o gerenciamento do ciclo de vida de armazenamento do Blob do Azure para o contêiner usado em um pool de storage do Cloud Storage. As operações de restauração PÓS-objeto em objetos no Cloud Storage Pool podem ser afetadas pelo ciclo de vida configurado.</p>
O que controla o posicionamento do objeto?	Uma regra ILM na política ILM ativa.	Uma regra ILM na política ILM ativa.
Que método de proteção de dados é usado?	Replicação ou codificação de apagamento.	Replicação.
Quantas cópias de cada objeto são permitidas?	Vários.	<p>Uma cópia no pool de storage de nuvem e, opcionalmente, uma ou mais cópias no StorageGRID.</p> <p>Observação: você não pode armazenar um objeto em mais de um pool de armazenamento em nuvem a qualquer momento.</p>
Quais são as vantagens?	Os objetos são rapidamente acessíveis a qualquer momento.	Armazenamento de baixo custo.
		Nota: Os dados do FabricPool não podem ser dispostos em camadas nos pools de armazenamento em nuvem. Os objetos com bloqueio de objeto S3 ativado não podem ser colocados em pools de armazenamento em nuvem.

Ciclo de vida de um objeto Cloud Storage Pool

Antes de implementar Cloud Storage Pools, revise o ciclo de vida dos objetos armazenados em cada tipo de Cloud Storage Pool.

- [S3: Ciclo de vida de um objeto Cloud Storage Pool](#)
- [Azure: Ciclo de vida de um objeto Cloud Storage Pool](#)

S3: Ciclo de vida de um objeto Cloud Storage Pool

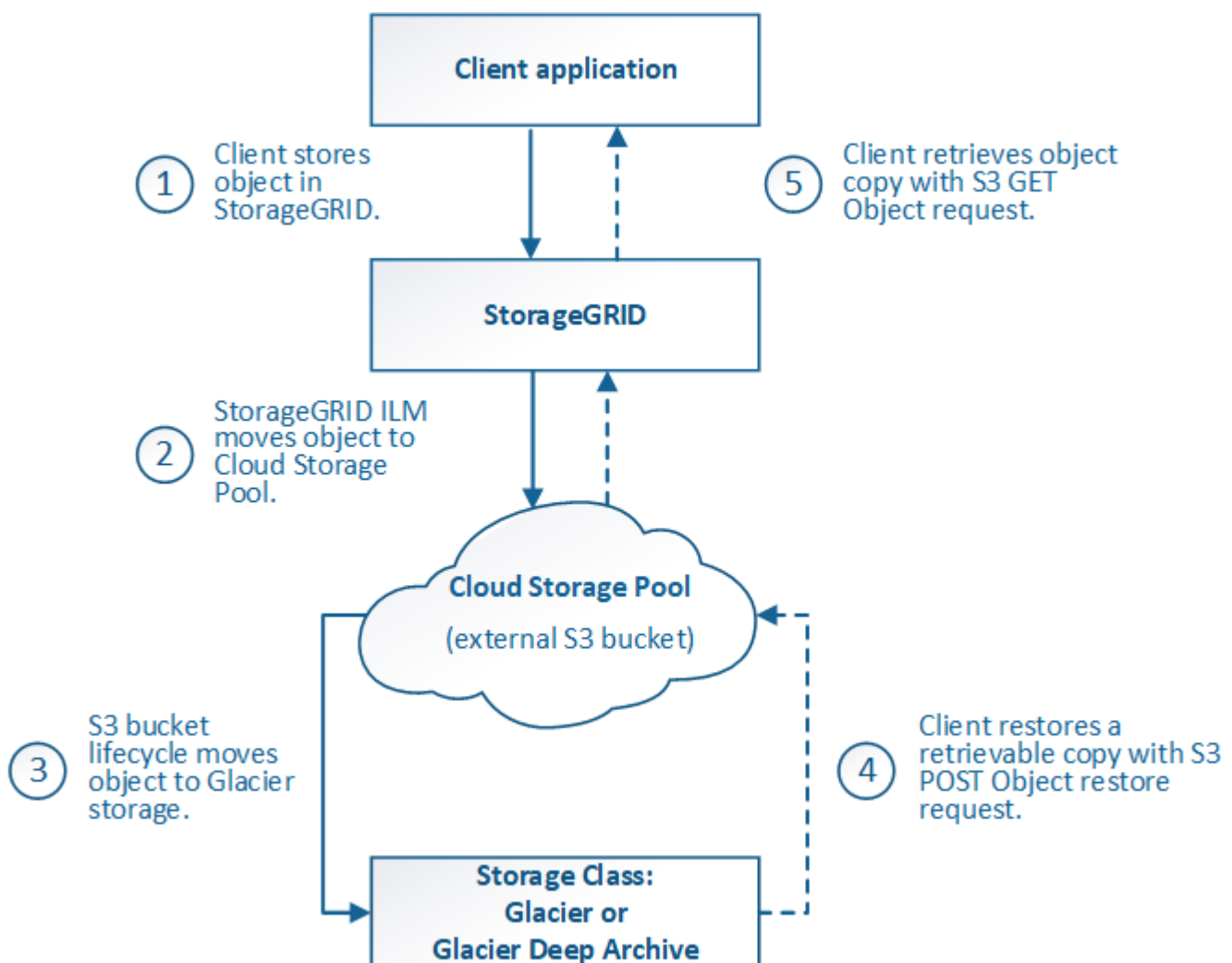
A figura mostra os estágios do ciclo de vida de um objeto que é armazenado em um pool de armazenamento em nuvem do S3.



Na figura e explicações, "Glacier" refere-se à classe de armazenamento Glacier e à classe de armazenamento Glacier Deep Archive, com uma exceção: A classe de armazenamento Glacier Deep Archive não suporta o nível de restauração Expedited. Apenas a recuperação em massa ou padrão é suportada.



O Google Cloud Platform (GCP) oferece suporte à recuperação de objetos de armazenamento de longo prazo sem exigir uma operação PÓS-restauração.



1. Objeto armazenado no StorageGRID

Para iniciar o ciclo de vida, um aplicativo cliente armazena um objeto no StorageGRID.

2. Objeto movido para o pool de armazenamento em nuvem S3

- Quando o objeto é correspondido por uma regra ILM que usa um pool de armazenamento em nuvem S3 como local de colocação, o StorageGRID move o objeto para o bucket externo S3 especificado pelo pool de armazenamento em nuvem.
- Quando o objeto for movido para o pool de armazenamento em nuvem S3, o aplicativo cliente poderá recuperá-lo usando uma solicitação de objeto S3 GET do StorageGRID, a menos que o objeto tenha sido transferido para o armazenamento Glacier.

3. Objeto transicionado para Glacier (estado não recuperável)

- Opcionalmente, o objeto pode ser transferido para o armazenamento Glacier. Por exemplo, o bucket externo do S3 pode usar a configuração do ciclo de vida para fazer a transição de um objeto para o armazenamento do Glacier imediatamente ou após algum número de dias.



Se você quiser fazer a transição de objetos, crie uma configuração de ciclo de vida para o bucket externo do S3 e use uma solução de armazenamento que implemente a classe de armazenamento Glacier e ofereça suporte à API de restauração PÓS-objetos do S3.



Não use Cloud Storage Pools para objetos que foram ingeridos por clientes Swift. O Swift não suporta solicitações de restauração PÓS-objeto, portanto, o StorageGRID não poderá recuperar quaisquer objetos Swift que tenham sido transferidos para o armazenamento do Glacier S3. Emitir uma solicitação de objeto Swift GET para recuperar esses objetos falhará (403 Forbidden).

- Durante a transição, o aplicativo cliente pode usar uma solicitação de objeto S3 HEAD para monitorar o status do objeto.

4. * Objeto restaurado a partir do armazenamento Glacier*

Se um objeto tiver sido transferido para o armazenamento Glacier, o aplicativo cliente poderá emitir uma solicitação de restauração PÓS-objeto S3 para restaurar uma cópia recuperável para o pool de armazenamento em nuvem S3. A solicitação especifica quantos dias a cópia deve estar disponível no Cloud Storage Pool e no nível de acesso a dados a ser usado para a operação de restauração (Expedited, Standard ou Bulk). Quando a data de expiração da cópia recuperável é atingida, a cópia é automaticamente devolvida a um estado não recuperável.



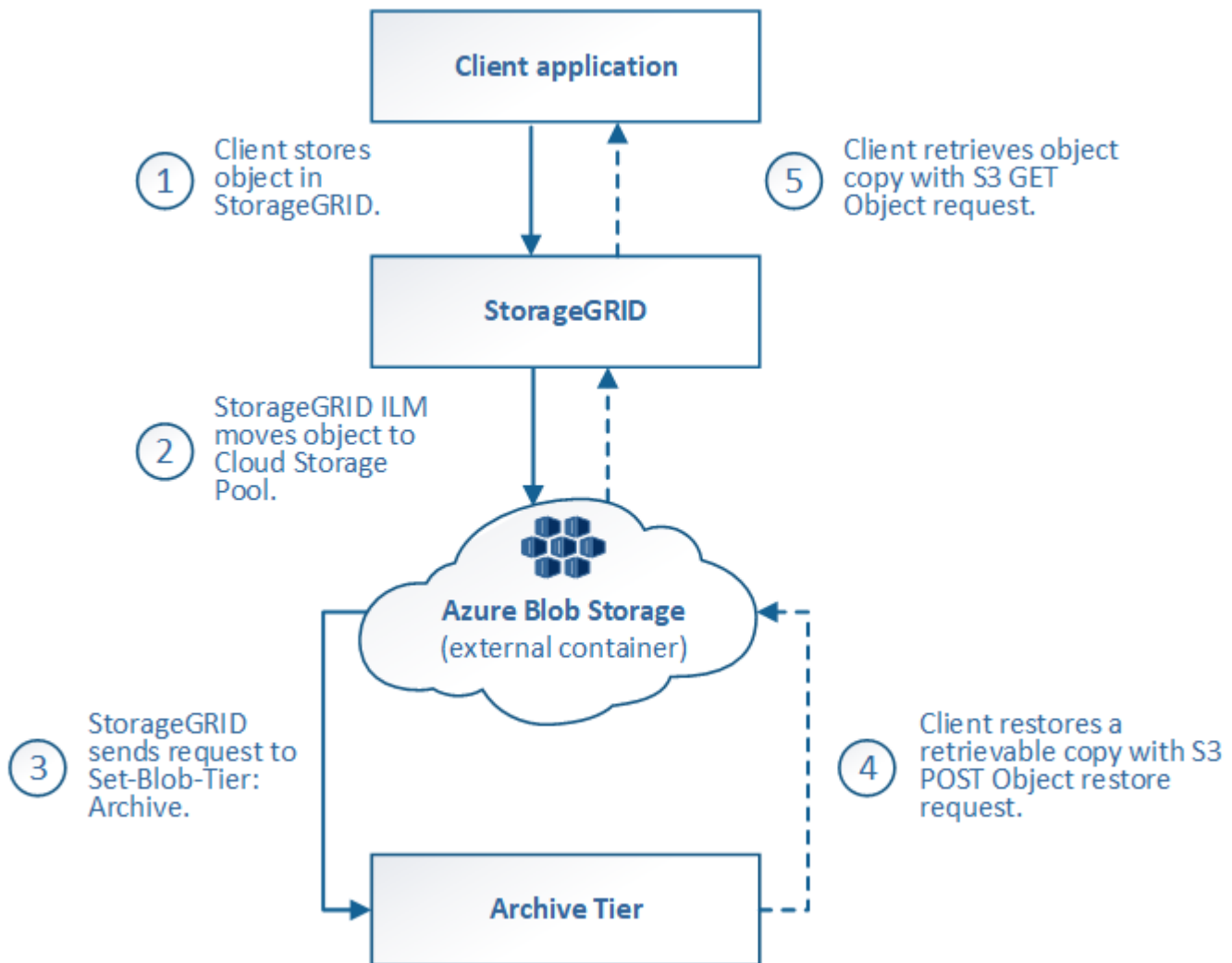
Se uma ou mais cópias do objeto também existirem em nós de storage no StorageGRID, não será necessário restaurar o objeto do Glacier emitindo uma solicitação de restauração PÓS-objeto. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma SOLICITAÇÃO GET Object.

5. Objeto recuperado

Uma vez que um objeto foi restaurado, o aplicativo cliente pode emitir uma solicitação GET Object para recuperar o objeto restaurado.

Azure: Ciclo de vida de um objeto Cloud Storage Pool

A figura mostra os estágios do ciclo de vida de um objeto que é armazenado em um pool de armazenamento em nuvem do Azure.



1. Objeto armazenado no StorageGRID

Para iniciar o ciclo de vida, um aplicativo cliente armazena um objeto no StorageGRID.

2. Objeto movido para o Azure Cloud Storage Pool

Quando o objeto é correspondido por uma regra de ILM que usa um pool de storage do Azure Cloud como local de posicionamento, o StorageGRID move o objeto para o contêiner de storage externo de Blob especificado pelo pool de storage do Cloud



Não use Cloud Storage Pools para objetos que foram ingeridos por clientes Swift. O Swift não oferece suporte a solicitações de restauração PÓS-objeto, portanto, o StorageGRID não será capaz de recuperar objetos Swift que tenham sido transferidos para a camada de arquivamento de armazenamento de Blobs do Azure. Emitir uma solicitação de objeto Swift GET para recuperar esses objetos falhará (403 Forbidden).

3. Objeto transicionado para o nível de Arquivo (estado não recuperável)

Imediatamente após a migração do objeto para o pool de storage de nuvem do Azure, o StorageGRID faz a transição automática do objeto para a categoria de arquivamento de storage de Blob do Azure.

4. Objeto restaurado a partir do nível de Arquivo

Se um objeto tiver sido transferido para a camada de arquivamento, o aplicativo cliente poderá emitir uma solicitação de restauração PÓS-Objeto S3 para restaurar uma cópia recuperável para o pool de armazenamento em nuvem do Azure.

Quando o StorageGRID recebe a Restauração PÓS-Objeto, ele faz a transição temporária do objeto para a camada de recuperação de storage do Blob do Azure. Assim que a data de expiração na solicitação de restauração PÓS-objeto for atingida, o StorageGRID faz a transição do objeto de volta para o nível de arquivamento.



Se uma ou mais cópias do objeto também existirem em nós de storage no StorageGRID, não será necessário restaurar o objeto do nível de acesso de arquivamento emitindo uma solicitação de restauração PÓS-objeto. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma SOLICITAÇÃO GET Object.

5. Objeto recuperado

Depois que um objeto for restaurado para o Azure Cloud Storage Pool, o aplicativo cliente poderá emitir uma SOLICITAÇÃO GET Object para recuperar o objeto restaurado.

Informações relacionadas

["USE A API REST DO S3"](#)

Quando usar Cloud Storage Pools

Com o Cloud Storage Pools, é possível fazer backup ou categorizar dados em um local externo. Além disso, você pode fazer backup ou categorizar dados em mais de uma nuvem.

Faça backup dos dados do StorageGRID em um local externo

Você pode usar um pool de armazenamento em nuvem para fazer backup de objetos do StorageGRID para um local externo.

Se as cópias no StorageGRID estiverem inacessíveis, os dados de objeto no pool de armazenamento em nuvem podem ser usados para atender solicitações de clientes. No entanto, talvez seja necessário emitir uma solicitação de restauração PÓS-objeto S3 para acessar a cópia de objeto de backup no Cloud Storage Pool.

Os dados de objeto em um pool de storage de nuvem também podem ser usados para recuperar dados perdidos do StorageGRID devido a uma falha de volume de storage ou nó de storage. Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID restaurará temporariamente o objeto e criará uma nova cópia no nó de armazenamento recuperado.

Para implementar uma solução de backup:

1. Crie um único pool de storage de nuvem.
2. Configurar uma regra de ILM que armazene simultaneamente cópias de objetos em nós de storage (como cópias replicadas ou codificadas por apagamento) e uma única cópia de objeto no Cloud Storage Pool.

3. Adicione a regra à sua política ILM. Em seguida, simule e ative a política.

Categorize os dados do StorageGRID para o local externo

Você pode usar um pool de armazenamento em nuvem para armazenar objetos fora do sistema StorageGRID. Por exemplo, suponha que você tenha um grande número de objetos que você precisa reter, mas você espera acessar esses objetos raramente, se nunca. Você pode usar um pool de storage de nuvem para categorizar os objetos em storage de baixo custo e liberar espaço no StorageGRID.

Para implementar uma solução de disposição em camadas:

1. Crie um único pool de storage de nuvem.
2. Configure uma regra de ILM que mova objetos raramente usados de nós de storage para o Cloud Storage Pool.
3. Adicione a regra à sua política ILM. Em seguida, simule e ative a política.

Manter vários pontos de extremidade de nuvem

Você pode configurar vários pontos de extremidade do Cloud Storage Pool se quiser categorizar ou fazer backup de dados de objetos em mais de uma nuvem. Os filtros nas regras do ILM permitem especificar quais objetos são armazenados em cada pool de armazenamento em nuvem. Por exemplo, você pode querer armazenar objetos de alguns locatários ou buckets no Amazon S3 Glacier e objetos de outros locatários ou buckets no storage Blob do Azure. Ou, talvez você queira mover dados entre o Amazon S3 Glacier e o storage Azure Blob.



Ao usar vários pontos de extremidade do Cloud Storage Pool, lembre-se de que um objeto pode ser armazenado em apenas um pool de armazenamento em nuvem de cada vez.

Para implementar vários pontos de extremidade de nuvem:

1. Crie até 10 pools de armazenamento em nuvem.
2. Configure as regras do ILM para armazenar os dados de objeto apropriados no momento apropriado em cada pool de armazenamento em nuvem. Por exemplo, armazene objetos do bucket A no Cloud Storage Pool A e armazene objetos do bucket B no Cloud Storage Pool B. ou armazene objetos no Cloud Storage Pool A por algum tempo e, em seguida, mova-os para o Cloud Storage Pool B.
3. Adicione as regras à sua política ILM. Em seguida, simule e ative a política.

Considerações para pools de storage em nuvem

Se você planeja usar um pool de armazenamento em nuvem para mover objetos para fora do sistema StorageGRID, leia as considerações sobre como configurar e usar pools de armazenamento em nuvem.

Considerações gerais

- Em geral, o storage de arquivamento em nuvem, como o armazenamento Amazon S3 Glacier ou Azure Blob, é um local econômico para armazenar dados de objetos. No entanto, os custos para recuperar dados do armazenamento de arquivamento em nuvem são relativamente altos. Para alcançar o menor custo geral, você deve considerar quando e com que frequência acessará os objetos no Cloud Storage Pool. O uso de um Cloud Storage Pool é recomendado apenas para conteúdo que você espera acessar com pouca frequência.

- Não use Cloud Storage Pools para objetos que foram ingeridos por clientes Swift. O Swift não oferece suporte a solicitações de restauração PÓS-objeto, portanto, o StorageGRID não poderá recuperar objetos Swift que tenham sido transferidos para o armazenamento do Glacier S3 ou para o nível de arquivamento de armazenamento Blob do Azure. Emitir uma solicitação de objeto Swift GET para recuperar esses objetos falhará (403 Forbidden).
- O uso de pools de armazenamento em nuvem com FabricPool não é suportado devido à latência adicional para recuperar um objeto do destino de pool de armazenamento em nuvem.
- Os objetos com bloqueio de objeto S3 ativado não podem ser colocados em pools de armazenamento em nuvem.
- Se o bucket S3 de destino para um pool de armazenamento em nuvem tiver o bloqueio de objeto S3 ativado, a tentativa de configurar a replicação de bucket (PutBucketReplication) falhará com um erro AccessDenied.

Considerações para as portas usadas para pools de armazenamento em nuvem

Para garantir que as regras do ILM possam mover objetos de e para o pool de armazenamento em nuvem especificado, você deve configurar a rede ou redes que contêm os nós de armazenamento do sistema. Você deve garantir que as seguintes portas possam se comunicar com o Cloud Storage Pool.

Por padrão, os pools de armazenamento em nuvem usam as seguintes portas:

- **80**: Para URIs de endpoint que começam com http
- **443**: Para URIs de endpoint que começam com https

Você pode especificar uma porta diferente ao criar ou editar um pool de armazenamento em nuvem.

Se você usar um servidor proxy não transparente, também deverá "[Configurar um proxy de armazenamento](#)" para permitir que as mensagens sejam enviadas para endpoints externos, como um endpoint na Internet.

Considerações sobre custos

O acesso ao storage na nuvem usando um pool de armazenamento em nuvem requer conectividade de rede com a nuvem. Você deve considerar o custo da infraestrutura de rede que usará para acessar a nuvem e provisioná-la adequadamente, com base na quantidade de dados que espera mover entre o StorageGRID e a nuvem usando o pool de armazenamento em nuvem.

Quando o StorageGRID se conecta ao endpoint externo do pool de armazenamento em nuvem, ele emite várias solicitações para monitorar a conectividade e garantir que ele possa executar as operações necessárias. Embora alguns custos adicionais sejam associados a essas solicitações, o custo do monitoramento de um pool de armazenamento em nuvem deve ser apenas uma pequena fração do custo geral de armazenamento de objetos no S3 ou Azure.

Custos mais significativos podem ser incorridos se você precisar mover objetos de um endpoint externo do pool de armazenamento em nuvem de volta para o StorageGRID. Os objetos podem ser movidos de volta para o StorageGRID em qualquer um destes casos:

- A única cópia do objeto está em um pool de storage de nuvem e você decide armazenar o objeto no StorageGRID. Nesse caso, você reconfigura suas regras e políticas de ILM. Quando a avaliação do ILM ocorre, o StorageGRID emite várias solicitações para recuperar o objeto do pool de armazenamento em nuvem. Em seguida, o StorageGRID cria o número especificado de cópias replicadas ou codificadas para apagamento localmente. Depois que o objeto é movido de volta para o StorageGRID, a cópia no pool de armazenamento em nuvem é excluída.

- Os objetos são perdidos devido à falha do nó de storage. Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID restaurará temporariamente o objeto e criará uma nova cópia no nó de armazenamento recuperado.



Quando os objetos são movidos de volta para o StorageGRID de um pool de armazenamento em nuvem, o StorageGRID emite várias solicitações para o ponto de extremidade do pool de armazenamento em nuvem para cada objeto. Antes de mover um grande número de objetos, entre em Contato com o suporte técnico para obter ajuda na estimativa do prazo e dos custos associados.

S3: Permissões necessárias para o bucket do Cloud Storage Pool

A política de bucket do bucket externo do S3 usada em um pool de armazenamento em nuvem deve conceder permissão StorageGRID para mover um objeto para o bucket, obter o status de um objeto, restaurar um objeto do armazenamento do Glacier quando necessário e muito mais. Idealmente, o StorageGRID deve ter acesso de controle total ao bucket (`s3:*`); no entanto, se isso não for possível, a política de bucket deve conceder as seguintes permissões do S3 ao StorageGRID:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Considerações sobre o ciclo de vida do balde externo

O movimento de objetos entre o StorageGRID e o bucket externo do S3 especificado no pool de storage de nuvem é controlado pelas regras do ILM e pela política de ILM ativa no StorageGRID. Em contraste, a transição de objetos do bucket externo S3 especificado no pool de armazenamento em nuvem para o Amazon S3 Glacier ou o S3 Glacier Deep Archive (ou para uma solução de armazenamento que implemente a classe de armazenamento Glacier) é controlada pela configuração do ciclo de vida desse bucket.

Se você quiser fazer a transição de objetos do Cloud Storage Pool, crie a configuração de ciclo de vida apropriada no bucket externo do S3 e use uma solução de armazenamento que implemente a classe de armazenamento Glacier e ofereça suporte à API de restauração PÓS-objeto do S3.

Por exemplo, suponha que você queira que todos os objetos movidos do StorageGRID para o pool de armazenamento em nuvem sejam transferidos imediatamente para o armazenamento do Amazon S3 Glacier. Você criaria uma configuração de ciclo de vida no bucket externo do S3 que especifica uma única ação (**transition**) da seguinte forma:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Essa regra faria a transição de todos os objetos de bucket para o Amazon S3 Glacier no dia em que foram criados (ou seja, no dia em que foram movidos do StorageGRID para o pool de storage de nuvem).



Ao configurar o ciclo de vida do bucket externo, nunca use as ações **Expiration** para definir quando os objetos expiram. As ações de expiração fazem com que o sistema de armazenamento externo exclua objetos expirados. Se você tentar acessar um objeto expirado do StorageGRID, o objeto excluído não será encontrado.

Se você quiser fazer a transição de objetos no Cloud Storage Pool para o S3 Glacier Deep Archive (em vez de para o Amazon S3 Glacier), especifique `<StorageClass>DEEP_ARCHIVE</StorageClass>` no ciclo de vida do bucket. No entanto, esteja ciente de que você não pode usar o Expedited nível para restaurar objetos do S3 Glacier Deep Archive.

Azure: Considerações para o nível de acesso

Ao configurar uma conta de armazenamento do Azure, você pode definir o nível de acesso padrão como Hot or Cool. Ao criar uma conta de storage para uso com um Cloud Storage Pool, você deve usar o Hot Tier como o nível padrão. Mesmo que o StorageGRID defina imediatamente o nível para Arquivo quando ele move objetos para o pool de armazenamento em nuvem, usar uma configuração padrão do Hot garante que você não será cobrada uma taxa de exclusão antecipada para objetos removidos do nível Cool antes do mínimo de 30 dias.

Azure: Gerenciamento de ciclo de vida não suportado

Não use o gerenciamento do ciclo de vida do storage Azure Blob para o contêiner usado com um Cloud Storage Pool. As operações do ciclo de vida podem interferir nas operações do Cloud Storage Pool.

Informações relacionadas

- ["Crie um pool de storage em nuvem"](#)

Compare os pools do Cloud Storage e a replicação do CloudMirror

À medida que você começa a usar o Cloud Storage Pools, pode ser útil entender as semelhanças e diferenças entre o Cloud Storage Pools e o serviço de replicação do StorageGRID CloudMirror.

	Cloud Storage Pool	Serviço de replicação do CloudMirror
Qual é o objetivo principal?	Atua como um destino de arquivo. A cópia de objeto no Cloud Storage Pool pode ser a única cópia do objeto ou pode ser uma cópia adicional. Ou seja, em vez de manter duas cópias no local, você pode manter uma cópia no StorageGRID e enviar uma cópia para o pool de storage de nuvem.	Permite que um locatário replique automaticamente objetos de um bucket no StorageGRID (origem) para um bucket externo do S3 (destino). Cria uma cópia independente de um objeto em uma infraestrutura S3 independente.
Como é configurado?	Definido da mesma forma que os pools de armazenamento, usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Pode ser selecionado como o local de colocação em uma regra ILM. Enquanto um pool de storage consiste em um grupo de nós de storage, um pool de armazenamento em nuvem é definido usando um endpoint remoto S3 ou Azure (endereço IP, credenciais etc.).	Um usuário de locatário " Configura a replicação do CloudMirror " definindo um endpoint do CloudMirror (endereço IP, credenciais, etc.) usando o Gerenciador do locatário ou a API do S3. Depois que o endpoint do CloudMirror for configurado, qualquer bucket de propriedade dessa conta de locatário poderá ser configurado para apontar para o endpoint do CloudMirror.
Quem é responsável por montá-lo?	Normalmente, um administrador de grade	Normalmente, um usuário locatário
Qual é o destino?	<ul style="list-style-type: none"> • Qualquer infraestrutura S3 compatível (incluindo Amazon S3) • Camada de arquivamento de Blob do Azure • Google Cloud Platform (GCP) 	<ul style="list-style-type: none"> • Qualquer infraestrutura S3 compatível (incluindo Amazon S3) • Google Cloud Platform (GCP)
O que faz com que os objetos sejam movidos para o destino?	Uma ou mais regras ILM na política ILM ativa. As regras do ILM definem quais objetos o StorageGRID move para o pool de armazenamento em nuvem e quando os objetos são movidos.	O ato de inserir um novo objeto em um bucket de origem que foi configurado com um endpoint do CloudMirror. Os objetos que existiam no bucket de origem antes do bucket ser configurado com o endpoint do CloudMirror não são replicados, a menos que sejam modificados.
Como os objetos são recuperados?	Os aplicativos devem fazer solicitações ao StorageGRID para recuperar objetos que foram movidos para um pool de armazenamento em nuvem. Se a única cópia de um objeto tiver sido transferida para armazenamento de arquivo, o StorageGRID gerencia o processo de restauração do objeto para que ele possa ser recuperado.	Como a cópia espelhada no intervalo de destino é uma cópia independente, os aplicativos podem recuperar o objeto fazendo solicitações para o StorageGRID ou para o destino S3. Por exemplo, suponha que você use a replicação do CloudMirror para espelhar objetos em uma organização parceira. O parceiro pode usar seus próprios aplicativos para ler ou atualizar objetos diretamente do destino S3. Não é necessário utilizar o StorageGRID.

	Cloud Storage Pool	Serviço de replicação do CloudMirror
Você pode ler diretamente do destino?	Não. Os objetos movidos para um pool de storage de nuvem são gerenciados pelo StorageGRID. As solicitações de leitura devem ser direcionadas ao StorageGRID (e o StorageGRID será responsável pela recuperação do pool de armazenamento em nuvem).	Sim, porque a cópia espelhada é uma cópia independente.
O que acontece se um objeto for excluído da origem?	O objeto também é excluído do Cloud Storage Pool.	A ação de exclusão não é replicada. Um objeto excluído não existe mais no bucket do StorageGRID, mas continua a existir no bucket de destino. Da mesma forma, os objetos no intervalo de destino podem ser excluídos sem afetar a origem.
Como você acessa objetos após um desastre (sistema StorageGRID não operacional)?	Os nós de StorageGRID com falha devem ser recuperados. Durante esse processo, cópias de objetos replicados podem ser restauradas usando as cópias no Cloud Storage Pool.	As cópias de objeto no destino do CloudMirror são independentes do StorageGRID, portanto, podem ser acessadas diretamente antes que os nós do StorageGRID sejam recuperados.

Crie um pool de storage em nuvem

Um Cloud Storage Pool especifica um único bucket externo do Amazon S3 ou outro provedor compatível com o S3 ou contêiner de storage Azure Blob.

Ao criar um pool de storage de nuvem, especifique o nome e o local do bucket ou do contêiner externo que o StorageGRID usará para armazenar objetos, o tipo de provedor de nuvem (storage Amazon S3/GCP ou Azure Blob) e as informações que o StorageGRID precisa para acessar o bucket ou o contêiner externo.

O StorageGRID valida o pool de armazenamento em nuvem assim que você o salva, portanto, você deve garantir que o bucket ou o contêiner especificado no pool de armazenamento em nuvem existe e está acessível.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["permissões de acesso necessárias"](#).
- Você revisou o ["Considerações para pools de storage em nuvem"](#).
- O bucket externo ou o contêiner referenciado pelo Cloud Storage Pool já existe e você sabe o nome e a localização dele.
- Para acessar o bucket ou o contêiner, você tem as seguintes informações para o tipo de autenticação que você escolherá:

S3 tecla de acesso

Para o bucket externo S3

- O ID da chave de acesso para a conta que possui o bucket externo.
- A chave de acesso secreto associada.

Alternativamente, você pode especificar Anonymous para o tipo de autenticação.

Portal de acesso C2S

Para serviços comerciais de nuvem (C2S) S3 Service

Você tem o seguinte:

- URL completa que o StorageGRID usará para obter credenciais temporárias do servidor do portal de acesso C2S (CAP), incluindo todos os parâmetros de API necessários e opcionais atribuídos à sua conta C2S.
- Certificado de CA do servidor emitido por uma autoridade de certificação governamental (CA) apropriada. O StorageGRID usa esse certificado para verificar a identidade do SERVIDOR CAP. O certificado de CA do servidor deve usar a codificação PEM.
- Certificado de cliente emitido por uma autoridade de certificação governamental (CA) adequada. O StorageGRID usa esse certificado para identificar-se para o servidor CAP. O certificado de cliente deve usar codificação PEM e deve ter acesso à sua conta C2S.
- Chave privada codificada PEM para o certificado do cliente.
- Frase-passe para descriptar a chave privada do certificado do cliente, se estiver encriptada.



Se o certificado de cliente for encriptado, utilize o formato tradicional para a encriptação. O formato criptografado PKCS nº 8 não é suportado.

Storage Azure Blob

Para o contentor externo

- URI (Uniform Resource Identifier) usado para acessar o contentor de armazenamento de Blob.
- Nome da conta de armazenamento e da chave de conta. Você pode usar o portal do Azure para encontrar esses valores.

Passos

1. Selecione **ILM > Storage Pools > Cloud Storage Pools**.
2. Selecione **criar** e insira as seguintes informações:

Campo	Descrição
Nome do Cloud Storage Pool	Um nome que descreve brevemente o Cloud Storage Pool e sua finalidade. Use um nome que será fácil de identificar quando você configurar regras ILM.

Campo	Descrição
Tipo de fornecedor	<p data-bbox="513 153 1446 222">Qual provedor de nuvem você usará para este pool de armazenamento em nuvem:</p> <ul data-bbox="537 254 1446 407" style="list-style-type: none"> <li data-bbox="537 254 1446 359">• Amazon S3/GCP: Selecione essa opção para um Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) ou outro provedor compatível com S3. <li data-bbox="537 369 1029 407">• Armazenamento de Blobs do Azure
Balde ou recipiente	<p data-bbox="513 459 1463 529">O nome do bucket externo do S3 ou do recipiente do Azure. Não é possível alterar esse valor depois que o pool de armazenamento em nuvem for salvo.</p>

3. Com base na seleção do tipo de fornecedor, introduza as informações do ponto de extremidade do serviço.

Amazon S3/GCP

a. Para o protocolo, selecione HTTPS ou HTTP.



Não use conexões HTTP para dados confidenciais.

b. Introduza o nome do anfitrião. Exemplo:

`s3-aws-region.amazonaws.com`

c. Selecione o estilo de URL:

Opção	Descrição
Detecção automática	Tente detetar automaticamente qual estilo de URL usar, com base nas informações fornecidas. Por exemplo, se você especificar um endereço IP, o StorageGRID usará um URL estilo caminho. Selecione esta opção somente se você não souber qual estilo específico usar.
Virtual-hospedado-estilo	Use um URL de estilo virtual hospedado para acessar o bucket. URLs de estilo virtual hospedadas incluem o nome do intervalo como parte do nome de domínio. Exemplo: <code>https://bucket-name.s3.company.com/key-name</code>
Estilo de caminho	Use um URL de estilo de caminho para acessar o bucket. URLs de estilo de caminho incluem o nome do intervalo no final Exemplo: <code>https://s3.company.com/bucket-name/key-name</code> Nota: a opção URL estilo caminho não é recomendada e será obsoleta em uma versão futura do StorageGRID.

d. Opcionalmente, insira o número da porta ou use a porta padrão: 443 para HTTPS ou 80 para HTTP.

Storage Blob do Azure

a. Usando um dos formatos a seguir, insira o URI para o endpoint de serviço.

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

Exemplo: `https://myaccount.blob.core.windows.net:443`

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

4. Selecione **continuar**. Em seguida, selecione o tipo de autenticação e insira as informações necessárias para o endpoint do Cloud Storage Pool:

Chave de acesso

Somente para o tipo de provedor do Amazon S3/GCP

- a. Para **ID da chave de acesso**, insira o ID da chave de acesso para a conta que possui o bucket externo.
- b. Para **chave de acesso secreta**, insira a chave de acesso secreto.

CAP (portal de acesso C2S)

Para serviços comerciais de nuvem (C2S) S3 Service

- a. Para **URL de credenciais temporárias**, insira o URL completo que o StorageGRID usará para obter credenciais temporárias do SERVIDOR CAP, incluindo todos os parâmetros de API necessários e opcionais atribuídos à sua conta C2S.
- b. Para **certificado CA do servidor**, selecione **Procurar** e carregue o certificado CA codificado em PEM que o StorageGRID usará para verificar o servidor CAP.
- c. Para **certificado de cliente**, selecione **Procurar** e carregue o certificado codificado PEM que o StorageGRID usará para se identificar no servidor CAP.
- d. Para **chave privada do cliente**, selecione **Procurar** e carregue a chave privada codificada pelo PEM para o certificado do cliente.
- e. Se a chave privada do cliente estiver encriptada, introduza a frase-passe para descriptar a chave privada do cliente. Caso contrário, deixe o campo **Client private key passphrase** em branco.

Storage Blob do Azure

- a. Para **Nome da conta**, insira o nome da conta de armazenamento Blob que possui o contentor de serviço externo.
- b. Para **chave de conta**, insira a chave secreta da conta de armazenamento Blob.

Anônimo

Nenhuma informação adicional é necessária.

5. Selecione **continuar**. Em seguida, escolha o tipo de verificação de servidor que você deseja usar:

Opção	Descrição
Use certificados de CA raiz no SO nó de armazenamento	Use os certificados Grid CA instalados no sistema operacional para proteger conexões.
Use certificado CA personalizado	Use um certificado de CA personalizado. Selecione Procurar e carregue o certificado codificado em PEM.
Não verifique o certificado	O certificado usado para a conexão TLS não é verificado.

6. Selecione **Guardar**.

Quando você salva um pool de storage de nuvem, o StorageGRID faz o seguinte:

- Valida que o bucket ou o contentor e o endpoint de serviço existem e que eles podem ser alcançados usando as credenciais que você especificou.
- Grava um arquivo de marcador no bucket ou no contêiner para identificá-lo como um pool de armazenamento em nuvem. Nunca remova esse arquivo, que é `x-ntap-sgws-cloud-pool-uuid` chamado .

Se a validação do Cloud Storage Pool falhar, você receberá uma mensagem de erro que explica por que a validação falhou. Por exemplo, um erro pode ser relatado se houver um erro de certificado ou se o bucket ou contentor especificado ainda não existir.

7. Se ocorrer um erro, consulte o "[Instruções para solução de problemas de Cloud Storage Pools](#)", resolva quaisquer problemas e, em seguida, tente salvar o pool de armazenamento em nuvem novamente.

Edite um pool de armazenamento em nuvem

Você pode editar um pool de armazenamento em nuvem para alterar seu nome, ponto de extremidade de serviço ou outros detalhes; no entanto, não é possível alterar o bucket do S3 ou o contentor do Azure para um pool de armazenamento em nuvem.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador da web suportado](#)".
- Você tem permissões de acesso específicas.
- Você revisou o "[Considerações para pools de storage em nuvem](#)".

Passos

1. Selecione **ILM > Storage Pools > Cloud Storage Pools**.

A tabela Cloud Storage Pools lista os pools de armazenamento em nuvem existentes.

2. Marque a caixa de seleção do pool de armazenamento em nuvem que deseja editar.
3. Selecione **ações > Editar**.
4. Conforme necessário, altere o nome de exibição, o ponto de extremidade do serviço, as credenciais de autenticação ou o método de validação do certificado.



Não é possível alterar o tipo de provedor, o bucket do S3 ou o contentor do Azure para um pool de armazenamento em nuvem.

Se você carregou anteriormente um certificado de servidor ou cliente, você pode selecionar **Detalhes do certificado** para revisar o certificado que está atualmente em uso.

5. Selecione **Guardar**.

Quando você salva um pool de armazenamento em nuvem, o StorageGRID valida que o bucket ou o contentor e o endpoint de serviço existem e que eles podem ser alcançados usando as credenciais especificadas.

Se a validação do Cloud Storage Pool falhar, uma mensagem de erro será exibida. Por exemplo, um erro pode ser relatado se houver um erro de certificado.

Consulte as instruções do "[Solução de problemas de Cloud Storage Pools](#)", resolva o problema e tente salvar o pool de armazenamento em nuvem novamente.

Remova um pool de armazenamento em nuvem

Você pode remover um Cloud Storage Pool se ele não for usado em uma regra ILM e não contiver dados de objeto.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["permissões de acesso necessárias"](#).

Se necessário, use o ILM para mover dados de objeto

Se o pool de armazenamento em nuvem que você deseja remover contiver dados de objeto, use o ILM para mover os dados para um local diferente. Por exemplo, você pode mover os dados para nós de storage na grade ou para um pool de storage de nuvem diferente.

Passos

1. Selecione **ILM > Storage Pools > Cloud Storage Pools**.
2. Veja a coluna de uso do ILM na tabela para determinar se você pode remover o pool de armazenamento em nuvem.

Não é possível remover um Cloud Storage Pool se ele estiver sendo usado em uma regra ILM ou em um perfil de codificação de apagamento.

3. Se o Cloud Storage Pool estiver sendo usado, selecione **cloud storage pool name > ILM usage**.
4. ["Clonar cada regra de ILM"](#) Que atualmente coloca objetos no pool de armazenamento em nuvem que você deseja remover.
5. Determine onde você deseja mover os objetos existentes gerenciados por cada regra clonada.

Você pode usar um ou mais pools de storage ou outro pool de storage de nuvem.

6. Edite cada uma das regras que clonou.

Para a Etapa 2 do assistente criar regra ILM, selecione o novo local no campo **Copies at**.

7. ["Crie uma nova política proposta de ILM"](#) e substituir cada uma das regras antigas por uma regra clonada.
8. Ative a nova política.
9. Aguarde que o ILM remova objetos do pool de armazenamento em nuvem e os coloque no novo local.

Excluir Cloud Storage Pool

Quando o pool de armazenamento em nuvem está vazio e não é usado em nenhuma regra ILM, você pode excluí-lo.

Antes de começar

- Você removeu quaisquer regras ILM que possam ter usado o pool.
- Você confirmou que o bucket do S3 ou o contentor do Azure não contém nenhum objeto.

Um erro ocorre se você tentar remover um pool de armazenamento em nuvem se ele contém objetos. ["Solucionar problemas em Cloud Storage Pools"](#) Consulte .



Quando você cria um pool de storage de nuvem, o StorageGRID grava um arquivo de marcador no bucket ou no contentor para identificá-lo como um pool de storage de nuvem. Não remova esse arquivo, que é `x-ntap-sgws-cloud-pool-uuid` chamado .

Passos

1. Selecione **ILM > Storage Pools > Cloud Storage Pools**.
2. Se a coluna de uso do ILM indicar que o Cloud Storage Pool não está sendo usado, marque a caixa de seleção.
3. Selecione **ações > Remove**.
4. Selecione **OK**.

Solucionar problemas em Cloud Storage Pools

Use estas etapas de solução de problemas para ajudar a resolver erros que você pode encontrar ao criar, editar ou excluir um pool de armazenamento em nuvem.

Determine se ocorreu um erro

O StorageGRID executa uma verificação simples de integridade em cada pool de armazenamento em nuvem uma vez por minuto para garantir que o pool de armazenamento em nuvem possa ser acessado e que ele esteja funcionando corretamente. Se a verificação de integridade detectar um problema, uma mensagem será exibida na coluna último erro da tabela Cloud Storage Pools na página Storage Pools.

A tabela mostra o erro mais recente detectado para cada pool de armazenamento em nuvem e indica há quanto tempo o erro ocorreu.

Além disso, um alerta de **erro de conectividade do Cloud Storage Pool** é acionado se a verificação de integridade detectar que um ou mais novos erros do Cloud Storage Pool ocorreram nos últimos 5 minutos. Se você receber uma notificação por e-mail para esse alerta, vá para a página pools de armazenamento (selecione **ILM > pools de armazenamento**), revise as mensagens de erro na coluna último erro e consulte as diretrizes de solução de problemas abaixo.

Verifique se um erro foi resolvido

Depois de resolver quaisquer problemas subjacentes, você pode determinar se o erro foi resolvido. Na página Cloud Storage Pool, selecione o ponto final e selecione **Limpar erro**. Uma mensagem de confirmação indica que o StorageGRID apagou o erro do pool de armazenamento em nuvem.

Se o problema subjacente tiver sido resolvido, a mensagem de erro já não é apresentada. No entanto, se o problema subjacente não foi corrigido (ou se um erro diferente for encontrado), a mensagem de erro será mostrada na coluna último erro dentro de alguns minutos.

Erro: Este pool de armazenamento em nuvem contém conteúdo inesperado

Você pode encontrar esse erro ao tentar criar, editar ou excluir um pool de armazenamento em nuvem. Este erro ocorre se o intervalo ou recipiente incluir o `x-ntap-sgws-cloud-pool-uuid` arquivo marcador, mas esse arquivo não tiver o UUID esperado.

Normalmente, você só verá esse erro se estiver criando um novo pool de armazenamento em nuvem e outra instância do StorageGRID já estiver usando o mesmo pool de armazenamento em nuvem.

Tente estas etapas para corrigir o problema:

- Verifique se ninguém na sua organização também está usando este pool de armazenamento em nuvem.
- Exclua o `x-ntap-sgws-cloud-pool-uuid` arquivo e tente configurar o pool de armazenamento em nuvem novamente.

Erro: Não foi possível criar ou atualizar o Cloud Storage Pool. Erro do endpoint

Você pode encontrar esse erro ao tentar criar ou editar um pool de armazenamento em nuvem. Esse erro indica que algum tipo de problema de conectividade ou configuração está impedindo a gravação do StorageGRID no pool de armazenamento em nuvem.

Para corrigir o problema, revise a mensagem de erro do endpoint.

- Se a mensagem de erro contiver `Get url: EOF`, verifique se o endpoint de serviço usado para o Cloud Storage Pool não usa HTTP para um contentor ou bucket que requer HTTPS.
- Se a mensagem de erro contiver `Get url: net/http: request canceled while waiting for connection`, verifique se a configuração de rede permite que os nós de armazenamento acessem o endpoint de serviço usado para o pool de armazenamento em nuvem.
- Para todas as outras mensagens de erro de endpoint, tente uma ou mais das seguintes opções:
 - Crie um recipiente ou bucket externo com o mesmo nome que você inseriu para o Cloud Storage Pool e tente salvar o novo Cloud Storage Pool novamente.
 - Corrija o nome do recipiente ou do bucket especificado para o pool de armazenamento em nuvem e tente salvar o novo pool de armazenamento em nuvem novamente.

Erro: Falha ao analisar o certificado CA

Você pode encontrar esse erro ao tentar criar ou editar um pool de armazenamento em nuvem. O erro ocorre se o StorageGRID não puder analisar o certificado digitado ao configurar o pool de armazenamento em nuvem.

Para corrigir o problema, verifique se há problemas no certificado da CA fornecido.

Erro: Um pool de armazenamento em nuvem com esta ID não foi encontrado

Você pode encontrar esse erro ao tentar editar ou excluir um pool de armazenamento em nuvem. Esse erro ocorre se o endpoint retornar uma resposta 404, o que pode significar uma das seguintes opções:

- As credenciais usadas para o Cloud Storage Pool não têm permissão de leitura para o bucket.
- O intervalo usado para o pool de armazenamento em nuvem não inclui o `x-ntap-sgws-cloud-pool-uuid` arquivo de marcador.

Tente um ou mais destes passos para corrigir o problema:

- Verifique se o usuário associado à chave de acesso configurada tem as permissões necessárias.
- Edite o Cloud Storage Pool com credenciais que tenham as permissões necessárias.
- Se as permissões estiverem corretas, entre em Contato com o suporte.

Erro: Não foi possível verificar o conteúdo do pool de armazenamento em nuvem. Erro do endpoint

Você pode encontrar esse erro ao tentar excluir um pool de armazenamento em nuvem. Esse erro indica que algum tipo de problema de conectividade ou configuração está impedindo o StorageGRID de ler o conteúdo do bucket do pool de armazenamento em nuvem.

Para corrigir o problema, revise a mensagem de erro do endpoint.

Erro: Os objetos já foram colocados neste intervalo

Você pode encontrar esse erro ao tentar excluir um pool de armazenamento em nuvem. Não é possível excluir um Cloud Storage Pool se ele contiver dados que foram movidos pelo ILM, dados que estavam no bucket antes de configurar o Cloud Storage Pool ou dados que foram colocados no bucket por outra fonte após a criação do Cloud Storage Pool.

Tente um ou mais destes passos para corrigir o problema:

- Siga as instruções para mover objetos de volta para o StorageGRID no "ciclo de vida de um objeto de pool de armazenamento em nuvem".
- Se você tiver certeza de que os objetos restantes não foram colocados no Cloud Storage Pool pelo ILM, exclua manualmente os objetos do bucket.



Nunca exclua manualmente objetos de um pool de armazenamento em nuvem que possam ter sido colocados lá pelo ILM. Se você tentar acessar um objeto excluído manualmente do StorageGRID, o objeto excluído não será encontrado.

Erro: O proxy encontrou um erro externo ao tentar alcançar o pool de armazenamento em nuvem

Você pode encontrar esse erro se tiver configurado um proxy de armazenamento não transparente entre nós de armazenamento e o endpoint S3 externo usado para o pool de armazenamento em nuvem. Esse erro ocorre se o servidor proxy externo não conseguir alcançar o ponto de extremidade do Cloud Storage Pool. Por exemplo, o servidor DNS pode não conseguir resolver o nome do host ou pode haver um problema de rede externo.

Tente um ou mais destes passos para corrigir o problema:

- Verifique as configurações do pool de armazenamento em nuvem (**ILM > pools de armazenamento**).
- Verifique a configuração de rede do servidor proxy de armazenamento.

Informações relacionadas

["Ciclo de vida de um objeto Cloud Storage Pool"](#)

Gerenciar perfis de codificação de apagamento

Você pode renomear um perfil de codificação de apagamento, se necessário. Você pode desativar um perfil de codificação de apagamento se ele não for usado atualmente em nenhuma regra ILM.

Renomear um perfil de codificação de apagamento

Você pode querer renomear um perfil de codificação de apagamento para torná-lo mais óbvio o que o perfil

faz.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["permissões de acesso necessárias"](#).

Passos

1. Selecione **ILM > codificação de apagamento**.
2. Selecione o perfil que deseja renomear.
3. Selecione **Renomear**.
4. Insira um nome exclusivo para o perfil de codificação de apagamento.

O nome do perfil de codificação de apagamento é anexado ao nome do pool de armazenamento na instrução de colocação de uma regra ILM.



Os nomes de perfis de codificação de apagamento devem ser exclusivos. Um erro de validação ocorre se você usar o nome de um perfil existente, mesmo que esse perfil tenha sido desativado.

5. Selecione **Guardar**.

Desativar um perfil de codificação de apagamento

Você pode desativar um perfil de codificação de apagamento se você não planeja mais usá-lo e se o perfil não for usado atualmente em nenhuma regra ILM.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["permissões de acesso necessárias"](#).
- Você confirmou que nenhuma operação de reparo de dados codificados de apagamento ou procedimentos de desativação estão em andamento. Uma mensagem de erro será retornada se você tentar desativar um perfil de codificação de apagamento enquanto qualquer uma dessas operações estiver em andamento.

Sobre esta tarefa

Quando você desativa um perfil de codificação de apagamento, o perfil ainda aparece na página Perfis de codificação de apagamento, mas seu status é **desativado**.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
<input type="radio"/> 2+1 Data Center 1	Used In ILM Rule	Data Center 1	3	1	2+1	50	1	No
<input checked="" type="radio"/> New profile	Deactivated	Data Center 1	3	1	2+1	50	1	No

Você não pode mais usar um perfil de codificação de apagamento que tenha sido desativado. Um perfil desativado não é exibido quando você cria as instruções de colocação para uma regra ILM. Não é possível reativar um perfil desativado.

O StorageGRID impede que você desative um perfil de codificação de apagamento se uma das seguintes opções for verdadeira:

- O perfil de codificação de apagamento é usado atualmente em uma regra ILM.
- O perfil de codificação de apagamento não é mais usado em nenhuma regra ILM, mas os dados de objeto e fragmentos de paridade para o perfil ainda existem.

Passos

1. Selecione **ILM > Codificação de apagamento**.
2. Revise a coluna **Status** para confirmar que o perfil de codificação de apagamento que você deseja desativar não é usado em nenhuma regra ILM.

Você não pode desativar um perfil de codificação de apagamento se ele for usado em qualquer regra ILM. No exemplo, o perfil **2 e 1 Data Center 1** é usado em pelo menos uma regra ILM.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
<input checked="" type="radio"/> 2+1 Data Center 1	Used in ILM Rule	Data Center 1	3	1	2+1	50	1	No
<input type="radio"/> New profile	Deactivated	Data Center 1	3	1	2+1	50	1	No

3. Se o perfil for usado em uma regra ILM, siga estas etapas:
 - a. Selecione **ILM > regras**.
 - b. Selecione cada regra e revise o diagrama de retenção para determinar se a regra usa o perfil de codificação de apagamento que você deseja desativar.
 - c. Se a regra ILM usar o perfil de codificação de apagamento que você deseja desativar, determine se a regra é usada na política ILM ativa ou em uma política proposta.
 - d. Conclua as etapas adicionais na tabela, com base em onde o perfil de codificação de apagamento é usado.

Onde o perfil foi usado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Nunca usado em nenhuma regra ILM	Não são necessários passos adicionais. Continue com este procedimento.	<i>Nenhum</i>
Em uma regra ILM que nunca foi usada em nenhuma política ILM	<ol style="list-style-type: none"> i. Edite ou exclua todas as regras ILM afetadas. Se você editar a regra, remova todos os canais que usam o perfil de codificação de apagamento. ii. Continue com este procedimento. 	"Trabalhe com regras ILM e políticas ILM"

Onde o perfil foi usado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Em uma regra ILM que está atualmente na política ILM ativa	<ul style="list-style-type: none"> i. Clonar a política ativa. ii. Remova a regra ILM que usa o perfil de codificação de apagamento. iii. Adicione uma ou mais novas regras ILM para garantir que os objetos estejam protegidos. iv. Salve, simule e ative a nova política. v. Aguarde que a nova política seja aplicada e que os objetos existentes sejam movidos para novos locais com base nas novas regras adicionadas. <p>Observação: dependendo do número de objetos e do tamanho do seu sistema StorageGRID, pode levar semanas ou até meses para que as operações do ILM movam os objetos para novos locais, com base nas novas regras do ILM.</p> <p>Embora você possa tentar desativar um perfil de codificação de apagamento com segurança enquanto ele ainda estiver associado a dados, a operação de desativação falhará. Uma mensagem de erro irá informá-lo se o perfil ainda não está pronto para ser desativado.</p> <ul style="list-style-type: none"> vi. Edite ou exclua a regra que você removeu da política. Se você editar a regra, remova todos os canais que usam o perfil de codificação de apagamento. vii. Continue com este procedimento. 	<p>"Crie uma política ILM"</p> <p>"Trabalhe com regras ILM e políticas ILM"</p>
Em uma regra ILM que está atualmente em uma política de ILM proposta	<ul style="list-style-type: none"> i. Edite a política proposta. ii. Remova a regra ILM que usa o perfil de codificação de apagamento. iii. Adicione uma ou mais novas regras ILM para garantir que todos os objetos estejam protegidos. iv. Salve a política proposta. v. Edite ou exclua a regra que você removeu da política. Se você editar a regra, remova todos os canais que usam o perfil de codificação de apagamento. vi. Continue com este procedimento. 	<p>"Crie uma política ILM"</p> <p>"Trabalhe com regras ILM e políticas ILM"</p>

Onde o perfil foi usado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Em uma regra ILM que está em uma política ILM histórica	<ul style="list-style-type: none"> i. Edite ou exclua a regra. Se você editar a regra, remova todos os canais que usam o perfil de codificação de apagamento. (A regra agora aparecerá como uma regra histórica na política histórica.) ii. Continue com este procedimento. 	"Trabalhe com regras ILM e políticas ILM"

e. Atualize a página Perfis de codificação de apagamento para garantir que o perfil não seja usado em uma regra ILM.

4. Se o perfil não for usado em uma regra ILM, selecione o botão de opção e selecione **Deactivate**.

A caixa de diálogo Desativar perfil EC é exibida.

5. Se tiver a certeza de que pretende desativar o perfil, selecione **Desativar**.

- Se o StorageGRID for capaz de desativar o perfil de codificação de apagamento, seu status será **desativado**. Você não pode mais selecionar este perfil para qualquer regra ILM.
- Se o StorageGRID não conseguir desativar o perfil, é apresentada uma mensagem de erro. Por exemplo, uma mensagem de erro será exibida se os dados do objeto ainda estiverem associados a esse perfil. Talvez seja necessário esperar várias semanas antes de tentar novamente o processo de desativação.

Configurar regiões (opcional e apenas S3)

As regras do ILM podem filtrar objetos com base nas regiões em que os buckets do S3 são criados, permitindo armazenar objetos de diferentes regiões em diferentes locais de armazenamento.

Se você quiser usar uma região de bucket do S3 como filtro em uma regra, primeiro crie as regiões que podem ser usadas pelos buckets do sistema.



Não é possível alterar a região de um bucket após o bucket ter sido criado.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem permissões de acesso específicas.

Sobre esta tarefa

Ao criar um bucket do S3, você pode especificar que o bucket seja criado em uma região específica. A especificação de uma região permite que o bucket esteja geograficamente próximo de seus usuários, o que pode ajudar a otimizar a latência, minimizar custos e atender aos requisitos regulatórios.

Ao criar uma regra ILM, você pode querer usar a região associada a um bucket do S3 como um filtro avançado. Por exemplo, você pode projetar uma regra que se aplica apenas a objetos em buckets do S3 criados na região US-West-2. Em seguida, é possível especificar que as cópias desses objetos serão

colocadas em nós de storage em um local de data center nessa região para otimizar a latência.

Ao configurar regiões, siga estas diretrizes:

- Por padrão, todos os baldes são considerados como pertencentes à região US-East-1.
- Você deve criar as regiões usando o Gerenciador de Grade antes de especificar uma região não padrão ao criar buckets usando o Gerenciador de locatário ou a API de gerenciamento de locatário ou com o elemento de solicitação de LocationConstraint para solicitações de API de bucket do S3 PUT. Um erro ocorre se uma solicitação COLOCAR balde usar uma região que não foi definida no StorageGRID.
- Você deve usar o nome exato da região ao criar o bucket do S3. Os nomes de região são sensíveis a maiúsculas e minúsculas. Os caracteres válidos são números, letras e hífens.



A UE não é considerada um apelido para a ue-oeste-1. Se você quiser usar a região da UE ou da ue-oeste-1, você deve usar o nome exato.

- Não é possível excluir ou modificar uma região se ela for usada atualmente na política ILM ativa ou na política ILM proposta.
- Se a região usada como filtro avançado em uma regra ILM for inválida, ainda será possível adicionar essa regra à política proposta. No entanto, um erro ocorre se você tentar salvar ou ativar a política proposta.

Uma região inválida pode resultar se você usar uma região como um filtro avançado em uma regra ILM, mas excluir essa região posteriormente, ou se você usar a API de Gerenciamento de Grade para criar uma regra e especificar uma região que você não definiu.

- Se você excluir uma região depois de usá-la para criar um bucket do S3, será necessário adicionar novamente a região se quiser usar o filtro avançado restrição de localização para encontrar objetos nesse bucket.

Passos

1. Selecione **ILM > Regiões**.

É apresentada a página Regiões, com as regiões atualmente definidas listadas. **Região 1** mostra a região padrão `us-east-1`, que não pode ser modificada ou removida.

2. Para adicionar uma região:

- a. Selecione o ícone de inserção **+** à direita da última entrada.
- b. Insira o nome de uma região que você deseja usar ao criar buckets do S3.

Você deve usar esse nome exato da região como o elemento de solicitação LocationConstraint ao criar o bucket S3 correspondente.

3. Para remover uma região não utilizada, selecione o ícone de exclusão **X**.

Uma mensagem de erro será exibida se você tentar remover uma região atualmente usada na política ativa ou na política proposta.

4. Quando terminar de fazer alterações, selecione **Guardar**.

Agora você pode selecionar essas regiões na seção filtros avançados na etapa 1 do assistente criar regra ILM. "[Use filtros avançados nas regras do ILM](#)" Consulte .

Criar regra ILM

Criar uma regra ILM: Visão geral

Para gerenciar objetos, você cria um conjunto de regras de gerenciamento do ciclo de vida das informações (ILM) e as organiza em uma política ILM.

Cada objeto ingerido no sistema é avaliado em relação à política ativa. Quando uma regra na política corresponde aos metadados de um objeto, as instruções na regra determinam quais ações o StorageGRID executa para copiar e armazenar esse objeto.



Os metadados de objetos não são gerenciados pelas regras do ILM. Em vez disso, os metadados de objetos são armazenados em um banco de dados Cassandra no que é conhecido como armazenamento de metadados. Três cópias dos metadados de objetos são mantidas automaticamente em cada local para proteger os dados da perda.

Elementos de uma regra ILM

Uma regra ILM tem três elementos:

- **Critérios de filtragem:** Os filtros básicos e avançados de uma regra definem a que objetos a regra se aplica. Se um objeto corresponder a todos os filtros, o StorageGRID aplicará a regra e criará as cópias de objeto especificadas nas instruções de colocação da regra.
- **Instruções de colocação:** As instruções de colocação de uma regra definem o número, o tipo e a localização das cópias de objetos. Cada regra pode incluir uma sequência de instruções de posicionamento para alterar o número, o tipo e a localização das cópias de objetos ao longo do tempo. Quando o período de tempo para um posicionamento expira, as instruções na próxima colocação são aplicadas automaticamente pela próxima avaliação ILM.
- **Comportamento de ingestão:** O comportamento de ingestão de uma regra permite que você escolha como os objetos filtrados pela regra são protegidos à medida que são ingeridos (quando um cliente S3 ou Swift salva um objeto na grade).

Filtragem de regras ILM

Quando você cria uma regra ILM, você especifica filtros para identificar quais objetos a regra se aplica.

No caso mais simples, uma regra pode não usar nenhum filtro. Qualquer regra que não use filtros se aplica a todos os objetos, portanto, deve ser a última regra (padrão) em uma política ILM. A regra padrão fornece instruções de armazenamento para objetos que não correspondem aos filtros em outra regra.

- Os filtros básicos permitem que você aplique regras diferentes a grupos grandes e distintos de objetos. Esses filtros permitem que você aplique uma regra a contas de locatário específicas, buckets específicos do S3 ou contentores Swift, ou ambos.

Os filtros básicos oferecem uma maneira simples de aplicar regras diferentes a um grande número de objetos. Por exemplo, os Registros financeiros da sua empresa podem precisar ser armazenados para atender aos requisitos regulatórios, enquanto os dados do departamento de marketing podem precisar ser armazenados para facilitar as operações diárias. Depois de criar contas de inquilino separadas para cada departamento ou depois de segregar dados dos diferentes departamentos em intervalos separados do S3, você pode facilmente criar uma regra que se aplica a todos os Registros financeiros e uma segunda regra que se aplica a todos os dados de marketing.

- Filtros avançados oferecem controle granular. Você pode criar filtros para selecionar objetos com base nas seguintes propriedades do objeto:
 - Tempo de ingestão
 - Último tempo de acesso
 - Todo ou parte do nome do objeto (chave)
 - Restrição de localização (apenas S3)
 - Tamanho do objeto
 - Metadados do usuário
 - Etiqueta de objeto (apenas S3)

Você pode filtrar objetos em critérios muito específicos. Por exemplo, os objetos armazenados pelo departamento de imagiologia de um hospital podem ser utilizados frequentemente quando têm menos de 30 dias de idade e pouco depois, enquanto os objetos que contêm informações sobre a visita do paciente podem precisar de ser copiados para o departamento de faturação na sede da rede de saúde. Você pode criar filtros que identificam cada tipo de objeto com base no nome, tamanho, tags de objeto S3D ou qualquer outro critério relevante e, em seguida, criar regras separadas para armazenar cada conjunto de objetos adequadamente.

Você pode combinar filtros conforme necessário em uma única regra. Por exemplo, o departamento de marketing pode querer armazenar arquivos de imagem grandes de forma diferente dos Registros de seus fornecedores, enquanto o departamento de recursos humanos pode precisar armazenar Registros de pessoal em uma geografia específica e informações de políticas centralmente. Nesse caso, você pode criar regras que filtram por conta de locatário para segregar os Registros de cada departamento, enquanto usa filtros em cada regra para identificar o tipo específico de objetos aos quais a regra se aplica.

Instruções de colocação de regra ILM

As instruções de posicionamento determinam onde, quando e como os dados do objeto são armazenados. Uma regra ILM pode incluir uma ou mais instruções de colocação. Cada instrução de colocação aplica-se a um único período de tempo.

Ao criar instruções de colocação:

- Você começa especificando o tempo de referência, que determina quando as instruções de colocação começam. O tempo de referência pode ser quando um objeto é ingerido, quando um objeto é acessado, quando um objeto versionado se torna não atual ou um tempo definido pelo usuário.
- Em seguida, você especifica quando o posicionamento será aplicado, em relação ao tempo de referência. Por exemplo, uma colocação pode começar no dia 0 e continuar por 365 dias, em relação a quando o objeto foi ingerido.
- Por fim, você especifica o tipo de cópias (replicação ou codificação de apagamento) e o local onde as cópias são armazenadas. Por exemplo, você pode querer armazenar duas cópias replicadas em dois sites diferentes.

Cada regra pode definir vários posicionamentos para um único período de tempo e diferentes posicionamentos para diferentes períodos de tempo.

- Para colocar objetos em vários locais durante um único período de tempo, selecione **Adicionar outro tipo ou local** para adicionar mais de uma linha para esse período de tempo.
- Para colocar objetos em locais diferentes em períodos de tempo diferentes, selecione **Adicionar outro período de tempo** para adicionar o próximo período de tempo. Em seguida, especifique uma ou mais

linhas dentro do período de tempo.

O exemplo mostra duas instruções de posicionamento na página Definir posicionamentos do assistente criar regra ILM.

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

The screenshot displays the configuration for two time periods.
Time period 1: From Day 0, store for 365 days. It includes two placement instructions: 1) 'Store objects by replicating 2 copies at Data Center 1, Data Center 2' (circled with a '1') and 2) 'and store objects by erasure coding using 6+3 EC scheme at All 3 sites (6 plus 3)'.
Time period 2: From Day 365, store forever. It includes one placement instruction: 'Store objects by replicating 2 copies at Archive' (circled with a '2').

A primeira instrução de colocação **1** tem duas linhas para o primeiro ano:

- A primeira linha cria duas cópias de objeto replicadas em dois locais de data center.
- A segunda linha cria uma cópia codificada por apagamento de mais de 6 3 usando três locais de data center.

A segunda instrução de colocação **2** cria duas cópias arquivadas após um ano e mantém essas cópias para sempre.

Quando você define o conjunto de instruções de colocação para uma regra, você deve garantir que pelo menos uma instrução de colocação comece no dia 0, que não haja lacunas entre os períodos de tempo definidos e que a instrução de colocação final continue para sempre ou até que você não precise mais nenhuma cópia de objeto.

À medida que cada período de tempo na regra expira, as instruções de colocação de conteúdo para o próximo período de tempo são aplicadas. Novas cópias de objetos são criadas e todas as cópias desnecessárias são excluídas.

Comportamento de ingestão de regra de ILM

O comportamento de ingestão controla se as cópias de objeto são imediatamente colocadas de acordo com as instruções na regra, ou se cópias provisórias são feitas e as instruções de posicionamento são aplicadas posteriormente. Os seguintes comportamentos de ingestão estão disponíveis para regras ILM:

- **Balanced:** O StorageGRID tenta fazer todas as cópias especificadas na regra ILM no ingest; se isso não for possível, cópias provisórias são feitas e o sucesso é retornado ao cliente. As cópias especificadas na

regra ILM são feitas quando possível.

- **Strict:** Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja devolvido ao cliente.
- * Commit duplo*: O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

Informações relacionadas

- ["Opções de ingestão"](#)
- ["Vantagens, desvantagens e limitações das opções de ingestão"](#)
- ["Como os controles de consistência e as regras de ILM interagem para afetar a proteção de dados"](#)

Exemplo de regra ILM

Como exemplo, uma regra ILM pode especificar o seguinte:

- Aplicar apenas aos objetos pertencentes ao Locatário A..
- Faça duas cópias replicadas desses objetos e armazene cada cópia em um local diferente.
- Guarde as duas cópias para sempre, o que significa que o StorageGRID não as eliminará automaticamente. Em vez disso, o StorageGRID manterá esses objetos até que sejam excluídos por uma solicitação de exclusão de cliente ou pela expiração de um ciclo de vida de bucket.
- Use a opção equilibrada para comportamento de ingestão: A instrução de colocação de dois locais é aplicada assim que o locatário A salva um objeto no StorageGRID, a menos que não seja possível fazer imediatamente ambas as cópias necessárias.

Por exemplo, se o local 2 estiver inacessível quando o locatário A salva um objeto, o StorageGRID fará duas cópias provisórias nos nós de storage no local 1. Assim que o Site 2 estiver disponível, a StorageGRID fará a cópia necessária nesse site.

Informações relacionadas

- ["O que é um pool de storage?"](#)
- ["O que é um Cloud Storage Pool?"](#)

Acesse o assistente criar uma regra ILM

As regras do ILM permitem gerenciar o posicionamento dos dados do objeto ao longo do tempo. Para criar uma regra ILM, use o assistente criar uma regra ILM.



Se você quiser criar a regra ILM padrão para uma política, siga o ["Instruções para criar uma regra ILM padrão"](#) em vez disso.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem permissões de acesso específicas.
- Se você quiser especificar a que contas de inquilino esta regra se aplica, você tem a permissão Contas de locatário ou você sabe o ID da conta para cada conta.
- Se você quiser que a regra filtre objetos nos metadados da última hora de acesso, as atualizações da última hora de acesso devem ser habilitadas por bucket para S3 ou por container para Swift.

- Você configurou todos os pools de armazenamento em nuvem que planeja usar. "[Crie Cloud Storage Pool](#)" Consulte .
- Você está familiarizado com o "[opções de ingestão](#)".
- Se você precisar criar uma regra compatível para usar com o bloqueio de objetos S3, você estará familiarizado com o "[Requisitos para o bloqueio de objetos S3](#)".
- Opcionalmente, você assistiu o vídeo: "[Vídeo: Regras de gerenciamento do ciclo de vida das informações no StorageGRID 11,7](#)".

-

Sobre esta tarefa

Ao criar regras ILM:

- Considere a topologia do sistema StorageGRID e as configurações de storage.
- Considere quais tipos de cópias de objetos você deseja fazer (replicadas ou codificadas para apagamento) e o número de cópias de cada objeto que são necessárias.
- Determine quais tipos de metadados de objetos são usados nos aplicativos que se conectam ao sistema StorageGRID. As regras do ILM filtram objetos com base em seus metadados.
- Considere onde você quer que cópias de objeto sejam colocadas ao longo do tempo.
- Decida qual opção de ingestão usar (Balanced, strict ou Dual Commit).

Passos

1. Selecione **ILM > regras**.

Com base no número de sites na grade, a regra fazer 2 cópias ou a regra 1 cópia por local é mostrada na lista de regras.



Se a configuração bloqueio de objetos S3D global tiver sido ativada para o sistema StorageGRID, a tabela de resumo inclui uma coluna **compatível** e os detalhes da regra selecionada incluem um campo **compatível**.

2. Selecione **criar**. "[Passo 1 \(introduzir detalhes\)](#)" Do assistente criar uma regra ILM é exibido.

Passo 1 de 3: Insira os detalhes

A etapa **Inserir detalhes** do assistente criar uma regra ILM permite inserir um nome e uma descrição para a regra e definir filtros para a regra.

Inserir uma descrição e definir filtros para a regra são opcionais.

Sobre esta tarefa

Ao avaliar um objeto em relação a um "[Regra ILM](#)", o StorageGRID compara os metadados do objeto com os filtros da regra. Se os metadados do objeto corresponderem a todos os filtros, o StorageGRID usará a regra para colocar o objeto. Você pode criar uma regra para aplicar a todos os objetos ou especificar filtros básicos, como uma ou mais contas de locatário ou nomes de bucket, ou filtros avançados, como o tamanho do objeto ou metadados do usuário.

Passos

1. Digite um nome exclusivo para a regra no campo **Nome**.

2. Opcionalmente, insira uma breve descrição para a regra no campo **Description**.

Você deve descrever o propósito ou função da regra para que você possa reconhecer a regra mais tarde.

3. Opcionalmente, selecione uma ou mais contas de inquilino S3 ou Swift às quais esta regra se aplica. Se esta regra se aplicar a todos os inquilinos, deixe este campo em branco.

Se você não tiver a permissão de acesso root ou a permissão Contas do locatário, não será possível selecionar locatários na lista. Em vez disso, insira o ID do locatário ou insira vários IDs como uma cadeia delimitada por vírgulas.

4. Opcionalmente, especifique os buckets S3 ou os contentores Swift aos quais esta regra se aplica.

Se **Matches All** estiver selecionado (padrão), a regra se aplica a todos os buckets do S3 ou contentores Swift.

5. Para locatários S3, selecione opcionalmente **Yes** para aplicar a regra apenas a versões de objetos mais antigas em buckets do S3 que tenham o controle de versão habilitado.

Se você selecionar **Sim**, "'hora não atual"' será automaticamente selecionado para o tempo de referência em ["Etapa 2 do assistente criar uma regra ILM"](#).



O tempo não atual aplica-se apenas a objetos S3D em buckets habilitados para versionamento. ["Operações em baldes, COLOQUE o controle de versão do balde"](#) Consulte e ["Gerencie objetos com o S3 Object Lock"](#).

Você pode usar essa opção para reduzir o impactos de armazenamento de objetos com controle de versão filtrando versões de objetos não atuais. ["Exemplo 4: Regras ILM e política para objetos com versão S3"](#) Consulte .

6. Opcionalmente, selecione **Adicionar um filtro avançado** para especificar filtros adicionais.

Se você não configurar a filtragem avançada, a regra se aplica a todos os objetos que correspondem aos filtros básicos. Para obter mais informações sobre filtragem avançada, [Use filtros avançados nas regras do ILM](#) consulte e [Especifique vários tipos e valores de metadados](#).

7. Selecione **continuar**. ["Passo 2 \(definir posicionamentos\)"](#) Do assistente criar uma regra ILM é exibido.

Use filtros avançados nas regras do ILM

A filtragem avançada permite criar regras ILM que se aplicam somente a objetos específicos com base em seus metadados. Ao configurar a filtragem avançada para uma regra, você seleciona o tipo de metadados que deseja corresponder, seleciona um operador e especifica um valor de metadados. Quando os objetos são avaliados, a regra ILM é aplicada somente aos objetos que têm metadados correspondentes ao filtro avançado.

A tabela mostra os tipos de metadados que você pode especificar em filtros avançados, os operadores que você pode usar para cada tipo de metadados e os valores de metadados esperados.

Tipo de metadados	Operadores suportados	Valor dos metadados
Tempo de ingestão	<ul style="list-style-type: none"> • is • não é • é antes • está ligado ou antes • é depois • está ligado ou depois 	<p>Hora e data em que o objeto foi ingerido.</p> <p>Observação: para evitar problemas de recursos ao ativar uma nova política ILM, você pode usar o filtro avançado de tempo de ingestão em qualquer regra que possa alterar a localização de grandes números de objetos existentes. Defina o tempo de ingestão para ser maior ou igual ao tempo aproximado em que a nova política entrará em vigor para garantir que os objetos existentes não sejam movidos desnecessariamente.</p>
Chave	<ul style="list-style-type: none"> • igual a • não é igual • contém • não contém • começa com • não começa com • termina com • não termina com 	<p>Toda ou parte de uma chave de objeto S3 ou Swift única.</p> <p>Por exemplo, você pode querer combinar objetos que terminam com <code>.txt</code> ou começam <code>test-object/</code> com <code>.</code></p>
Último tempo de acesso	<ul style="list-style-type: none"> • is • não é • é antes • está ligado ou antes • é depois • está ligado ou depois 	<p>Hora e data em que o objeto foi recuperado pela última vez (lido ou visualizado).</p> <p>Observação: se você planeja "use o último tempo de acesso" como um filtro avançado, as atualizações do último tempo de acesso devem estar ativadas para o bucket S3 ou o contentor Swift.</p>
Restrição de localização (apenas S3)	<ul style="list-style-type: none"> • igual a • não é igual 	<p>A região onde foi criado um bucket S3. Utilize ILM > Regiões para definir as regiões que são apresentadas.</p> <p>Nota: Um valor de US-East-1 irá corresponder objetos em buckets criados na região US-East-1, bem como objetos em buckets que não têm nenhuma região especificada. "Configurar regiões (opcional e apenas S3)" Consulte .</p>

Tipo de metadados	Operadores suportados	Valor dos metadados
Tamanho do objeto	<ul style="list-style-type: none"> • igual a • não é igual • menos de • inferior ou igual a • superior a. • maior ou igual a 	<p>O tamanho do objeto.</p> <p>A codificação de apagamento é mais adequada para objetos com mais de 1 MB. Não use a codificação de apagamento para objetos com menos de 200 KB para evitar a sobrecarga de gerenciamento de fragmentos codificados de apagamento muito pequenos.</p> <p>Nota: para filtrar em tamanhos de objetos menores que 1 MB, insira um valor decimal. O tipo de navegador e as configurações de localidade controlam se você precisa usar um ponto ou uma vírgula como separador decimal.</p>
Metadados do usuário	<ul style="list-style-type: none"> • contém • termina com • igual a • existe • não contém • não termina com • não é igual • não existe • não começa com • começa com 	<p>Par chave-valor, onde Nome dos metadados do usuário é a chave e valor dos metadados é o valor.</p> <p>Por exemplo, para filtrar objetos que têm metadados de usuário do <code>color=blue</code>, especifique <code>color</code> para Nome de metadados de usuário, <code>equals</code> para o operador e <code>blue</code> para valor de metadados.</p> <p>Observação: os nomes de metadados do usuário não são sensíveis a maiúsculas e minúsculas; os valores de metadados do usuário são sensíveis a maiúsculas e minúsculas.</p>
Etiqueta de objeto (apenas S3)	<ul style="list-style-type: none"> • contém • termina com • igual a • existe • não contém • não termina com • não é igual • não existe • não começa com • começa com 	<p>Par chave-valor, onde Nome da tag objeto é a chave e valor da tag objeto é o valor.</p> <p>Por exemplo, para filtrar objetos que têm uma tag de objeto de <code>Image=True</code>, especifique <code>Image</code> para Nome da tag de objeto, <code>equals</code> para o operador e <code>True</code> para valor da tag de objeto.</p> <p>Nota: nomes de marcas de objetos e valores de tags de objetos são sensíveis a maiúsculas e minúsculas. Você deve inserir esses itens exatamente como eles foram definidos para o objeto.</p>

Especifique vários tipos e valores de metadados

Ao definir filtragem avançada, você pode especificar vários tipos de metadados e vários valores de metadados. Por exemplo, se você quiser que uma regra corresponda a objetos entre 10 MB e 100 MB de tamanho, você selecionaria o tipo de metadados **tamanho do objeto** e especificaria dois valores de

metadados.

- O primeiro valor de metadados especifica objetos maiores ou iguais a 10 MB.
- O segundo valor de metadados especifica objetos menores ou iguais a 100 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

Object size greater than or equal to 10 MB

and Object size less than or equal to 100 MB

O uso de várias entradas permite que você tenha controle preciso sobre quais objetos são correspondidos. No exemplo a seguir, a regra se aplica a objetos que têm uma marca A ou marca B como o valor dos metadados do usuário `camera_type`. No entanto, a regra só se aplica aos objetos da marca B menores que 10 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

User metadata camera_type equals Brand A

Add another advanced filter

or Filter group 2 Objects with all of following metadata will be evaluated by this rule:

User metadata camera_type equals Brand B

and Object size less than or equal to 10 MB

Add another advanced filter

Passo 2 de 3: Definir posicionamentos

A etapa **Definir posicionamentos** do assistente criar regra ILM permite definir as instruções de posicionamento que determinam quanto tempo os objetos são armazenados, o tipo de cópias (replicadas ou codificadas de apagamento), o local de armazenamento e o número de cópias.

Sobre esta tarefa

Uma regra ILM pode incluir uma ou mais instruções de colocação. Cada instrução de colocação aplica-se a um único período de tempo. Quando você usa mais de uma instrução, os períodos de tempo devem ser contíguos, e pelo menos uma instrução deve começar no dia 0. As instruções podem continuar para sempre ou até que você não precise mais nenhuma cópia de objeto.

Cada instrução de colocação pode ter várias linhas se você quiser criar diferentes tipos de cópias ou usar locais diferentes durante esse período de tempo.

Neste exemplo, a regra ILM armazena uma cópia replicada no local 1 e uma cópia replicada no local 2 para o primeiro ano. Após um ano, uma cópia codificada por apagamento de 2 mais de 1 é feita e salva em apenas um local.

Time period 1
From Day store for days
✕

Store objects by

replicating

1

copies at

Site 1

✕
✎
✕

and store objects by

replicating

1

copies at

Site 2

✕
✎
✕

[Add other type or location](#)

Time period 2
From Day store forever
✕

Store objects by

erasure coding

using

2+1 EC scheme at Site 3

✕
✎

[Add other type or location](#)

Passos

1. Para **tempo de referência**, selecione o tipo de tempo a ser utilizado para calcular a hora de início de uma instrução de colocação.

Opção	Descrição
Tempo de ingestão	O tempo em que o objeto foi ingerido.
Último tempo de acesso	A hora em que o objeto foi recuperado pela última vez (lido ou visualizado). Observação: para usar essa opção, as atualizações do último tempo de acesso devem estar ativadas para o bucket S3 ou o contendor Swift. "Use o último tempo de acesso nas regras do ILM" Consulte .
Tempo de criação definido pelo utilizador	Um tempo especificado nos metadados definidos pelo usuário.
Hora não atual	"hora não atual" será selecionado automaticamente se você selecionou Sim para a pergunta, "aplicar esta regra apenas a versões de objetos mais antigas (em buckets do S3 com controle de versão ativado)?" em "Etapa 1 do assistente criar uma regra ILM" .



Se você quiser criar uma regra compatível, selecione **tempo de ingestão**. ["Gerencie objetos com o S3 Object Lock"](#) Consulte .

2. Na seção **período de tempo e colocações**, insira uma hora de início e uma duração para o primeiro período de tempo.

Por exemplo, você pode querer especificar onde armazenar objetos para o primeiro ano (*from day 0 store for 365 Days*). Pelo menos uma instrução deve começar no dia 0.

3. Se você quiser criar cópias replicadas:
 - a. Na lista suspensa **Store Objects by**, selecione **replicating**.
 - b. Selecione o número de cópias que deseja fazer.

Um aviso será exibido se você alterar o número de cópias para 1. Uma regra de ILM que cria apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. "[Por que você não deve usar replicação de cópia única](#)" Consulte .

Para evitar o risco, faça um ou mais dos seguintes procedimentos:

- Aumente o número de cópias para o período de tempo.
- Adicione cópias a outros pools de storage ou a um pool de storage de nuvem.
- Selecione **codificação de apagamento** em vez de **replicação**.

Você pode ignorar esse aviso com segurança se essa regra já criar várias cópias para todos os períodos de tempo.

- c. No campo **Copies at**, selecione os pools de armazenamento que deseja adicionar.

Se você especificar apenas um pool de armazenamento, esteja ciente de que o StorageGRID pode armazenar apenas uma cópia replicada de um objeto em qualquer nó de armazenamento. Se a grade incluir três nós de storage e você selecionar 4 como o número de cópias, apenas três cópias serão feitas & no. 8212; uma cópia para cada nó de storage.



O alerta **ILM Placement Unachievable** é acionado para indicar que a regra ILM não pôde ser completamente aplicada.

Se você especificar mais de um pool de armazenamento, tenha em mente estas regras:

- O número de cópias não pode ser maior do que o número de pools de armazenamento.
- Se o número de cópias for igual ao número de pools de storage, uma cópia do objeto será armazenada em cada pool de storage.
- Se o número de cópias for menor que o número de pools de storage, uma cópia será armazenada no local de ingestão e, em seguida, o sistema distribui as cópias restantes para manter o uso do disco entre os pools balanceado, garantindo que nenhum local receba mais de uma cópia de um objeto.
- Se os pools de storage se sobreporem (contiverem os mesmos nós de storage), todas as cópias do objeto poderão ser salvas em apenas um local. Por esse motivo, não especifique o pool de storage de todos os nós de storage (StorageGRID 11,6 e anterior) e outro pool de storage.

4. Se você quiser criar uma cópia codificada por apagamento:

- a. Na lista suspensa **armazenar objetos por**, selecione **codificação de apagamento**.



A codificação de apagamento é mais adequada para objetos com mais de 1 MB. Não use a codificação de apagamento para objetos com menos de 200 KB para evitar a sobrecarga de gerenciamento de fragmentos codificados de apagamento muito pequenos.

- b. Se você não adicionou um filtro de tamanho de objeto para um valor maior que 0,2 MB, selecione **anterior** para retornar à Etapa 1. Em seguida, selecione **Adicionar um filtro avançado** e defina um filtro **tamanho do objeto** para qualquer valor maior que 0,2 MB.

- c. Selecione o pool de armazenamento que deseja adicionar e o esquema de codificação de apagamento que deseja usar.

O local de storage para uma cópia codificada de apagamento inclui o nome do esquema de codificação de apagamento, seguido do nome do pool de storage.

5. Opcionalmente:

- a. Selecione **Adicionar outro tipo ou local** para criar cópias adicionais em locais diferentes.
- b. Selecione **Adicionar outro período de tempo** para adicionar diferentes períodos de tempo.



Os objetos são automaticamente excluídos no final do período de tempo final, a menos que o período de tempo final termine com **Forever**.

6. Se você quiser armazenar objetos em um pool de armazenamento em nuvem:




- a. Na lista suspensa **Store Objects by**, selecione **replicating**.
- b. Selecione o campo **Copies at e**, em seguida, selecione um pool de armazenamento em nuvem.

Ao usar Cloud Storage Pools, tenha em mente estas regras:

- Você não pode selecionar mais de um pool de armazenamento em nuvem em uma única instrução de colocação. Da mesma forma, você não pode selecionar um pool de armazenamento em nuvem e um pool de armazenamento na mesma instrução de colocação.
- Você pode armazenar apenas uma cópia de um objeto em qualquer pool de armazenamento em nuvem. Uma mensagem de erro será exibida se você definir **Copies** como 2 ou mais.
- Você não pode armazenar mais de uma cópia de objeto em qualquer pool de armazenamento em nuvem ao mesmo tempo. Uma mensagem de erro será exibida se vários posicionamentos que usam um pool de armazenamento em nuvem tiverem datas sobrepostas ou se várias linhas no mesmo posicionamento usarem um pool de armazenamento em nuvem.
- Você pode armazenar um objeto em um pool de storage de nuvem ao mesmo tempo em que o objeto está sendo armazenado como cópias replicadas ou codificadas de apagamento no StorageGRID. No entanto, você deve incluir mais de uma linha na instrução de colocação para o período de tempo, para que você possa especificar o número e os tipos de cópias para cada local.

7. No diagrama de retenção, confirme as instruções de colocação.

Cada linha no diagrama mostra onde e quando cópias de objetos serão colocadas. A cor de uma linha representa o tipo de cópia:

	Cópia replicada
	Com codificação de apagamento
	Cópia do Cloud Storage Pool

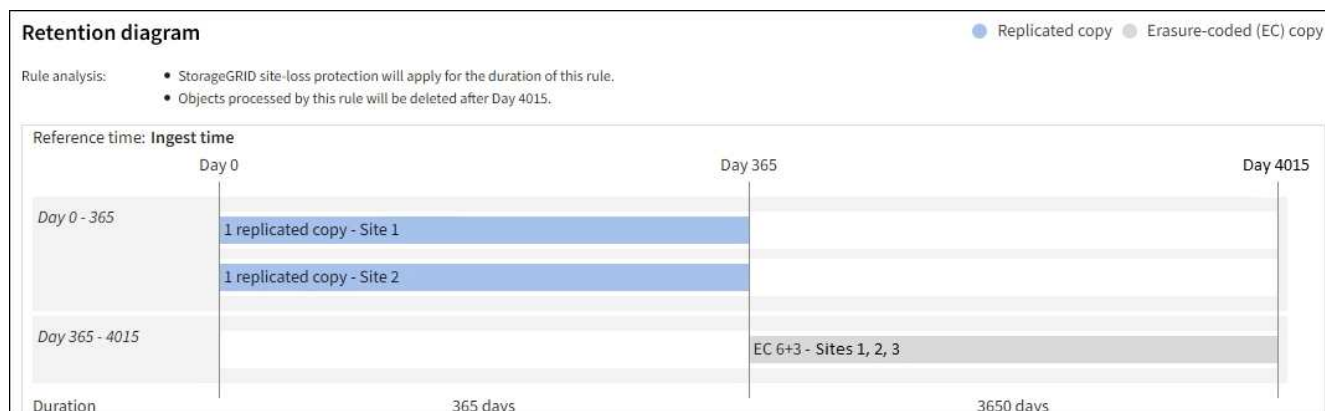
Neste exemplo, a regra ILM armazena uma cópia replicada no local 1 e uma cópia replicada no local 2 para o primeiro ano. Depois de um ano e por mais 10 anos, uma cópia codificada por apagamento 6-3 será salva em três sites. Após 11 anos no total, os objetos serão excluídos do StorageGRID.

A seção análise de regras do diagrama de retenção afirma:

- A proteção contra perda de site da StorageGRID será aplicada durante a duração desta regra.
- Os objetos processados por esta regra serão excluídos após o dia 4015.



Consulte "[Ativar a proteção contra perda de local.](#)"



8. Selecione **continuar**. "[Etapa 3 \(Selecionar comportamento de ingestão\)](#)" Do assistente criar uma regra ILM é exibido.

Use o último tempo de acesso nas regras do ILM

Você pode usar a hora do último acesso como hora de referência em uma regra ILM. Por exemplo, você pode querer deixar objetos que foram visualizados nos últimos três meses em nós de storage local, enquanto move objetos que não foram vistos recentemente para um local externo. Você também pode usar o último tempo de acesso como um filtro avançado se quiser que uma regra ILM se aplique apenas a objetos que foram acessados pela última vez em uma data específica.

Sobre esta tarefa

Antes de usar o último tempo de acesso em uma regra ILM, revise as seguintes considerações:

- Ao usar a hora do último acesso como hora de referência, esteja ciente de que alterar a hora do último acesso de um objeto não aciona uma avaliação ILM imediata. Em vez disso, os posicionamentos do objeto são avaliados e o objeto é movido conforme necessário quando ILM em segundo plano avalia o objeto. Isso pode levar duas semanas ou mais depois que o objeto é acessado.

Leve essa latência em consideração ao criar regras de ILM com base no último tempo de acesso e evite colocações que usam períodos de tempo curtos (menos de um mês).

- Ao usar o último tempo de acesso como um filtro avançado ou como uma hora de referência, você deve habilitar as atualizações da última hora de acesso para buckets do S3. Pode utilizar a "[Gerente do localatário](#)" ou a "[API de gerenciamento do localatário](#)".



As atualizações do último tempo de acesso são sempre ativadas para contentores Swift, mas são desativadas por padrão para buckets do S3.



Esteja ciente de que ativar as atualizações do último tempo de acesso pode reduzir o desempenho, especialmente em sistemas com objetos pequenos. O impacto no desempenho ocorre porque o StorageGRID deve atualizar os objetos com novos timestamps sempre que os objetos são recuperados.

A tabela a seguir resume se o último tempo de acesso é atualizado para todos os objetos no intervalo para diferentes tipos de solicitações.

Tipo de solicitação	Se a última hora de acesso é atualizada quando as atualizações da última hora de acesso são desativadas	Se a última hora de acesso é atualizada quando as atualizações da última hora de acesso estão ativadas
Solicitação para recuperar um objeto, sua lista de controle de acesso ou seus metadados	Não	Sim
Solicitação para atualizar os metadados de um objeto	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">• 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

Passo 3 de 3: Selecione comportamento de ingestão

A etapa **Selecionar comportamento de ingestão** do assistente criar regra ILM permite escolher como os objetos filtrados por essa regra são protegidos à medida que são ingeridos.

Sobre esta tarefa

O StorageGRID pode fazer cópias provisórias e enfileirar os objetos para avaliação do ILM mais tarde, ou pode fazer cópias para cumprir as instruções de colocação da regra imediatamente.

Passos

1. Selecione a "[comportamento de ingestão](#)" para utilizar.

Para obter mais informações, "[Vantagens, desvantagens e limitações das opções de ingestão](#)" consulte .

Você não pode usar a opção equilibrada ou rigorosa se a regra usar um desses posicionamentos:



- Um pool de armazenamento em nuvem no dia 0
- Um nó de arquivo no dia 0
- Um pool de armazenamento em nuvem ou um nó de arquivo quando a regra usa um tempo de criação definido pelo usuário como um tempo de referência

["Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"](#) Consulte .

2. Selecione **criar**.

A regra ILM é criada. A regra não se torna ativa até que seja adicionada a uma ["Política de ILM"](#) e essa política seja ativada.

Para exibir os detalhes da regra, selecione o nome da regra na página regras do ILM.

Crie uma regra ILM padrão

Antes de criar uma política de ILM, você deve criar uma regra padrão para colocar objetos não correspondidos por outra regra na política. A regra padrão não pode usar nenhum filtro. Ele deve se aplicar a todos os locatários, todos os buckets e todas as versões de objetos.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem permissões de acesso específicas.

Sobre esta tarefa

A regra padrão é a última regra a ser avaliada em uma política ILM, portanto, ela não pode usar nenhum filtro. As instruções de posicionamento para a regra padrão são aplicadas a quaisquer objetos que não sejam correspondidos por outra regra na política.

Neste exemplo de política, a primeira regra se aplica apenas a objetos pertencentes ao test-tenant-1. A regra padrão, que é a última, aplica-se a objetos pertencentes a todas as outras contas de inquilino.

Proposed policy name

Example ILM policy

Reason for change

Example

Manage rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	↕ EC for test-tenant-1	Tenant is test-tenant-1
Default	Default rule	—

Ao criar a regra padrão, lembre-se destes requisitos:

- A regra padrão é automaticamente colocada como a última regra na política.
- A regra padrão não pode usar nenhum filtro básico ou avançado.
- A regra padrão deve ser aplicada a todas as versões de objetos.
- A regra padrão deve criar cópias replicadas.



Não use uma regra que crie cópias codificadas por apagamento como regra padrão para uma política. As regras de codificação de apagamento devem usar um filtro avançado para evitar que objetos menores sejam codificados para apagamento.

- Em geral, a regra padrão deve manter objetos para sempre.
- Se você estiver usando (ou pretende ativar) a configuração global S3 Object Lock, a regra padrão para a política ativa ou proposta deve ser compatível.

Passos

1. Selecione **ILM > regras**.
2. Selecione **criar**.

O passo 1 (Inserir detalhes) do assistente criar regra ILM é exibido.

3. Digite um nome exclusivo para a regra no campo **Nome da regra**.
4. Opcionalmente, insira uma breve descrição para a regra no campo **Description**.
5. Deixe o campo **Contas do locatário** em branco.

A regra padrão deve ser aplicada a todas as contas de locatário.

6. Deixe a seleção suspensa Nome do balde como **corresponde a todos**.

A regra padrão deve ser aplicada a todos os buckets do S3 e contentores Swift.

7. Mantenha a resposta padrão, **no**, para a pergunta, "aplicar esta regra apenas a versões de objetos mais antigas (em buckets do S3 com controle de versão habilitado)?"

8. Não adicione filtros avançados.

A regra padrão não pode especificar nenhum filtro.

9. Selecione **seguinte**.

É apresentado o passo 2 (Definir posicionamentos).

10. Para tempo de referência, selecione qualquer opção.

Se você manteve a resposta padrão, **não**, para a pergunta, "aplicar esta regra apenas para versões de objetos mais antigas?" o tempo não atual não será incluído na lista suspensa. A regra padrão deve aplicar todas as versões de objeto.

11. Especifique as instruções de colocação para a regra padrão.

- A regra padrão deve manter objetos para sempre. Um aviso aparece quando você ativa uma nova política se a regra padrão não reter objetos para sempre. Você deve confirmar que este é o comportamento que você espera.
- A regra padrão deve criar cópias replicadas.



Não use uma regra que crie cópias codificadas por apagamento como regra padrão para uma política. As regras de codificação de apagamento devem incluir o filtro avançado **Object Size (MB) maior que 0,2** para evitar que objetos menores sejam codificados para apagamento.

- Se você estiver usando (ou pretende ativar) a configuração global S3 Object Lock, a regra padrão deve ser compatível:
 - 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 objetos não podem ser salvas em um pool de armazenamento em nuvem.
 - As cópias de objetos não podem ser guardadas nos nós de arquivo.
 - Pelo menos uma linha das instruções de colocação deve começar no dia 0, usando o tempo de ingestão como o tempo de referência.
 - Pelo menos uma linha das instruções de colocação deve ser "para sempre".

12. Veja o diagrama de retenção para confirmar as instruções de colocação.

13. Selecione **continuar**.

A etapa 3 (Selecionar comportamento de ingestão) é exibida.

14. Selecione a opção de ingestão a utilizar e selecione **criar**.

Criar política ILM

Criar uma política ILM: Visão geral

Uma política de gerenciamento de ciclo de vida das informações (ILM) é um conjunto ordenado de regras ILM que determina como o sistema StorageGRID gerencia os dados de objetos ao longo do tempo.

Quando você cria uma política ILM, você começa selecionando e organizando as regras ILM. Em seguida, você verifica o comportamento de sua política proposta simulando-a contra objetos previamente ingeridos. Quando estiver satisfeito de que a política proposta está a funcionar conforme pretendido, pode ativá-la para criar a política ativa.



Uma política de ILM que foi configurada incorretamente pode resultar em perda de dados irrecoverável. Antes de ativar uma política ILM, revise cuidadosamente a política ILM e suas regras ILM e simule a política ILM. Confirme sempre que a política de ILM funcionará como pretendido.

Política ILM padrão

Quando você instala o StorageGRID e adiciona sites, uma política ILM padrão é criada automaticamente. Se a grade contiver um local, a política padrão conterá uma regra padrão que replica duas cópias de cada objeto nesse local. Se a grade contiver mais de um local, a regra padrão replicará uma cópia de cada objeto em cada local.

Se a política padrão não atender aos requisitos de storage, você poderá criar suas próprias regras e políticas. ["O que é uma regra ILM"](#) Consulte e ["Criando uma política proposta de ILM"](#).

Como uma política ILM avalia objetos?

A política de ILM ativa do seu sistema StorageGRID controla o posicionamento, a duração e a proteção de dados de todos os objetos.

Quando os clientes salvam objetos no StorageGRID, os objetos são avaliados em relação ao conjunto ordenado de regras ILM na política ativa, da seguinte forma:

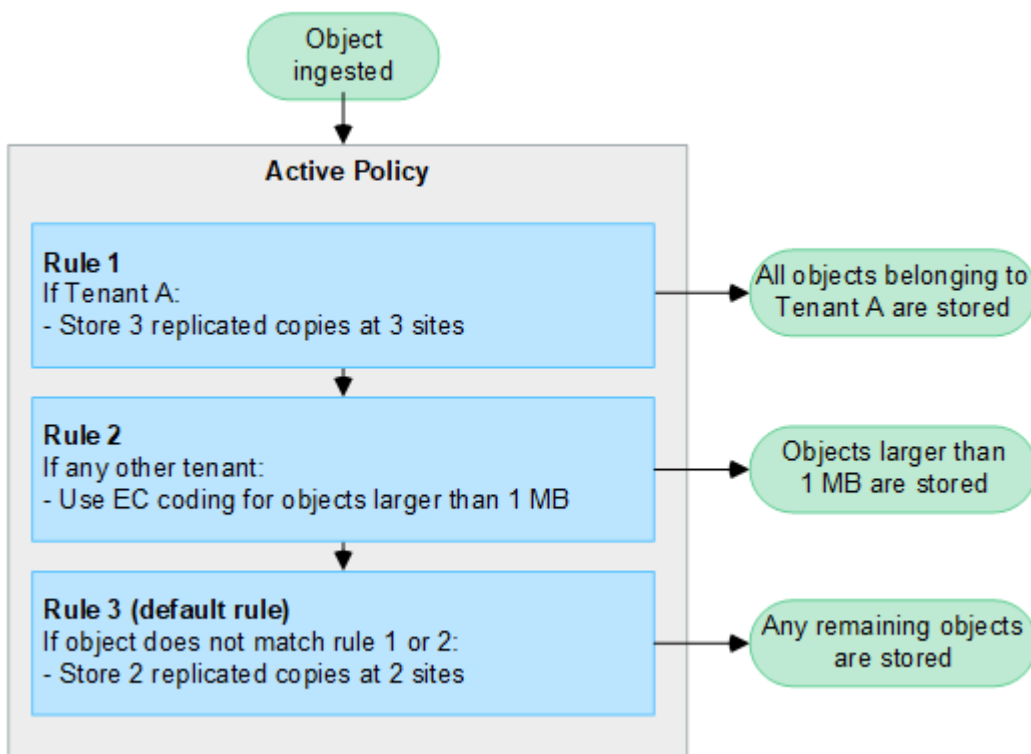
1. Se os filtros da primeira regra na política corresponderem a um objeto, o objeto será ingerido de acordo com o comportamento de ingestão dessa regra e armazenado de acordo com as instruções de colocação dessa regra.
2. Se os filtros da primeira regra não corresponderem ao objeto, o objeto será avaliado em relação a cada regra subsequente na política até que uma correspondência seja feita.
3. Se nenhuma regra corresponder a um objeto, as instruções de comportamento de ingestão e posicionamento da regra padrão na política serão aplicadas. A regra padrão é a última regra de uma política. A regra padrão deve ser aplicada a todos os locatários, todos os buckets e todas as versões de objetos e não pode usar nenhum filtro avançado.

Exemplo de política ILM

Como exemplo, uma política ILM pode conter três regras ILM que especificam o seguinte:

- **Regra 1: Cópias replicadas para o locatário A**

- Corresponder todos os objetos pertencentes ao locatário A..
 - Armazene esses objetos como três cópias replicadas em três locais.
 - Objetos pertencentes a outros inquilinos não são correspondidos pela regra 1, portanto, eles são avaliados em relação à regra 2.
- **Regra 2: Codificação de apagamento para objetos com mais de 1 MB**
 - Combine todos os objetos de outros inquilinos, mas somente se eles forem maiores que 1 MB. Esses objetos maiores são armazenados usando codificação de apagamento 6-3 em três locais.
 - Não corresponde a objetos de 1 MB ou menores, portanto, esses objetos são avaliados em relação à regra 3.
- **Regra 3: 2 cópias 2 data centers (padrão)**
 - É a última regra e padrão na política. Não utiliza filtros.
 - Faça duas cópias replicadas de todos os objetos não correspondidos pela regra 1 ou regra 2 (objetos não pertencentes ao locatário A que tenham 1 MB ou menos).



Quais são as políticas propostas, ativas e históricas?

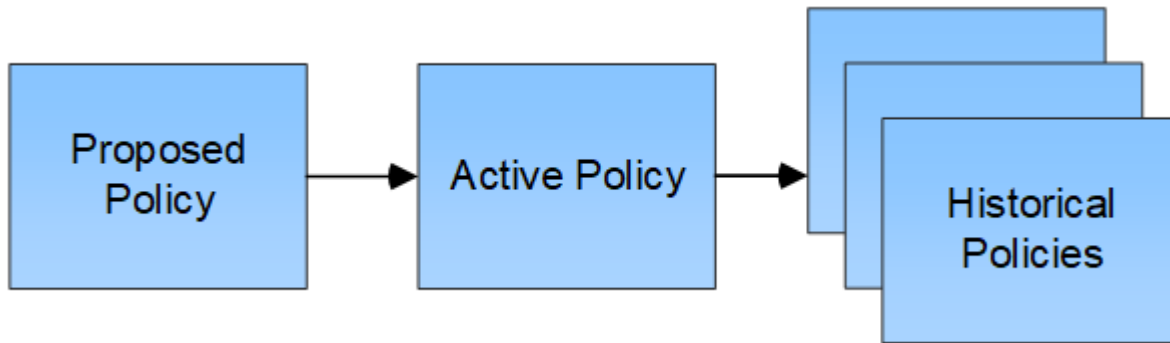
Cada sistema StorageGRID deve ter uma política ILM ativa. Um sistema StorageGRID também pode ter uma política de ILM proposta e qualquer número de políticas históricas.

Ao criar uma política ILM pela primeira vez, você cria uma política proposta selecionando uma ou mais regras ILM e organizando-as em uma ordem específica. Depois de simular a política proposta para confirmar o seu comportamento, ative-a para criar a política ativa.

Quando você ativa uma nova política de ILM, o StorageGRID usa essa política para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Os objetos existentes podem ser movidos para novos locais quando as regras ILM na nova política são implementadas.

Ativar a política proposta faz com que a política anteriormente ativa se torne uma política histórica. As políticas

históricas de ILM não podem ser excluídas.



Considerações para criar uma política ILM

- Utilize apenas a política fornecida pelo sistema, a política de cópias Baseline 2, em sistemas de teste. Para o StorageGRID 11,6 e versões anteriores, a regra fazer 2 cópias nesta política usa o pool de storage de todos os nós de storage, que contém todos os locais. Se o seu sistema StorageGRID tiver mais de um local, duas cópias de um objeto poderão ser colocadas no mesmo local.



O pool de storage de todos os nós de storage é criado automaticamente durante a instalação do StorageGRID 11,6 e versões anteriores. Se você atualizar para uma versão posterior do StorageGRID, o pool todos os nós de storage ainda existirá. Se você instalar o StorageGRID 11,7 ou posterior como uma nova instalação, o pool todos os nós de storage não será criado.

- Ao projetar uma nova política, considere todos os diferentes tipos de objetos que podem ser ingeridos em sua grade. Certifique-se de que a política inclui regras para corresponder e colocar esses objetos conforme necessário.
- Mantenha a política ILM o mais simples possível. Isso evita situações potencialmente perigosas em que os dados de objetos não são protegidos como pretendido quando as alterações são feitas no sistema StorageGRID ao longo do tempo.
- Certifique-se de que as regras da política estão na ordem correta. Quando a política é ativada, objetos novos e existentes são avaliados pelas regras na ordem listada, começando na parte superior. Por exemplo, se a primeira regra de uma política corresponder a um objeto, esse objeto não será avaliado por nenhuma outra regra.
- A última regra em cada política ILM é a regra ILM padrão, que não pode usar nenhum filtro. Se um objeto não tiver sido correspondido por outra regra, a regra padrão controla onde esse objeto é colocado e por quanto tempo ele é retido.
- Antes de ativar uma nova política, revise todas as alterações que a política está fazendo no posicionamento de objetos existentes. Alterar a localização de um objeto existente pode resultar em problemas de recursos temporários quando os novos posicionamentos são avaliados e implementados.

Crie uma política de ILM proposta

Você pode criar uma política de ILM proposta do zero ou clonar a política ativa atual se quiser começar com o mesmo conjunto de regras.

Antes de criar sua própria política, verifique se o "[Política ILM padrão](#)" não atende aos requisitos de storage.



Se o "A definição Global S3 Object Lock foi ativada", você deve garantir que a diretiva ILM esteja em conformidade com os requisitos dos buckets que têm o bloqueio de objeto S3 ativado. Nesta seção, siga as instruções que mencionam ter o bloqueio de objeto S3 ativado.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["permissões de acesso necessárias"](#).
- Você ["Regras ILM criadas"](#) tem baseado se o bloqueio de objeto S3 está ativado.

S3 bloqueio de objetos não ativado

- Você ["Criou as regras ILM"](#) deseja adicionar à política proposta. Conforme necessário, você pode salvar uma política proposta, criar regras adicionais e editar a política proposta para adicionar as novas regras.
- Você tem ["Criou uma regra ILM padrão"](#) que não contém nenhum filtro.

S3 bloqueio de objetos ativado

- ["A definição Global S3 Object Lock já está ativada"](#) para o sistema StorageGRID.
- Você ["Criou as regras ILM em conformidade e não compatível"](#) deseja adicionar à política proposta. Conforme necessário, você pode salvar uma política proposta, criar regras adicionais e editar a política proposta para adicionar as novas regras.
- Você tem ["Criou uma regra ILM padrão"](#) para a política que é compatível.

- Opcionalmente, você assistiu ao vídeo: ["Vídeo: Políticas de gerenciamento do ciclo de vida das informações no StorageGRID 11,7"](#)

■

Consulte também ["Criar uma política ILM: Visão geral"](#).

Sobre esta tarefa

As razões típicas para criar uma política de ILM proposta incluem:

- Você adicionou um novo site e precisa usar novas regras ILM para colocar objetos nesse site.
- Você está desativando um site e você precisa remover todas as regras ILM que se referem ao site.
- Você adicionou um novo localitário com requisitos especiais de proteção de dados.
- Você começou a usar um Cloud Storage Pool.



Utilize apenas a política fornecida pelo sistema, a política de cópias Baseline 2, em sistemas de teste. Para o StorageGRID 11,6 e versões anteriores, a regra padrão dessa política usa o pool de storage de todos os nós de storage, que contém todos os sites. Se o seu sistema StorageGRID tiver mais de um local, duas cópias de um objeto poderão ser colocadas no mesmo local.

Passos

1. Selecione **ILM > políticas**.

Se a configuração Global S3 Object Lock estiver ativada, a página ILM Policies (políticas ILM) indica quais

regras ILM são compatíveis.

2. Determine como você deseja criar a política de ILM proposta. E

Comece do zero

1. Se uma política de ILM proposta existir atualmente, selecione **Política proposta > ações > Remover**.

Não é possível criar uma nova política proposta se uma política proposta já existir.

2. Selecione **criar política proposta > criar nova política**.

Comece com as regras da política ativa

1. Se uma política de ILM proposta existir atualmente, selecione **Política proposta > ações > Remover**.

Não é possível clonar a política ativa se uma política proposta já existir.

2. Selecione **criar política proposta > Clone política ativa**.

Editar a política proposta existente

1. Selecione **Política proposta > ações > Editar**.

1. No campo **Nome da política proposta**, insira um nome exclusivo para a política proposta.
2. No campo **motivo da mudança**, insira o motivo pelo qual você está criando uma nova política proposta.
3. Para adicionar regras à política, selecione **Selecionar regras**. Selecione um nome de regra para exibir as configurações dessa regra.




Periodicamente, a lista de regras é atualizada automaticamente para refletir adições ou remoções. Se uma regra for removida depois de selecioná-la, será exibida uma mensagem de erro.

Se você estiver clonando uma política:

- As regras usadas pela política de clonagem são selecionadas.
- Se a política que você está clonando usou quaisquer regras sem filtros que não eram a regra padrão, você será solicitado a remover todas, exceto uma dessas regras.
- Se a regra padrão usou um filtro, você será solicitado a selecionar uma nova regra padrão.
- Se a regra padrão não for a última regra, você poderá mover a regra para o fim da nova política.

S3 bloqueio de objetos não ativado


1. Selecione uma regra padrão para a política proposta. Para criar uma nova regra padrão, selecione **ILM rules page** .

A regra padrão se aplica a quaisquer objetos que não correspondam a outra regra na política. A regra padrão não pode usar nenhum filtro e é sempre avaliada por último.



Não use a regra fazer cópias 2 como regra padrão para uma política. A regra fazer 2 cópias usa um único pool de storage, todos os nós de storage, que contém todos os locais. Se o seu sistema StorageGRID tiver mais de um local, duas cópias de um objeto poderão ser colocadas no mesmo local.

S3 bloqueio de objetos ativado

1. Selecione uma regra padrão para a política proposta. Para criar uma nova regra padrão, selecione **ILM rules page** .

A lista de regras contém apenas as regras que são compatíveis e não usam filtros.



Não use a regra fazer cópias 2 como regra padrão para uma política. A regra fazer 2 cópias usa um único pool de storage, todos os nós de storage, que contém todos os locais. Se você usar essa regra, várias cópias de um objeto podem ser colocadas no mesmo site.

2. Se você precisar de uma regra diferente de "falha" para objetos em buckets S3 não compatíveis, selecione **incluir uma regra sem filtros para buckets S3 não compatíveis** e selecione uma regra não compatível que não use um filtro.

Por exemplo, você pode querer usar um pool de armazenamento em nuvem para armazenar objetos em buckets que não têm o bloqueio de objeto S3 ativado.



Você só pode selecionar uma regra não compatível que não use um filtro.

Consulte também ["Exemplo 7: Política de ILM compatível para bloqueio de objetos S3"](#).

1. Quando terminar de selecionar a regra padrão, selecione **continuar**.
2. Para a etapa outras regras, selecione quaisquer outras regras que você deseja adicionar à política. Essas regras usam pelo menos um filtro (conta de locatário, nome do bucket, filtro avançado ou tempo de referência não atual). Em seguida, selecione **Select**.

A janela criar uma política proposta agora lista as regras selecionadas. A regra padrão está no final, com as outras regras acima dela.

Se o bloqueio de objeto S3 estiver ativado e você também tiver selecionado uma regra "falha" não compatível, essa regra será adicionada como a regra de segunda a última na política.



Um aviso aparece se qualquer regra não reter objetos para sempre. Quando você ativa essa política, você deve confirmar que deseja que o StorageGRID exclua objetos quando as instruções de posicionamento da regra padrão decorrerem (a menos que um ciclo de vida de bucket mantenha os objetos por um período de tempo mais longo).

3. Arraste as linhas para as regras não padrão para determinar a ordem em que essas regras serão avaliadas.

Não é possível mover a regra padrão. Se o bloqueio de objetos S3 estiver ativado, você também não poderá mover a regra "falha" não compatível se uma tiver sido selecionada.



Você deve confirmar se as regras ILM estão na ordem correta. Quando a política é ativada, objetos novos e existentes são avaliados pelas regras na ordem listada, começando na parte superior.

4. Conforme necessário, selecione **Selecionar regras** para adicionar ou remover regras.
5. Quando terminar, selecione **Guardar**.
6. Vá para "[Simule uma política de ILM](#)". Você deve sempre simular uma política proposta antes de ativá-la para garantir que funcione como esperado.

Simule uma política de ILM

Simule uma política proposta em objetos de teste antes de ativar a política e aplicá-la aos dados de produção. A janela de simulação fornece um ambiente autônomo que é seguro para políticas de teste antes de serem ativadas e aplicadas aos dados no ambiente de produção.

Antes de começar


- Você está conectado ao Gerenciador de Grade usando um "[navegador da web suportado](#)".
- Você tem o "[permissões de acesso necessárias](#)".
- Você conhece o bucket/object-key do S3 ou o container/object-name do Swift para cada objeto que deseja testar.

Sobre esta tarefa

Selecione cuidadosamente os objetos que deseja testar a política proposta. Para simular uma política completamente, você deve testar pelo menos um objeto para cada filtro em cada regra.

Por exemplo, se uma política incluir uma regra para combinar objetos no bucket A e outra regra para corresponder objetos no bucket B, você deve selecionar pelo menos um objeto do bucket A e um objeto do bucket B para testar a política completamente. Você também deve selecionar pelo menos um objeto de outro intervalo para testar a regra padrão.

Ao simular uma política, aplicam-se as seguintes considerações:

- Depois de fazer alterações em uma política, salve a política proposta. Em seguida, simule o comportamento da política proposta salva.
- Ao simular uma política, as regras ILM na política filtram os objetos de teste, para que você possa ver qual regra foi aplicada a cada objeto. No entanto, nenhuma cópia de objeto é feita e nenhum objeto é colocado. Executar uma simulação não modifica seus dados, regras ou política de forma alguma.
- A janela simular política proposta mantém os objetos testados até selecionar **Clear All** (Limpar tudo) ou o ícone remove (remover ) para cada objeto na lista Simulation Results (resultados da simulação).
- Simulação retorna o nome da regra correspondente. Para determinar qual pool de armazenamento ou perfil de codificação de apagamento está em vigor, selecione o nome da regra para ir para a página de detalhes da regra, onde você pode visualizar o diagrama de retenção e outros detalhes sobre a regra.

- Se o controle de versão S3 estiver ativado, você poderá inserir o ID da versão para a versão do objeto que deseja usar para a simulação.

Passos

1. "Criar uma política proposta".
2. Usando um cliente S3 ou Swift ou o "Console experimental S3", que está disponível no Gerenciador de inquilinos para cada locatário, ingira os objetos necessários para testar cada regra.
3. Na página de política ILM, guia política proposta, selecione **simular**.
4. No campo **Object**, digite S3 bucket/object-key ou Swift container/object-name para um objeto de teste. Por exemplo, bucket-01/filename.png.
5. Opcionalmente, insira um ID de versão para o objeto no campo **Version ID**.
6. Selecione **simular**.
7. Na seção resultados da simulação, confirme se cada objeto foi correspondido pela regra correta.

Exemplo 1: Verificar regras ao simular uma política de ILM proposta

Este exemplo descreve como verificar regras ao simular uma política proposta.

Neste exemplo, a política **exemplo de ILM** está sendo simulada contra os objetos ingeridos em dois buckets. A política inclui três regras, como segue:

- A primeira regra, **duas cópias, dois anos para bucket-a**, aplica-se apenas a objetos em bucket-a.
- A segunda regra, **objetos EC > 1 MB**, aplica-se a todos os intervalos, mas filtros em objetos com mais de 1 MB.
- A terceira regra, **duas cópias, dois data centers**, é a regra padrão. Ele não inclui nenhum filtro e não usa o tempo de referência não atual.

Depois de simular a política, confirme se cada objeto foi correspondido pela regra correta.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
<input type="button" value="Clear all"/>				
Object	Version ID	Rule matched	Previous match	Actions
bucket-a/bucket-a object.pdf	—	Two copies, two years for bucket-a	—	
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	

Neste exemplo:

- bucket-a/bucket-a object.pdf corresponde corretamente à primeira regra, que filtra os objetos no bucket-a.
- bucket-b/test object greater than 1 MB.pdf está em bucket-b, por isso não corresponde à

primeira regra. Em vez disso, foi corretamente correspondido pela segunda regra, que filtra em objetos com mais de 1 MB.

- `bucket-b/test object less than 1 MB.pdf` não corresponde aos filtros nas duas primeiras regras, por isso será colocado pela regra padrão, que não inclui filtros.

Exemplo 2: Reordenar regras ao simular uma política de ILM proposta

Este exemplo mostra como você pode reordenar regras para alterar os resultados ao simular uma política.

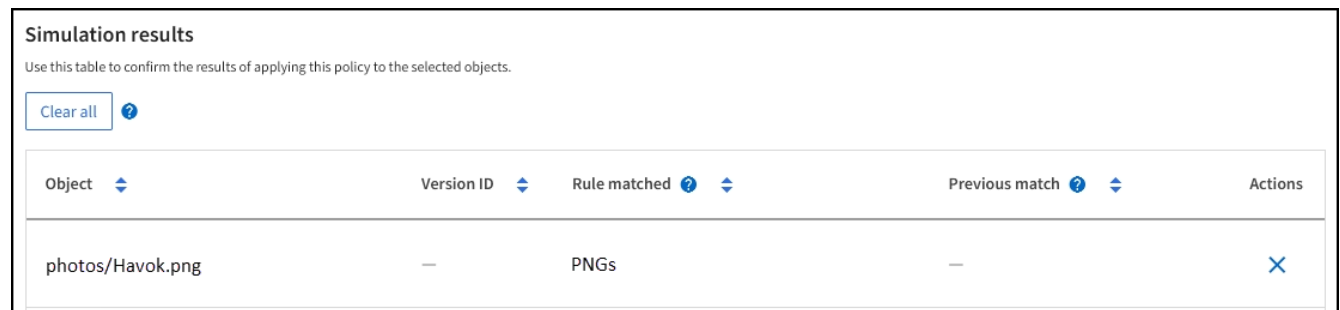
Neste exemplo, a política **Demo** está sendo simulada. Esta política, que se destina a encontrar objetos que tenham metadados de usuário de série X-men, inclui três regras, como segue:

- A primeira regra, **PNGs**, filtra os nomes das chaves que terminam em `.png`.
- A segunda regra, **X-meN**, aplica-se apenas a objetos para o locatário A e filtra os metadados `series=x-men` do usuário.
- A última regra, **duas cópias dois data centers**, é a regra padrão, que corresponde a quaisquer objetos que não correspondam às duas primeiras regras.

Passos

1. Depois de adicionar as regras e salvar a política, selecione **simular**.
2. No campo **Object**, insira o `bucket/object-key S3` ou o `container/object-name Swift` para um objeto de teste e selecione **Simulate**.

Os resultados da simulação aparecem, mostrando que o `Havok.png` objeto foi correspondido pela regra **PNGs**.



Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNGs	—	X

No entanto, `Havok.png` foi feito para testar a regra **X-men**.

3. Para resolver o problema, reordene as regras.
 - a. Selecione **Finish** (concluir) para fechar a janela Simulate ILM Policy (simular política ILM).
 - b. Selecione **ações > Editar** para editar a política.
 - c. Arraste a regra **X-man** para o topo da lista.
 - d. Selecione **Guardar**.
4. Selecione **simular**.

Os objetos que você testou anteriormente são reavaliados em relação à política atualizada e os novos resultados da simulação são mostrados. No exemplo, a coluna Rule Matched mostra que o `Havok.png` objeto agora corresponde à regra de metadados X-men, conforme esperado. A coluna correspondência anterior mostra que a regra PNGs correspondia ao objeto na simulação anterior.

Simulation results
Use this table to confirm the results of applying this policy to the selected objects.

Clear all ?

Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	X-men	PNGs	X



Se você permanecer na guia de política proposta, poderá simular novamente uma política depois de fazer alterações sem precisar digitar novamente os nomes dos objetos de teste.

Exemplo 3: Corrija uma regra ao simular uma política de ILM proposta

Este exemplo mostra como simular uma política, corrigir uma regra na política e continuar a simulação.

Neste exemplo, a política **Demo** está sendo simulada. Esta política destina-se a localizar objetos que tenham `series=x-men` metadados de usuário. No entanto, resultados inesperados ocorreram ao simular essa política contra o `Beast.jpg` objeto. Em vez de corresponder à regra de metadados X-men, o objeto correspondia à regra padrão, duas cópias de dois data centers.

Simulation results
Use this table to confirm the results of applying this policy to the selected objects.

Clear all ?

Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	Two copies two data centers	—	X

Quando um objeto de teste não é correspondido pela regra esperada na política, você deve examinar cada regra na política e corrigir quaisquer erros.

Passos

1. Selecione **Finish** (concluir) para fechar a caixa de diálogo Simulate policy (simular política). Na guia política proposta, selecione **Diagrama de retenção**. Em seguida, selecione **expandir tudo** ou **Exibir detalhes** para cada regra conforme necessário.
2. Revise a conta de locatário da regra, o tempo de referência e os critérios de filtragem.

Como exemplo, suponha que os metadados para a regra X-meN foram inseridos como "x-men01" em vez de "x-men."

3. Para resolver o erro, corrija a regra da seguinte forma:
 - Se a regra fizer parte da política proposta, você pode clonar a regra ou remover a regra da política e editá-la.
 - Se a regra fizer parte da política ativa, você deverá clonar a regra. Não é possível editar ou remover uma regra da política ativa.

Opção	Passos
Clone a regra	<ul style="list-style-type: none"> i. Selecione ILM > regras. ii. Selecione a regra incorreta e selecione Clone. iii. Insira um nome para a nova regra, altere as informações incorretas e selecione criar. iv. Selecione ILM > políticas > Política proposta. v. Selecione ações > Editar. vi. Selecione Selecionar regras e, em seguida, selecione continuar para aceitar a mesma regra padrão. vii. Na etapa Selecionar outras regras, marque a caixa de seleção da nova regra, desmarque a caixa de seleção da regra original e selecione Selecionar. viii. Se necessário, reordene as regras arrastando a nova regra para o local correto. ix. Selecione Guardar.
Edite a regra	<ul style="list-style-type: none"> i. Selecione ILM > políticas > Política proposta e remova a regra que deseja editar. ii. Selecione ILM > regras. iii. Selecione a regra que deseja editar e selecione Editar. Ou marque a caixa de seleção da regra e selecione ações > Editar. iv. Altere as informações incorretas para cada parte do assistente e selecione Atualizar. v. Selecione ILM > políticas > Política proposta. vi. Selecione ações > Editar. vii. Selecione Selecionar regras e, em seguida, selecione continuar para aceitar a mesma regra padrão. viii. Na caixa de diálogo Selecionar outras regras, marque a caixa de seleção para a regra corrigida, selecione Selecionar e, em seguida, selecione Salvar. ix. Arraste as linhas para as regras não padrão para determinar a ordem em que essas regras serão avaliadas.

4. Execute a simulação novamente.

Neste exemplo, a regra X-meN corrigida agora corresponde ao `Beast.jpg` objeto com base nos `series=x-men` metadados do usuário, conforme esperado.

Simulation results
Use this table to confirm the results of applying this policy to the selected objects.

Clear all ?

Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	X-men	—	X

Ative a política ILM

Depois de adicionar regras ILM a uma política ILM proposta, simule a política e confirme que ela se comporta como você espera, você está pronto para ativar a política proposta.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você ["permissões de acesso específicas"](#) tem .
- Você salvou e simulou a política de ILM proposta.



Erros em uma política ILM podem causar perda de dados irrecuperável. Analise e simule cuidadosamente a política antes de ativá-la para confirmar que funcionará como pretendido. Quando você ativa uma nova política de ILM, o StorageGRID a usa para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Antes de ativar uma nova política de ILM, revise todas as alterações no posicionamento de objetos replicados e codificados por apagamento existentes. Alterar a localização de um objeto existente pode resultar em problemas de recursos temporários quando os novos posicionamentos são avaliados e implementados.

Sobre esta tarefa

Quando você ativa uma política de ILM, o sistema distribui a nova política para todos os nós. No entanto, a nova política ativa pode não ter efeito até que todos os nós de grade estejam disponíveis para receber a nova política. Em alguns casos, o sistema espera implementar uma nova política ativa para garantir que os objetos de grade não sejam removidos acidentalmente.

- Se você fizer alterações de política que aumentem a redundância ou a durabilidade dos dados, essas alterações serão implementadas imediatamente. Por exemplo, se você ativar uma nova política que inclua uma regra de três cópias em vez de uma regra de duas cópias, essa política será implementada imediatamente porque aumenta a redundância de dados.
- Se você fizer alterações de política que possam diminuir a redundância de dados ou a durabilidade, essas alterações não serão implementadas até que todos os nós de grade estejam disponíveis. Por exemplo, se você ativar uma nova política que usa uma regra de duas cópias em vez de uma regra de três cópias, a nova política aparecerá na guia diretiva ativa, mas ela não entrará em vigor até que todos os nós estejam online e disponíveis.

Passos

1. Quando estiver pronto para ativar uma política proposta, selecione **políticas ILM > Política proposta** e, em seguida, selecione **Ativar**.

É apresentada uma mensagem de aviso, solicitando-lhe que confirme que pretende ativar a política proposta.

Um prompt aparece na mensagem de aviso se a regra padrão não reter objetos para sempre. Neste exemplo, o diagrama de retenção mostra que a regra padrão excluirá objetos após 730 dias (2 anos). Você deve digitar **730** na caixa de texto para confirmar que quaisquer objetos não correspondidos por outra regra na política serão removidos do StorageGRID após 730 dias.

Activate the proposed policy

Errors in an ILM policy can cause irreparable data loss. Review and test the policy carefully before activating.

The following rules do not store objects forever. When the last time period ends, objects will be automatically purged.

- **Rule 1 (730 days)**

The default rule in the policy does not retain objects forever. Confirm this is the behavior you want by referring to the retention diagram for the default rule:

Reference time: **Ingest time** Ingest behavior: **Balanced**

Day 0 Day 730

Day 0 - 730

2 replicated copies - Data Center 2

2 replicated copies - Data Center 1

Duration 730 days

Now, complete the following prompt:

Any objects that are not matched by another rule in this policy will be deleted after days.

Are you sure you want to activate the proposed policy?

Cancel OK

2. Selecione **OK**.

Resultado

Quando uma nova política ILM tiver sido ativada:

- A política é apresentada no separador ative policy (Política ativa). A entrada de data de início indica a data e a hora em que a política foi ativada.
- A política ativa anteriormente aparece na guia Histórico de políticas. As entradas de data de início e data de término indicam quando a política se tornou ativa e quando ela não estava mais em vigor.

Informações relacionadas

["Exemplo 6: Alterando uma política ILM"](#)

Verifique uma política ILM com pesquisa de metadados de objeto

Depois de ativar uma política ILM, você deve ingerir objetos de teste representativos no sistema StorageGRID. Em seguida, você deve fazer uma pesquisa de metadados de objeto para confirmar que as cópias estão sendo feitas conforme o pretendido e colocadas nos locais corretos.

Antes de começar

- Você tem um identificador de objeto, que pode ser um dos seguintes:
 - **UUID:** O Identificador universalmente exclusivo do objeto. Introduza o UUID em todas as maiúsculas.
 - **CBID:** O identificador exclusivo do objeto dentro do StorageGRID. Você pode obter o CBID de um objeto a partir do log de auditoria. Introduza o CBID em todas as maiúsculas.
 - **S3 bucket e chave de objeto:** Quando um objeto é ingerido através da interface S3, o aplicativo cliente usa uma combinação de bucket e chave de objeto para armazenar e identificar o objeto. Se o bucket S3 estiver versionado e você quiser procurar uma versão específica de um objeto S3 usando o bucket e a chave do objeto, você tem o **version ID**.
 - * Nome do contentor e objeto Swift*: Quando um objeto é ingerido através da interface Swift, o aplicativo cliente usa uma combinação de nome de contentor e objeto para armazenar e identificar o objeto.

Passos

1. Ingrida o objeto.
2. Selecione **ILM > Object metadata lookup**.
3. Digite o identificador do objeto no campo **Identificador**. Você pode inserir um UUID, CBID, S3 bucket/object-key ou Swift container/object-name.
4. Opcionalmente, insira um ID de versão para o objeto (apenas S3).

5. Selecione **Procurar**.

Os resultados da pesquisa de metadados de objeto aparecem. Esta página lista os seguintes tipos de informações:

- Metadados do sistema, incluindo o ID do objeto (UUID), o nome do objeto, o nome do contentor, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e hora em que o objeto foi criado pela primeira vez e a data e hora em que o objeto foi modificado pela última vez.
- Quaisquer pares de valor-chave de metadados de usuário personalizados associados ao objeto.
- Para objetos S3D, qualquer par de chave-valor de marca de objeto associado ao objeto.
- Para cópias de objetos replicadas, o local de storage atual de cada cópia.
- Para cópias de objetos com codificação de apagamento, o local de storage atual de cada fragmento.
- Para cópias de objetos em um Cloud Storage Pool, o local do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
- Para objetos segmentados e objetos de várias partes, uma lista de segmentos, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, apenas os primeiros 100 segmentos são mostrados.

- Todos os metadados de objetos no formato de armazenamento interno não processado. Esses metadados brutos incluem metadados internos do sistema que não são garantidos para persistir de liberação para liberação.

O exemplo a seguir mostra os resultados da pesquisa de metadados de objeto para um objeto de teste S3 que é armazenado como duas cópias replicadas.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x88230E7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36056",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAIRS": "2",

```

6. Confirme se o objeto está armazenado no local ou locais corretos e se é o tipo correto de cópia.



Se a opção Auditoria estiver ativada, você também poderá monitorar o log de auditoria para a mensagem regras de objeto ORLM atendidas. A mensagem de auditoria ORLM pode fornecer mais informações sobre o status do processo de avaliação ILM, mas não pode fornecer informações sobre a correção do posicionamento dos dados do objeto ou a integridade da política ILM. Você deve avaliar isso sozinho. Para obter detalhes, "[Rever registros de auditoria](#)" consulte .

Informações relacionadas

- ["USE A API REST DO S3"](#)

- ["Use a API Swift REST"](#)

Trabalhe com políticas ILM e regras ILM

À medida que seus requisitos de storage mudam, talvez seja necessário implementar uma política diferente ou modificar as regras de ILM associadas à política. Você pode visualizar métricas ILM para determinar o desempenho do sistema.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem permissões de acesso específicas.

Ver políticas ILM

Para visualizar políticas ILM ativas, propostas e históricas:

1. Selecione **ILM > políticas**.
2. Conforme necessário, selecione **Política ativa**, **Política proposta** ou **Histórico da política** para visualizar os detalhes de cada um. Em cada guia, você pode selecionar **regras de política** e **Diagrama de retenção**.

The screenshot displays the 'Active policy' tab in the ILM management interface. At the top, there are three tabs: 'Active policy' (selected), 'Proposed policy', and 'Policy history'. A notification banner states: 'You have a proposed policy. Review details on the Proposed policy tab.' Below this, the policy details are shown: 'Policy name: Policy 1', 'Reason for change: test', and 'Start date: 2022-09-28 15:04:48 MDT'. A 'Simulate' button is visible. Underneath, there are two sub-tabs: 'Policy rules' (selected) and 'Retention diagram'. The 'Policy rules' section contains a table with the following data:

Rule order ?	Rule name	Filters ?
1	Project A	Ingest time is 2022-10-01 00:00:00 MDT
Default	Project B	—

Clonar uma política histórica de ILM

Para clonar uma política histórica de ILM:

1. Selecione **ILM > políticas > Histórico da política**.
2. Remova a política proposta se houver.
3. Selecione o botão de opção para a política que deseja clonar e, em seguida, selecione **Clone historical**

policy.

4. Preencha os detalhes necessários seguindo as instruções em "[Criar política proposta de ILM](#)".



Uma política de ILM que foi configurada incorretamente pode resultar em perda de dados irrecoverável. Antes de ativar uma política ILM, revise cuidadosamente a política ILM e suas regras ILM e simule a política ILM. Confirme sempre que a política de ILM funcionará como pretendido.

Remova a política proposta de ILM

Para remover a política proposta:

1. Selecione **ILM > políticas > Política proposta**.
2. Selecione **ações > Remover**.

A política proposta e a guia política proposta são removidas.

Exibir detalhes da regra ILM

Para exibir os detalhes de uma regra ILM, incluindo o diagrama de retenção e as instruções de posicionamento da regra:

1. Selecione **ILM > regras**.
2. Selecione a regra cujos detalhes você deseja exibir. Exemplo:

2 copies 2 data centers

Compliant:	Yes	Ingest behavior:	Strict
Used in active policy:	No	Reference time:	Ingest time
Used in proposed policy:	No		
Description:	test		

[Clone](#) [Edit](#) [Remove](#)

Time period and placements

Retention diagram [Placement instructions](#)

Sort placements by **Time period** [Storage pool](#) ● Replicated copy ● Erasure-coded (EC) copy

Reference time: **Ingest time** Ingest behavior: **Strict**

Day 0 Day 365

Day 0 - forever 2 replicated copies - Data Center 1 or Data Center 2

Day 0 - 365 EC 2+1 - Data Center 2

Duration 365 days Forever

Além disso, você pode usar a página de detalhes para clonar, editar ou remover uma regra.

Clonar uma regra ILM

Não é possível editar uma regra se ela estiver sendo usada na política ILM proposta ou na política ILM ativa. Em vez disso, você pode clonar uma regra e fazer as alterações necessárias à cópia clonada. Então, se necessário, você pode remover a regra original da política proposta e substituí-la pela versão modificada. Você não pode clonar uma regra ILM se ela foi criada usando o StorageGRID versão 10,2 ou anterior.

Antes de adicionar uma regra clonada à política ILM ativa, esteja ciente de que uma alteração nas instruções de posicionamento de um objeto pode causar um aumento de carga no sistema.

Passos

1. Selecione **ILM > regras**.
2. Marque a caixa de seleção da regra que deseja clonar e selecione **Clone**. Em alternativa, selecione o nome da regra e, em seguida, selecione **Clone** na página de detalhes da regra.
3. Atualize a regra clonada seguindo as etapas de [Editar uma regra ILM](#) e "[Usando filtros avançados em regras ILM](#)".

Ao clonar uma regra ILM, você deve inserir um novo nome.

Editar uma regra ILM

Talvez seja necessário editar uma regra ILM para alterar um filtro ou uma instrução de colocação.

Não é possível editar uma regra se ela estiver sendo usada na política ILM ativa ou na política ILM proposta. Em vez disso, você pode clonar essas regras e fazer as alterações necessárias na cópia clonada. Você também não pode editar a regra fornecida pelo sistema, faça 2 cópias.



Antes de adicionar uma regra editada à política ILM ativa, esteja ciente de que uma alteração nas instruções de posicionamento de um objeto pode causar um aumento de carga no sistema.

Passos

1. Selecione **ILM > regras**.
2. Confirme se a regra que você deseja editar não é usada na política ILM ativa ou na política ILM proposta.
3. Se a regra que você deseja editar não estiver em uso, marque a caixa de seleção da regra e selecione **ações > Editar**. Em alternativa, selecione o nome da regra e, em seguida, selecione **Editar** na página de detalhes da regra.
4. Complete as páginas do assistente Editar regra ILM. Conforme necessário, siga os passos para "[Criando uma regra ILM](#)" e "[Usando filtros avançados em regras ILM](#)".

Ao editar uma regra ILM, você não pode alterar seu nome.



Se você editar uma regra que é usada em uma política histórica, o ícone aparecerá para a regra quando você exibir a política, o que indica que a regra se tornou uma regra histórica.

Remova uma regra ILM

Para manter a lista de regras atuais do ILM gerenciável, remova todas as regras do ILM que você provavelmente não usará.

Passos

Para remover uma regra ILM que está atualmente usada na política ativa ou na política proposta:


1. Clonar a política ativa ou editar a política proposta.
2. Remova a regra ILM da política.
3. Salve, simule e ative a nova política para garantir que os objetos estejam protegidos conforme esperado.

Para remover uma regra ILM que não é usada atualmente:

1. Selecione **ILM > regras**.
2. Confirme se a regra que você deseja remover não é usada na política ativa ou na política proposta.
3. Se a regra que você deseja remover não estiver em uso, selecione a regra e selecione **Remover**. Você pode selecionar várias regras e remover todas elas ao mesmo tempo.
4. Selecione **Sim** para confirmar que deseja remover a regra ILM.

A regra ILM é removida.



Se você remover uma regra usada em uma política histórica, o  ícone aparecerá para a regra quando você exibir a política, o que indica que a regra se tornou uma regra histórica.

Ver métricas ILM

Você pode exibir métricas para ILM, como o número de objetos na fila e a taxa de avaliação. Você pode monitorar essas métricas para determinar o desempenho do sistema. Uma fila grande ou taxa de avaliação pode indicar que o sistema não é capaz de acompanhar a taxa de ingestão, a carga dos aplicativos cliente é excessiva ou que existe alguma condição anormal.


Passos

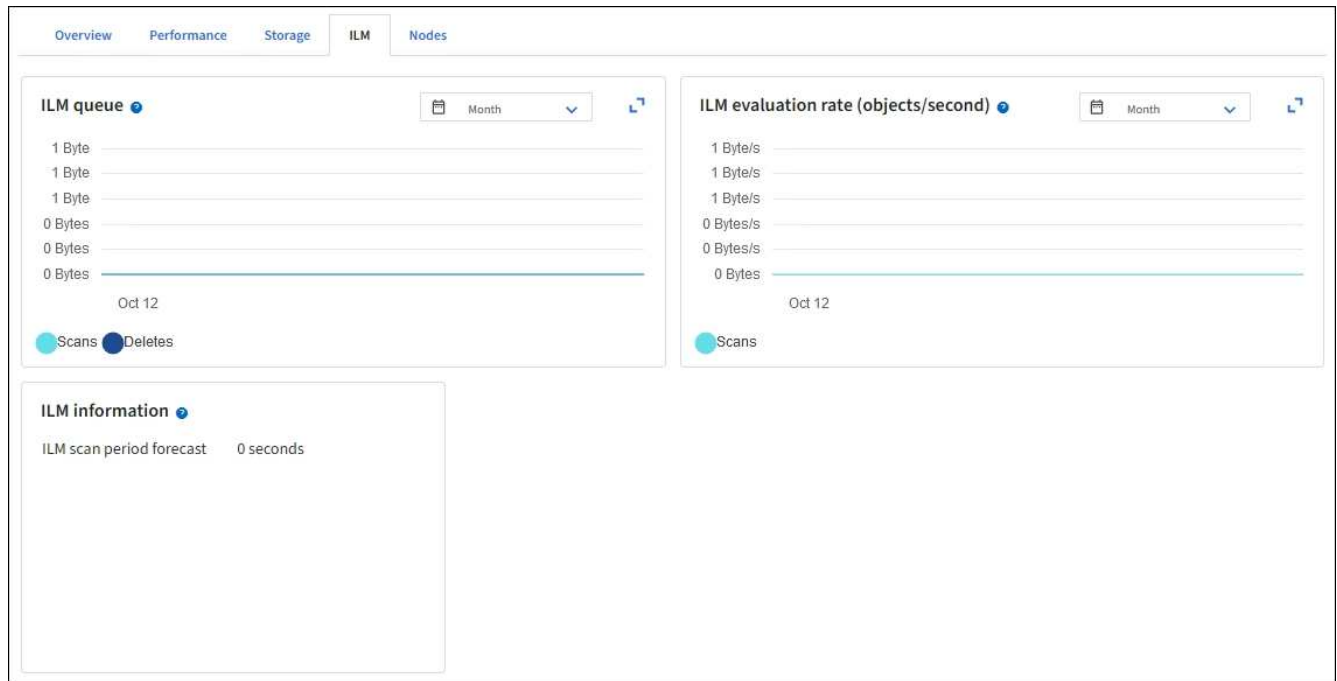
1. Selecione **Dashboard > ILM**.



Como o painel pode ser personalizado, a guia ILM pode não estar disponível.

2. Monitore as métricas na guia ILM.

Você pode selecionar o ponto de interrogação  para ver uma descrição dos itens na guia ILM.



Use o bloqueio de objetos S3D.

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?

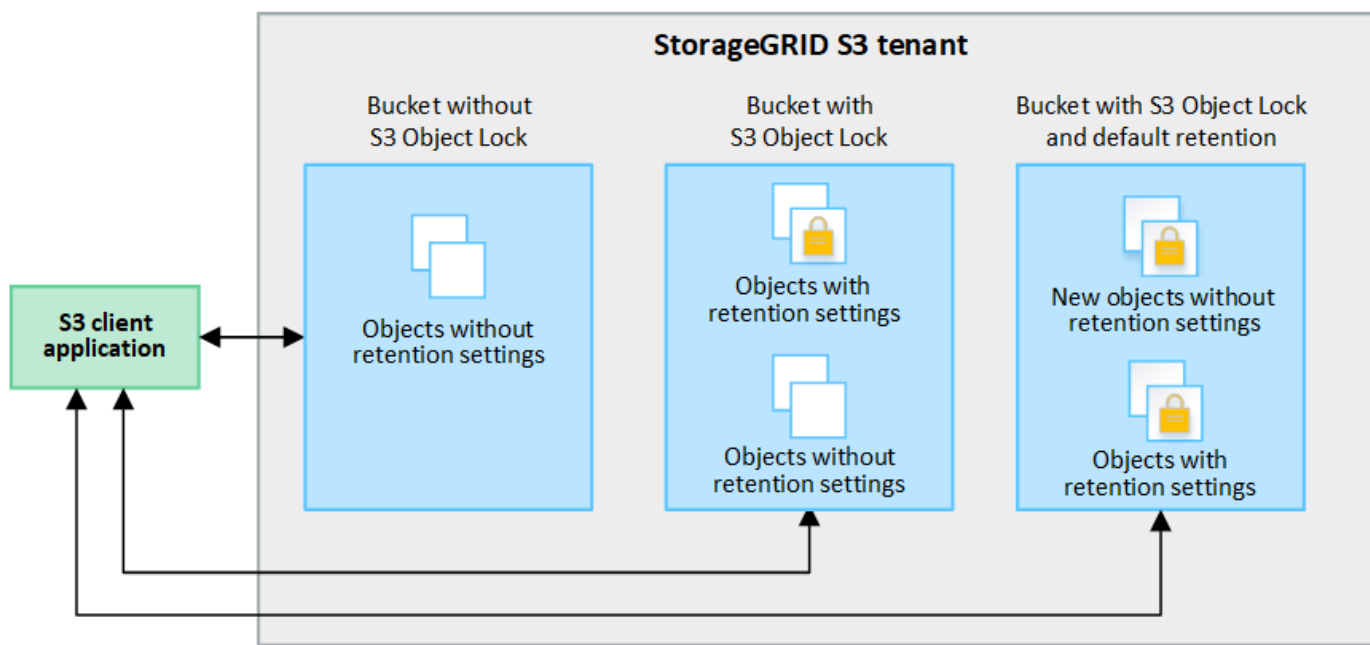
O recurso bloqueio de objetos do StorageGRID S3 é uma solução de proteção de objetos equivalente ao bloqueio de objetos do S3 no Amazon Simple Storage Service (Amazon S3).

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 objetos S3 ativado, o controle de versão do bucket é necessário e é ativado automaticamente.

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 salva nesse bucket.

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

StorageGRID with S3 Object Lock setting enabled



Modos de retenção

O recurso bloqueio de objetos do StorageGRID S3 suporta 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 alcançada.
 - O retent-until-date do objeto pode ser aumentado, mas não pode ser diminuído.
 - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- No modo de governança:
 - Os usuários com permissão especial podem usar um cabeçalho de desvio em solicitações para modificar determinadas configurações de retenção.
 - Esses usuários podem excluir uma versão de objeto antes de sua data de retenção ser alcançada.
 - Esses usuários podem aumentar, diminuir ou remover a data de retenção até um objeto.

Configurações de retenção para versões de objetos

Se um bucket for criado com o bloqueio de objeto S3 ativado, 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.
- **Retent-until-date:** Se a data de retent-until de uma versão de objeto estiver no futuro, o objeto pode ser recuperado, mas não pode ser excluído.
- **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.



Se um objeto estiver sob uma retenção legal, ninguém poderá excluir o objeto, independentemente de seu modo de retenção.

Para obter detalhes sobre as configurações do objeto, ["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#) consulte .

Configuração de retenção padrão para buckets

Se um bucket for criado com o bloqueio de objetos S3 ativado, os usuários podem especificar opcionalmente as seguintes configurações padrão para o bucket:

- **Modo de retenção padrão:** Conformidade ou governança.
- **Período de retenção padrão:** Quanto tempo as novas versões de objetos adicionadas a este intervalo devem ser mantidas, a partir do dia em que são adicionadas.

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

["Crie um bucket do S3"](#) Consulte e ["Atualização S3 retenção padrão bloqueio Objeto"](#).

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"".



A configuração de conformidade global está obsoleta. Se você ativou essa configuração usando uma versão anterior do StorageGRID, a configuração bloqueio de objeto S3 será ativada automaticamente. Você pode continuar usando o StorageGRID para gerenciar as configurações de buckets em conformidade existentes; no entanto, não é possível criar novos buckets em conformidade. Para obter detalhes, ["Base de Conhecimento da NetApp: Como gerenciar buckets em conformidade com o legado no StorageGRID 11,5"](#) consulte .

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.

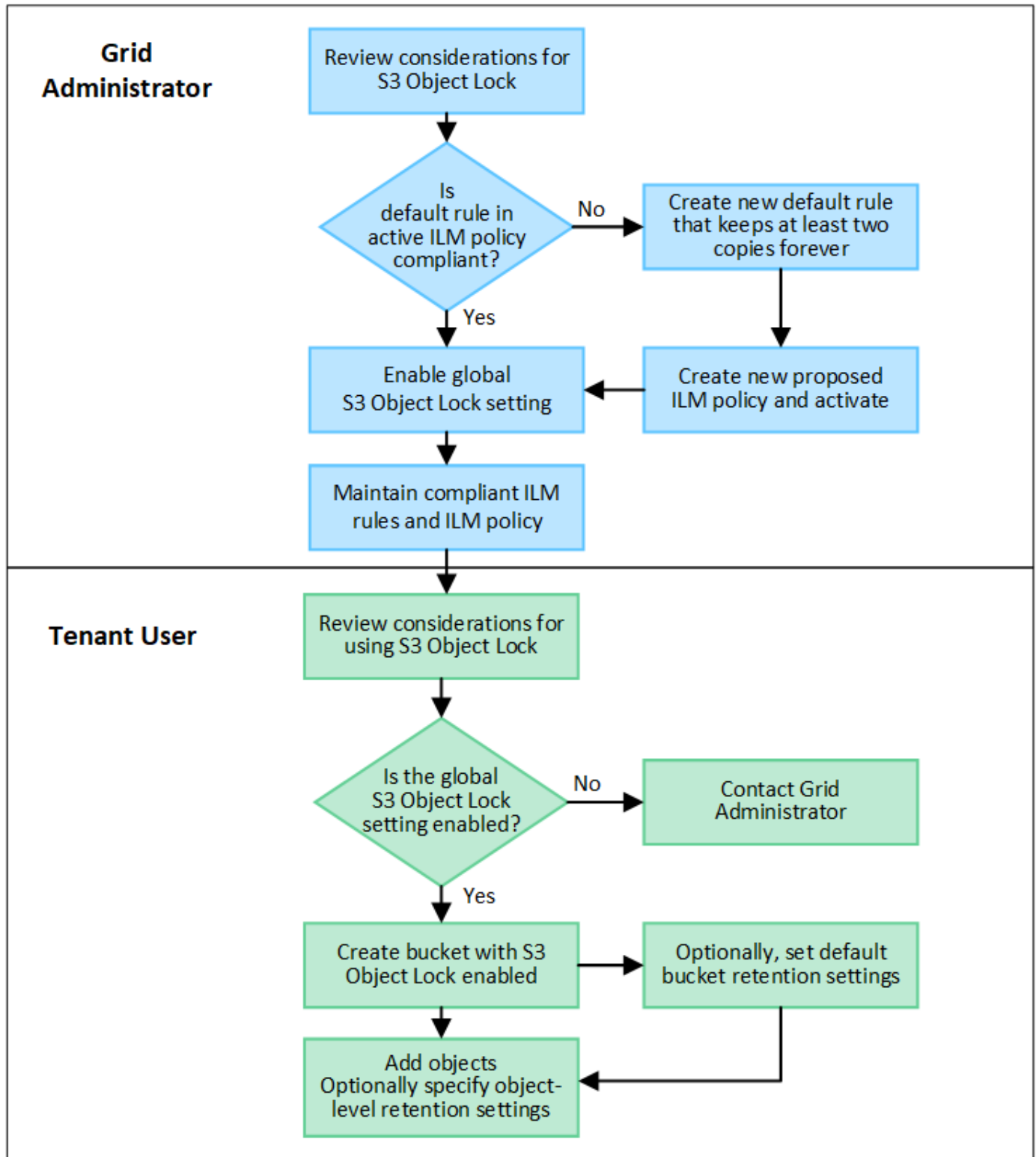
	S3 bloqueio de objetos	Conformidade (legado)
Como o recurso é ativado globalmente?	No Gerenciador de Grade, selecione CONFIGURATION > System > S3 Object Lock .	Já não é suportado.
Como o recurso está habilitado para um bucket?	Os usuários devem habilitar o bloqueio de objeto S3 ao criar um novo bucket usando o Gerenciador de locatário, a API de gerenciamento de locatário ou a API REST S3.	Já não é suportado.

	S3 bloqueio de objetos	Conformidade (legado)
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
Como a retenção de objetos é definida?	Os usuários podem definir uma data de retenção até cada versão do objeto ou 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 aplica-se a todos os objetos no balde.
O período de retenção pode ser alterado?	<ul style="list-style-type: none"> No modo de conformidade, a data de retenção até uma versão de objeto pode ser aumentada, mas nunca diminuída. No modo de governança, os usuários com permissões especiais podem diminuir ou até mesmo remover as configurações de retenção de um objeto. 	O período de retenção de um balde pode ser aumentado, mas nunca diminuído.
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?	<ul style="list-style-type: none"> No modo de conformidade, uma versão de objeto pode ser excluída após a data de retenção ser alcançada, assumindo que o objeto não está sob retenção legal. No modo de governança, os usuários com permissões especiais podem excluir um objeto antes de sua data de retenção ser alcançada, supondo que o objeto não esteja 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. Opcionalmente, especifique as configurações de retenção padrão para o bucket. Todas as configurações padrão de bucket são aplicadas apenas a novos objetos que não têm suas próprias configurações de retenção.
3. Adicione objetos a esses buckets e, opcionalmente, especifique períodos de retenção no nível do objeto e configurações de retenção legal.
4. Conforme necessário, atualize a retenção padrão para o bucket ou atualize o período de retenção ou a configuração de retenção legal para um objeto individual.

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 de regras ILM e políticas ILM indicam quais regras ILM são compatíveis.

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 objetos não podem ser salvas em um pool de armazenamento em nuvem.
- As cópias de objetos 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".

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.
- 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 S3 para um bucket existente.
- Quando o bloqueio de objeto S3 está ativado para um bucket, o StorageGRID ativa automaticamente o controle de versão desse bucket. Não é possível desativar o bloqueio de objetos S3 ou suspender o controle de versão para o bucket.
- Opcionalmente, você pode especificar um modo de retenção padrão e um período de retenção para cada bucket usando o Gerenciador de locatários, a API de gerenciamento do locatário ou a API REST do S3. 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 manter-até-data para cada versão do objeto quando ele é carregado.
- A configuração do ciclo de vida do bucket é compatível com buckets com o S3 Object Lock ativado.

- 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, 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 S3.
- 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 estes estágios:

1. * Ingestão de objetos*

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

- Se as configurações de retenção forem especificadas para o objeto, as configurações de nível do objeto serão aplicadas. Todas as configurações padrão do bucket são ignoradas.
- Se não forem especificadas configurações de retenção para o objeto, as configurações padrão de bucket serão aplicadas, se existirem.
- Se nenhuma configuração de retenção for especificada para o objeto ou o bucket, o objeto não será protegido pelo bloqueio de objeto S3.

Se as configurações de retenção forem aplicadas, o objeto e 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 durante o período de retenção especificado. O número exato e o tipo de cópias de objetos e os locais de storage são determinados pelas regras em conformidade na política de ILM ativa. Se um objeto protegido pode ser excluído antes de sua data de retenção ser alcançada depende de seu modo de retenção.

- Se um objeto estiver sob uma retenção legal, ninguém poderá excluir o objeto, independentemente de seu modo de retenção.

Informações relacionadas

- ["Crie um bucket do S3"](#)
- ["Atualização S3 retenção padrão bloqueio Objeto"](#)
- ["Use a API REST do S3 para configurar o bloqueio de objetos do S3"](#)
- ["Exemplo 7: Política de ILM compatível para 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.

Antes de começar

- Você tem a permissão de acesso root.
- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- 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. ["Crie uma regra ILM padrão"](#) Consulte para obter detalhes.

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 pode ser desativada.



A configuração de conformidade global está obsoleta. Se você ativou essa configuração usando uma versão anterior do StorageGRID, a configuração bloqueio de objeto S3 será ativada automaticamente. Você pode continuar usando o StorageGRID para gerenciar as configurações de buckets em conformidade existentes; no entanto, não é possível criar novos buckets em conformidade. Para obter detalhes, ["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.

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. Você deve criar e ativar uma nova política ILM que inclua uma regra compatível como regra padrão. Selecione **OK**. Em seguida, crie uma nova política proposta, simule-a e ative-a. ["Criar política ILM"](#) Consulte para obter instruções.

Depois de terminar

Depois de ativar a configuração global S3 Object Lock, talvez você queira ["Crie uma nova política ILM"](#). 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.

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 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 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 A API REST DO S3"](#)
- ["Recuperar e manter"](#)

Exemplo de regras e políticas ILM

Exemplo 1: Regras e política de ILM para armazenamento de objetos

Você pode usar as seguintes regras e políticas de exemplo como ponto de partida ao definir uma política de ILM para atender aos requisitos de proteção e retenção de objetos.



As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule a política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Regra ILM 1 por exemplo 1: Copiar dados de objeto para dois sites

Este exemplo de regra de ILM copia dados de objeto para pools de storage em dois locais.

Definição de regra	Exemplo de valor
Pools de armazenamento em um local	Dois pools de armazenamento, cada um contendo sites diferentes, denominados Site 1 e Site 2.
Nome da regra	Duas cópias de dois locais
Tempo de referência	Tempo de ingestão
Colocações	No dia 0 para sempre, mantenha uma cópia replicada no local 1 e uma cópia replicada no local 2.

A seção análise de regras do diagrama de retenção afirma:

- A proteção contra perda de site da StorageGRID será aplicada durante a duração desta regra.
- Os objetos processados por esta regra não serão excluídos pelo ILM.

Reference time [?](#)

Ingest time ▼

Time period and placements ↕ Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1 From Day 0 ⬇ store forever ▼ ✕

Store objects by replicating ▼ 1 ⬇ copies at Site 1 ✕ ✎ ✕

and store objects by replicating ▼ 1 ⬇ copies at Site 2 ✕ ✎ ✕

[Add other type or location](#)

[Add another time period](#)

Retention diagram ● Replicated copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

1 replicated copy - Site 1

1 replicated copy - Site 2

Duration Forever

Regra ILM 2 por exemplo 1: Perfil de codificação de apagamento com correspondência de intervalo

Este exemplo de regra ILM usa um perfil de codificação de apagamento e um bucket do S3 para determinar onde e quanto tempo o objeto é armazenado.

Definição de regra	Exemplo de valor
Pool de armazenamento com vários locais	<ul style="list-style-type: none"> • Um pool de armazenamento em três locais (locais 1, 2, 3) • Use o esquema de codificação de apagamento 6-3
Nome da regra	S3 Bucket finance-Records
Tempo de referência	Tempo de ingestão
Colocações	Para objetos no bucket do S3 chamado finance-Records, crie uma cópia codificada por apagamento no pool especificado pelo perfil de codificação de apagamento. Guarde esta cópia para sempre.

Time period and placements Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1 From Day 0 store forever

Store objects by erasure coding using 6+3 EC scheme at Sites 1, 2, 3

[Add other type or location](#)

[Add another time period](#)

Retention diagram ● Erasure-coded (EC) copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Política de ILM, por exemplo, 1

Na prática, a maioria das políticas de ILM são simples, mesmo que o sistema StorageGRID permita que você projete políticas de ILM sofisticadas e complexas.

Uma política ILM típica para uma grade de vários sites pode incluir regras ILM, como as seguintes:

- Na ingestão, armazene todos os objetos pertencentes ao bucket S3 nomeado `finance-records` em um pool de armazenamento que contém três locais. Use a codificação de apagamento 6-3.
- Se um objeto não corresponder à primeira regra ILM, use a regra ILM padrão da política, duas cópias de dois Data Centers, para armazenar uma cópia desse objeto no Site 1 e uma cópia no Site 2.

Informações relacionadas

- ["Criar uma política ILM: Visão geral"](#)

- "Crie uma política de ILM proposta"

Exemplo 2: Regras de ILM e política para filtragem de tamanho de objeto EC

Você pode usar as seguintes regras e políticas de exemplo como pontos de partida para definir uma política de ILM que filtra por tamanho do objeto para atender aos requisitos de EC recomendados.



As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule a política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Regra ILM 1 por exemplo 2: Use EC para objetos maiores que 1 MB

Este exemplo ILM regra de apagamento codifica objetos que são maiores que 1 MB.



A codificação de apagamento é mais adequada para objetos com mais de 1 MB. Não use a codificação de apagamento para objetos com menos de 200 KB para evitar a sobrecarga de gerenciamento de fragmentos codificados de apagamento muito pequenos.

Definição de regra	Exemplo de valor
Nome da regra	Objetos somente EC > 1 MB
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Tamanho do objeto superior a 1 MB
Colocações	Crie uma cópia codificada por apagamento 2-1 usando três sites

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size
▼

greater than
▼

1
↕

MB
▼
✕

Regra ILM 2 por exemplo 2: Duas cópias replicadas

Este exemplo de regra ILM cria duas cópias replicadas e não filtra pelo tamanho do objeto. Esta regra é a regra padrão da política. Como a primeira regra filtra todos os objetos com mais de 1 MB, essa regra só se aplica a objetos com 1 MB ou menos.

Definição de regra	Exemplo de valor
Nome da regra	Duas cópias replicadas
Tempo de referência	Tempo de ingestão

Definição de regra	Exemplo de valor
Filtro avançado para tamanho do objeto	Nenhum
Colocações	No dia 0 para sempre, mantenha uma cópia replicada no local 1 e uma cópia replicada no local 2.

Política ILM por exemplo 2: Use EC para objetos maiores que 1 MB

Este exemplo de política ILM inclui duas regras ILM:

- A primeira regra de apagamento codifica todos os objetos com mais de 1 MB.
- A segunda regra ILM (padrão) cria duas cópias replicadas. Como objetos com mais de 1 MB foram filtrados pela regra 1, a regra 2 aplica-se apenas a objetos com 1 MB ou menos.

Exemplo 3: Regras e política de ILM para melhor proteção para arquivos de imagem

Você pode usar as regras e a política de exemplo a seguir para garantir que imagens maiores que 1 MB sejam codificadas para apagamento e que duas cópias sejam feitas de imagens menores.



As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule a política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Regra ILM 1 por exemplo 3: Use EC para arquivos de imagem maiores que 1 MB

Este exemplo de regra ILM usa filtragem avançada para codificar todos os arquivos de imagem com mais de 1 MB.



A codificação de apagamento é mais adequada para objetos com mais de 1 MB. Não use a codificação de apagamento para objetos com menos de 200 KB para evitar a sobrecarga de gerenciamento de fragmentos codificados de apagamento muito pequenos.

Definição de regra	Exemplo de valor
Nome da regra	Ficheiros de imagem EC > 1 MB
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Tamanho do objeto superior a 1 MB
Filtros avançados para Key	<ul style="list-style-type: none"> • Termina com .jpg • Termina com .png

Definição de regra	Exemplo de valor
Colocações	Crie uma cópia codificada por apagamento 2-1 usando três sites

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼ greater than ▼ 1 ⌵ MB ▼ ✕

and Key ▼ ends with ▼ .jpg ✕

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼ greater than ▼ 1 ⌵ MB ▼ ✕

and Key ▼ ends with ▼ .png ✕

Como essa regra é configurada como a primeira regra na política, a instrução de colocação de codificação de apagamento só se aplica a arquivos .jpg e .png maiores que 1 MB.

Regra ILM 2 por exemplo 3: Crie 2 cópias replicadas para todos os arquivos de imagem restantes

Este exemplo de regra ILM usa filtragem avançada para especificar que arquivos de imagem menores sejam replicados. Como a primeira regra na política já corresponde a arquivos de imagem maiores que 1 MB, essa regra se aplica a arquivos de imagem com 1 MB ou menores.

Definição de regra	Exemplo de valor
Nome da regra	2 cópias para ficheiros de imagem
Tempo de referência	Tempo de ingestão
Filtros avançados para Key	<ul style="list-style-type: none"> • Termina com .jpg • Termina com .png
Colocações	Criar 2 cópias replicadas em dois pools de storage

Política ILM, por exemplo, 3: Melhor proteção para arquivos de imagem

Este exemplo de política ILM inclui três regras:

- A primeira regra de apagamento codifica todos os arquivos de imagem com mais de 1 MB.
- A segunda regra cria duas cópias de quaisquer arquivos de imagem restantes (ou seja, imagens com 1 MB ou menos).
- A regra padrão se aplica a todos os objetos restantes (ou seja, quaisquer arquivos que não sejam de imagem).

Exemplo 4: Regras ILM e política para objetos com versão S3

Se você tiver um bucket do S3 com controle de versão habilitado, poderá gerenciar as versões de objetos não atuais, incluindo regras em sua política de ILM que usam ""tempo não atual"" como o tempo de referência.



Se você especificar um tempo de retenção limitado para objetos, esses objetos serão excluídos permanentemente após o período de tempo ser atingido. Certifique-se de entender quanto tempo os objetos serão retidos.

Como este exemplo mostra, você pode controlar a quantidade de armazenamento usada por objetos com controle de versão usando instruções de posicionamento diferentes para versões de objetos não atuais.



As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule a política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.



Para executar a simulação de política ILM em uma versão não atual de um objeto, você deve conhecer o UUID ou CBID da versão do objeto. Para localizar UUID e CBID, use "[pesquisa de metadados de objetos](#)" enquanto o objeto ainda estiver atual.

Informações relacionadas

- "[Como os objetos são excluídos](#)"

Regra ILM 1 por exemplo 4: Salve três cópias por 10 anos

Este exemplo de regra ILM armazena uma cópia de cada objeto em três locais por 10 anos.

Esta regra se aplica a todos os objetos, quer eles sejam ou não versionados.

Definição de regra	Exemplo de valor
Pools de armazenamento	Três pools de armazenamento, cada um composto por diferentes data centers, denominados Site 1, Site 2 e Site 3.
Nome da regra	Três cópias dez anos
Tempo de referência	Tempo de ingestão
Colocações	No dia 0, mantenha três cópias replicadas por 10 anos (3.652 dias), uma no local 1, uma no local 2 e uma no local 3. No final de 10 anos, exclua todas as cópias do objeto.

Regra ILM 2 por exemplo 4: Salve duas cópias de versões não atuais por 2 anos

Este exemplo de regra ILM armazena duas cópias das versões não atuais de um objeto com versão S3 por 2 anos.

Como a regra ILM 1 se aplica a todas as versões do objeto, você deve criar outra regra para filtrar quaisquer versões não atuais.

Para criar uma regra que use ""hora não atual"" como tempo de referência, selecione **Sim** para a pergunta, ""aplicar esta regra apenas a versões de objetos mais antigas (em buckets do S3 com controle de versão ativado)?" na Etapa 1 (Inserir detalhes) do assistente criar uma regra ILM. Quando você seleciona **Yes**, *Noncurrent Time* é selecionado automaticamente para a hora de referência e você não pode selecionar uma hora de referência diferente.

The screenshot shows the 'Enter details' step of the AWS IAM console. At the top, there are three steps: 1. Enter details (active), 2. Define placements, and 3. Select ingest behavior. The form contains the following fields:

- Rule name:** Older Object Versions: Two Copies Two Years
- Description (optional):** Older versions only
- Basic filters (optional):** Specify which tenant accounts and buckets this rule applies to.
- Tenant accounts:** Select tenant accounts
- Bucket name:** matches all
- Apply this rule to older object versions only (in S3 buckets with versioning enabled)?** Yes (selected)

Neste exemplo, apenas duas cópias das versões não atuais são armazenadas e essas cópias serão armazenadas por dois anos.

Definição de regra	Exemplo de valor
Pools de armazenamento	Dois pools de armazenamento, cada um em diferentes data centers, o Site 1 e o Site 2.
Nome da regra	Versões não atuais: Duas cópias dois anos
Tempo de referência	Hora não atual Selecionada automaticamente quando você seleciona Sim para a pergunta, ""aplicar esta regra apenas a versões de objetos mais antigas (em buckets do S3 com controle de versão habilitado)?" no assistente criar uma regra ILM.

Definição de regra	Exemplo de valor
Colocações	No dia 0 em relação ao tempo não atual (ou seja, a partir do dia em que a versão do objeto se torna a versão não atual), mantenha duas cópias replicadas das versões de objetos não atuais por 2 anos (730 dias), uma no local 1 e outra no local 2. No final de 2 anos, exclua as versões não atuais.

Política ILM por exemplo 4: S3 objetos versionados

Se você quiser gerenciar versões mais antigas de um objeto de forma diferente da versão atual, as regras que usam ""hora não atual"" como o tempo de referência devem aparecer na política ILM antes das regras que se aplicam à versão atual do objeto.

Uma política ILM para objetos com versão S3 pode incluir regras ILM, como as seguintes:

- Mantenha quaisquer versões mais antigas (não atuais) de cada objeto por 2 anos, a partir do dia em que a versão se tornou não atual.



As regras de "hora não atual" devem aparecer na política antes das regras que se aplicam à versão atual do objeto. Caso contrário, as versões de objetos não atuais nunca serão correspondidas pela regra "tempo não atual".

- Na ingestão, crie três cópias replicadas e armazene uma cópia em cada um dos três locais. Mantenha cópias da versão atual do objeto por 10 anos.

Ao simular a política de exemplo, você espera que os objetos de teste sejam avaliados da seguinte forma:

- Qualquer versão de objeto não atual seria correspondida pela primeira regra. Se uma versão de objeto não atual tiver mais de 2 anos, ela será excluída permanentemente pelo ILM (todas as cópias da versão não atual removidas da grade).



Para simular versões de objetos não atuais, você deve usar o UUID ou CBID dessa versão. Enquanto o objeto ainda está atual, você pode usar "[pesquisa de metadados de objetos](#)" para encontrar seu UUID e CBID.

- A versão atual do objeto seria correspondida pela segunda regra. Quando a versão atual do objeto é armazenada por 10 anos, o processo ILM adiciona um marcador de exclusão como a versão atual do objeto, e torna a versão anterior do objeto "não atual". Na próxima vez que a avaliação do ILM ocorrer, essa versão não atual é correspondida pela primeira regra. Como resultado, a cópia no local 3 é purgada e as duas cópias no local 1 e no local 2 são armazenadas por mais 2 anos.

Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa

Você pode usar um filtro de local e o comportamento estrito de ingestão em uma regra para evitar que objetos sejam salvos em um local específico do data center.

Neste exemplo, um inquilino com sede em Paris não quer armazenar alguns objetos fora da UE devido a preocupações regulatórias. Outros objetos, incluindo todos os objetos de outras contas de inquilino, podem ser armazenados no data center de Paris ou no data center dos EUA.



As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule a política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Informações relacionadas

- ["Opções de ingestão"](#)
- ["Criar regra ILM: Selecione comportamento de ingestão"](#)

Regra 1 do ILM, por exemplo, 5: Ingestão rigorosa para garantir o data center de Paris

Este exemplo de regra de ILM usa o comportamento de ingestão rigoroso para garantir que os objetos salvos por um locatário baseado em Paris em buckets do S3 com a região definida como região eu-oeste-3 (Paris) nunca sejam armazenados no data center dos EUA.

Esta regra se aplica a objetos que pertencem ao inquilino de Paris e que têm a região de bucket S3 definida como eu-West-3 (Paris).

Definição de regra	Exemplo de valor
Conta de locatário	Inquilino de Paris
Filtro avançado	A restrição de localização é igual à eu-West-3
Pools de armazenamento	Local 1 (Paris)
Nome da regra	Ingestão rigorosa para garantir o data center de Paris
Tempo de referência	Tempo de ingestão
Colocações	No dia 0, mantenha duas cópias replicadas para sempre no Site 1 (Paris)
Comportamento de ingestão	Rigoroso. Sempre use os posicionamentos desta regra na ingestão. A ingestão falha se não for possível armazenar duas cópias do objeto no data center de Paris.

Strict ingest to guarantee Paris data center

Compliant: Yes
Used in active policy: No
Used in proposed policy: No

Ingest behavior: Strict
Reference time: Ingest time

Clone Edit Remove

Filters

This rule applies if:

- Tenant is Paris tenant

And it only applies if objects have this metadata:

- Location constraint is eu-west-3

Time period and placements

Retention diagram Placement instructions

Sort placements by Time period Storage pool

● Replicated copy

Rule analysis:

- StorageGRID site-loss protection will not apply from Day 0 - Forever:
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Site 1

Duration

Forever

Regra ILM 2 por exemplo 5: Ingestão equilibrada para outros objetos

Este exemplo de regra de ILM usa o comportamento de ingestão equilibrada para fornecer eficiência ideal de ILM para quaisquer objetos não correspondidos pela primeira regra. Duas cópias de todos os objetos correspondentes a essa regra serão armazenadas: Uma no data center dos EUA e outra no data center de Paris. Se a regra não puder ser satisfeita imediatamente, as cópias provisórias serão armazenadas em qualquer local disponível.

Esta regra se aplica a objetos que pertencem a qualquer locatário e a qualquer região.

Definição de regra	Exemplo de valor
Conta de locatário	Ignorar
Filtro avançado	<i>Não especificado</i>
Pools de armazenamento	Local 1 (Paris) e local 2 (EUA)
Nome da regra	2 cópias 2 Data Centers
Tempo de referência	Tempo de ingestão

Definição de regra	Exemplo de valor
Colocações	No dia 0, mantenha duas cópias replicadas para sempre em dois data centers
Comportamento de ingestão	Equilibrado. Os objetos que correspondem a essa regra são colocados de acordo com as instruções de colocação da regra, se possível. Caso contrário, cópias provisórias são feitas em qualquer local disponível.

Política de ILM, por exemplo, 5: Combinando comportamentos de ingestão

O exemplo de política ILM inclui duas regras que têm comportamentos de ingestão diferentes.

Uma política de ILM que usa dois comportamentos de ingestão diferentes pode incluir regras de ILM, como as seguintes:

- Armazene objetos que pertencem ao inquilino de Paris e que tenham a região de bucket S3 definida como eu-West-3 (Paris) apenas no data center de Paris. Falha na ingestão se o data center Paris não estiver disponível.
- Armazene todos os outros objetos (incluindo aqueles que pertencem ao locatário de Paris, mas que têm uma região de intervalo diferente) no data center dos EUA e no data center de Paris. Faça cópias provisórias em qualquer local disponível se a instrução de colocação não puder ser satisfeita.

Ao simular a política de exemplo, você espera que os objetos de teste sejam avaliados da seguinte forma:

- Quaisquer objetos que pertençam ao inquilino de Paris e que tenham a região de bucket S3 definida como eu-West-3 são correspondidos pela primeira regra e são armazenados no data center de Paris. Como a primeira regra usa ingestão rigorosa, esses objetos nunca são armazenados no data center dos EUA. Se os nós de storage no data center de Paris não estiverem disponíveis, a ingestão falhará.
- Todos os outros objetos são correspondidos pela segunda regra, incluindo objetos que pertencem ao inquilino de Paris e que não têm a região de bucket S3 definida como eu-West-3. Uma cópia de cada objeto é salva em cada data center. No entanto, como a segunda regra usa ingestão equilibrada, se um data center não estiver disponível, duas cópias provisórias serão salvas em qualquer local disponível.

Exemplo 6: Alterar uma política ILM

Se sua proteção de dados precisar ser alterada ou você adicionar novos sites, você poderá criar e ativar uma nova política de ILM.

Antes de alterar uma política, você deve entender como as alterações nos posicionamentos de ILM podem afetar temporariamente o desempenho geral de um sistema StorageGRID.

Neste exemplo, um novo site StorageGRID foi adicionado em uma expansão e uma nova política ILM ativa precisa ser implementada para armazenar dados no novo site. Para implementar uma nova política ativa, primeiro crie uma política proposta por qualquer um ["clonar uma política existente ou a partir do zero"](#) dos . Depois disso, você deve ["simular"](#) e, em seguida ["ativar"](#), a nova política.



As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule a política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Como alterar uma política ILM afeta o desempenho

Quando você ativa uma nova política de ILM, o desempenho do seu sistema StorageGRID pode ser temporariamente afetado, especialmente se as instruções de colocação na nova política exigirem que muitos objetos existentes sejam movidos para novos locais.

Quando você ativa uma nova política de ILM, o StorageGRID a usa para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Antes de ativar uma nova política de ILM, revise todas as alterações no posicionamento de objetos replicados e codificados por apagamento existentes. Alterar a localização de um objeto existente pode resultar em problemas de recursos temporários quando os novos posicionamentos são avaliados e implementados.

Para garantir que uma nova política de ILM não afete o posicionamento de objetos replicados e codificados por apagamento existentes, é possível "[Crie uma regra ILM com um filtro de tempo de ingestão](#)". Por exemplo, **o tempo de ingestão está ativado ou depois de** __, de modo que a nova regra se aplique apenas a objetos ingeridos na ou após a data e hora especificadas.

Os tipos de alterações de política ILM que podem afetar temporariamente o desempenho do StorageGRID incluem o seguinte:

- Aplicar um perfil de codificação de apagamento diferente a objetos codificados por apagamento existentes.



O StorageGRID considera que cada perfil de codificação de apagamento é exclusivo e não reutiliza fragmentos de codificação de apagamento quando um novo perfil é usado.

- Alterar o tipo de cópias necessárias para objetos existentes; por exemplo, converter uma grande porcentagem de objetos replicados em objetos codificados por apagamento.
- Mover cópias de objetos existentes para um local completamente diferente; por exemplo, mover um grande número de objetos de ou para um pool de armazenamento em nuvem ou de ou para um local remoto.

Política ILM ativa, por exemplo, 6: Proteção de dados em dois locais

Neste exemplo, a política ILM ativa foi inicialmente projetada para um sistema StorageGRID de dois locais e usa duas regras ILM.

Active policy
Policy history

Policy name: Data Protection for Two Sites (2 rules)
Reason for change: Data protection for two sites (using 2 rules)
Start date: 2022-10-11 10:37:11 MDT

Simulate

Policy rules
Retention diagram

Rule order ?	Rule name	Filters ?
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

Nesta política de ILM, os objetos pertencentes ao Tenant A são protegidos pela codificação de apagamento 2-1 em um único local, enquanto os objetos pertencentes a todos os outros locatários são protegidos em dois sites que usam replicação de cópia 2.



A primeira regra neste exemplo usa um filtro avançado para garantir que a codificação de apagamento não seja usada para objetos pequenos. Qualquer um dos objetos do Tenant A menores que 1 MB será protegido pela regra padrão, que usa replicação.

Regra 1: Codificação de apagamento de um local para o Locatário A.

Definição de regra	Exemplo de valor
Nome da regra	Codificação de apagamento de um local para o Locatário A.
Conta de locatário	Inquilino A
Pool de storage	Local 1
Colocações	Codificação de apagamento 2-1 no local 1 do dia 0 para sempre

Regra 2: Replicação de dois locais para outros locatários

Definição de regra	Exemplo de valor
Nome da regra	Replicação de dois locais para outros locatários
Conta de locatário	Ignorar
Pools de armazenamento	Site 1 e Site 2

Definição de regra	Exemplo de valor
Colocações	Duas cópias replicadas do dia 0 para sempre: Uma cópia no local 1 e uma cópia no local 2.

Proposta de política de ILM, por exemplo, 6: Proteção de dados em três locais

Neste exemplo, a política ILM está sendo substituída por uma nova política para um sistema StorageGRID de três locais.

Depois de executar uma expansão para adicionar o novo local, o administrador da grade criou dois novos pools de storage: Um pool de storage para o local 3 e um pool de storage contendo todos os três locais (não o mesmo que o pool de storage padrão todos os nós de storage). Em seguida, o administrador criou duas novas regras ILM e uma nova política ILM proposta, que é projetada para proteger dados em todos os três locais.

Quando esta nova política ILM é ativada, os objetos pertencentes ao Locatário A serão protegidos pela codificação de apagamento 2-1 em três sites, enquanto os objetos pertencentes a outros locatários (e objetos menores pertencentes ao Locatário A) serão protegidos em três sites que usam replicação de 3-copy.

Regra 1: Codificação de apagamento de três locais para o Locatário A.

Definição de regra	Exemplo de valor
Nome da regra	Codificação de apagamento de três locais para o Locatário A
Conta de locatário	Inquilino A
Pool de storage	Todos os sites 3 (inclui Site 1, Site 2 e Site 3)
Colocações	Codificação de apagamento 2-1 em todos os 3 sites do dia 0 para sempre

Regra 2: Replicação de três locais para outros locatários

Definição de regra	Exemplo de valor
Nome da regra	Replicação de três locais para outros locatários
Conta de locatário	Ignorar
Pools de armazenamento	Site 1, Site 2 e Site 3
Colocações	Três cópias replicadas do dia 0 para sempre: Uma cópia no local 1, uma cópia no local 2 e uma cópia no local 3.

Ativar a política de ILM proposta, por exemplo, 6

Quando você ativa uma nova política proposta de ILM, objetos existentes podem ser movidos para novos locais ou novas cópias de objetos podem ser criadas para objetos existentes, com base nas instruções de

posicionamento em quaisquer regras novas ou atualizadas.



Erros em uma política ILM podem causar perda de dados irrecuperável. Analise e simule cuidadosamente a política antes de ativá-la para confirmar que funcionará como pretendido.



Quando você ativa uma nova política de ILM, o StorageGRID a usa para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Antes de ativar uma nova política de ILM, revise todas as alterações no posicionamento de objetos replicados e codificados por apagamento existentes. Alterar a localização de um objeto existente pode resultar em problemas de recursos temporários quando os novos posicionamentos são avaliados e implementados.

O que acontece quando as instruções de codificação de apagamento mudam

Na política ILM atualmente ativa para este exemplo, os objetos pertencentes ao Tenant A são protegidos usando codificação de apagamento 2-1 no Site 1. Na nova política proposta de ILM, os objetos pertencentes ao Tenant A serão protegidos usando codificação de apagamento 2-1 nos sites 1, 2 e 3.

Quando a nova política ILM é ativada, ocorrem as seguintes operações ILM:

- Novos objetos ingeridos pelo Tenant A são divididos em dois fragmentos de dados e um fragmento de paridade é adicionado. Em seguida, cada um dos três fragmentos é armazenado em um local diferente.
- Os objetos existentes pertencentes ao locatário A são reavaliados durante o processo de digitalização ILM em curso. Como as instruções de posicionamento do ILM usam um novo perfil de codificação de apagamento, fragmentos totalmente novos codificados de apagamento são criados e distribuídos para os três sites.



Os fragmentos existentes de 2 e 1 no local 1 não são reutilizados. O StorageGRID considera que cada perfil de codificação de apagamento é exclusivo e não reutiliza fragmentos de codificação de apagamento quando um novo perfil é usado.

O que acontece quando as instruções de replicação mudam

Na política de ILM atualmente ativa, neste exemplo, os objetos pertencentes a outros locatários são protegidos usando duas cópias replicadas em pools de storage nos locais 1 e 2. Na nova política de ILM proposta, os objetos pertencentes a outros locatários serão protegidos usando três cópias replicadas em pools de storage nos locais 1, 2 e 3.

Quando a nova política ILM é ativada, ocorrem as seguintes operações ILM:

- Quando qualquer locatário que não o Locatário Ingerer um novo objeto, o StorageGRID cria três cópias e salva uma cópia em cada local.
- Os objetos existentes pertencentes a esses outros inquilinos são reavaliados durante o processo de digitalização ILM em curso. Como as cópias de objeto existentes no local 1 e no local 2 continuam a satisfazer os requisitos de replicação da nova regra ILM, o StorageGRID só precisa criar uma nova cópia do objeto para o local 3.

Impacto da ativação desta política no desempenho

Quando a política de ILM proposta neste exemplo é ativada, o desempenho geral deste sistema StorageGRID será temporariamente afetado. Níveis mais altos do que o normal de recursos de grade serão necessários para criar novos fragmentos codificados por apagamento para os objetos existentes do Locatário A e novas

cópias replicadas no local 3 para objetos existentes de outros locatários.

Como resultado da mudança de política do ILM, as solicitações de leitura e gravação do cliente podem ter latências temporariamente maiores do que as normais. As latências retornarão aos níveis normais depois que as instruções de colocação forem totalmente implementadas em toda a grade.

Para evitar problemas de recursos ao ativar uma nova política de ILM, você pode usar o filtro avançado de tempo de ingestão em qualquer regra que possa alterar o local de um grande número de objetos existentes. Defina o tempo de ingestão para ser maior ou igual ao tempo aproximado em que a nova política entrará em vigor para garantir que os objetos existentes não sejam movidos desnecessariamente.



Entre em Contato com o suporte técnico se precisar diminuir ou aumentar a taxa na qual os objetos são processados após uma alteração de política ILM.

Exemplo 7: Política de ILM compatível para bloqueio de objetos S3

Você pode usar o bucket S3, as regras ILM e a política ILM neste exemplo como ponto de partida ao definir uma política ILM para atender aos requisitos de proteção e retenção de objetos em buckets com o bloqueio de objetos S3 ativado.



Se você usou o recurso de conformidade legada em versões anteriores do StorageGRID, também poderá usar este exemplo para ajudar a gerenciar quaisquer buckets existentes que tenham o recurso de conformidade legada habilitado.



As seguintes regras e políticas do ILM são apenas exemplos. Existem muitas maneiras de configurar regras ILM. Antes de ativar uma nova política, simule a política proposta para confirmar que ela funcionará como a intenção de proteger o conteúdo contra perda.

Informações relacionadas

- ["Gerencie objetos com o S3 Object Lock"](#)
- ["Crie uma política ILM"](#)

Bucket e objetos para o exemplo de bloqueio de objetos do S3

Neste exemplo, uma conta de locatário do S3 chamada Bank of ABC usou o Gerenciador do Locatário para criar um bucket com o bloqueio de objeto do S3 habilitado para armazenar Registros bancários críticos.

Definição do balde	Exemplo de valor
Nome da conta do locatário	Banco do ABC
Nome do balde	registros bancários
Região do balde	us-east-1 (predefinição)

Cada versão de objeto e objeto adicionada ao bucket de Registros bancários usará os seguintes valores para `retain-until-date` as configurações e `legal hold`.

Definição para cada objeto	Exemplo de valor
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 de dezembro de 2030) Cada versão de objeto tem sua <code>retain-until-date</code> própria configuração. Esta definição pode ser aumentada, mas não diminuída.
<code>legal hold</code>	"OFF" (Não em vigor) Uma retenção legal pode ser colocada ou levantada em qualquer versão do objeto a qualquer momento durante o período de retenção. Se um objeto estiver sob uma retenção legal, o objeto não poderá ser excluído mesmo que o <code>retain-until-date</code> tenha sido alcançado.

Regra ILM 1 para o bloqueio de objetos S3 exemplo: Apagar perfil de codificação com correspondência de bucket

Este exemplo de regra ILM aplica-se apenas à conta de locatário S3 chamada Bank of ABC. Ele corresponde a qualquer objeto no `bank-records` bucket e, em seguida, usa a codificação de apagamento para armazenar o objeto em nós de storage em três locais de data center usando um 6 perfil de codificação de apagamento de mais de 3 anos. Essa regra atende aos requisitos dos buckets com o bloqueio de objetos S3 ativado: Uma cópia é mantida nos nós de storage do dia 0 para sempre, usando o tempo de ingestão como o tempo de referência.

Definição de regra	Exemplo de valor
Nome da regra	Regra compatível: Objetos EC no bucket de Registros bancários - Banco do ABC
Conta de locatário	Banco do ABC
Nome do balde	<code>bank-records</code>
Filtro avançado	Tamanho do objeto (MB) maior que 1 Nota: este filtro garante que a codificação de apagamento não seja usada para objetos de 1 MB ou menores.

Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
Colocações	Desde o dia 0 para sempre
Perfil de codificação de apagamento	<ul style="list-style-type: none"> • Crie uma cópia codificada por apagamento em nós de storage em três locais de data center • Usa o esquema de codificação de apagamento 6-3

Regra ILM 2 para o exemplo de bloqueio de objetos S3: Regra não compatível

Este exemplo de regra de ILM armazena inicialmente duas cópias de objeto replicadas em nós de storage. Após um ano, ele armazena uma cópia em um pool de storage de nuvem para sempre. Como essa regra usa um pool de armazenamento em nuvem, ela não é compatível e não se aplica aos objetos em buckets com o bloqueio de objetos do S3 ativado.

Definição de regra	Exemplo de valor
Nome da regra	Regra não compatível: Use o Cloud Storage Pool
Contas de inquilino	Não especificado
Nome do intervalo	Não especificado, mas só se aplicará a buckets que não tenham o bloqueio de objeto S3 (ou o recurso de conformidade legado) habilitado.
Filtro avançado	Não especificado

Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
Colocações	<ul style="list-style-type: none">• No dia 0, mantenha duas cópias replicadas nos nós de storage no data center 1 e no data center 2 por 365 dias• Após 1 ano, mantenha uma cópia replicada em um pool de storage de nuvem para sempre

Regra ILM 3 para o exemplo de bloqueio de objetos S3: Regra padrão

Este exemplo de regra de ILM copia dados de objetos para pools de storage em dois data centers. Esta regra compatível foi projetada para ser a regra padrão na política ILM. Ele não inclui nenhum filtro, não usa o tempo de referência não atual e satisfaz os requisitos de buckets com o bloqueio de objeto S3 ativado: Duas cópias de objeto são mantidas em nós de armazenamento do dia 0 para sempre, usando a ingestão como o tempo de referência.

Definição de regra	Exemplo de valor
Nome da regra	Regra de conformidade padrão: Duas cópias dois Data Centers
Conta de locatário	Não especificado
Nome do intervalo	Não especificado
Filtro avançado	Não especificado

Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão

Definição de regra	Exemplo de valor
Colocações	Do dia 0 até sempre, mantenha duas cópias replicadas: Uma em nós de storage no data center 1 e uma em nós de storage no data center 2.

Política ILM compatível para o exemplo de bloqueio de objetos S3

Para criar uma política de ILM que proteja efetivamente todos os objetos em seu sistema, incluindo aqueles em buckets com o bloqueio de objetos S3 ativado, você deve selecionar regras de ILM que atendam aos requisitos de armazenamento de todos os objetos. Em seguida, você deve simular e ativar a política proposta.

Adicione regras à política

Neste exemplo, a política ILM inclui três regras ILM, na seguinte ordem:

1. Uma regra compatível que usa codificação de apagamento para proteger objetos com mais de 1 MB em um bucket específico com o bloqueio de objetos S3 ativado. Os objetos são armazenados 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 um pool de storage de nuvem para sempre. Esta regra não se aplica a buckets com o bloqueio de objetos do S3 ativado porque usa um pool de armazenamento em nuvem.
3. A regra em conformidade padrão que cria duas cópias de objetos replicadas nos nós de storage do dia 0 para sempre.

Simule a política proposta

Depois de adicionar regras em sua política proposta, escolher uma regra compatível padrão e organizar as outras regras, você deve simular a política testando objetos do bucket com o bloqueio de objeto S3 ativado e de outros buckets. Por exemplo, quando você simula a política de exemplo, espera-se que os objetos de teste sejam avaliados da seguinte forma:

- A primeira regra só corresponderá a objetos de teste maiores que 1 MB nos Registros de banco de buckets para o locatário do Bank of ABC.
- A segunda regra corresponderá a todos os objetos em todos os buckets não compatíveis para todas as outras contas de inquilino.
- A regra padrão corresponderá a estes objetos:
 - Objetos 1 MB ou mais pequenos nos Registros de banco de buckets para o inquilino do Banco do ABC.
 - Objetos em qualquer outro bucket que tenha o bloqueio de objeto S3 ativado para todas as outras contas de locatário.

Ative a política

Quando você estiver completamente satisfeito que a nova política protege os dados de objetos conforme esperado, você pode ativá-los.

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.